Claude SERVIN

Préface de Jean-Pierre Arnaud

RÉSEAUX & TÉLÉCOMS

Cours avec 129 exercices corrigés

2e édition

DUNOD

RÉSEAUX & TÉLÉCOMS

Pour plus de livres rejoignez nous sur
heights-book.blogspot.com

Consultez nos catalogues sur le Web



www.dunod.com

RÉSEAUX & TÉLÉCOMS

Cours avec 129 exercices corrigés

Claude Servin
Chargé de cours au CNAM de Paris
Ancien responsable réseaux et télécoms
au sein du ministère de la Défense

Préface de
Jean-Pierre Arnaud
Professeur au CNAM

2e édition

DUNOD

Illustration de couverture :
Contexture, PhotoDisc by Getty Images

Ce pictogramme mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du **photocopillage**.

Le Code de la propriété intellectuelle du 1er juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée.



Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation du Centre français d'exploitation du droit de copie (**CFC**, 20 rue des Grands-Augustins, 75006 Paris).

© Dunod, Paris, 2003, 2006
ISBN 2 10 049148 2

Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite selon le Code de la propriété intellectuelle (Art L 122-4) et constitue une contrefaçon réprimée par le Code pénal. • Seules sont autorisées (Art L 122-5) les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective, ainsi que les analyses et courtes citations justifiées par le caractère critique, pédagogique ou d'information de l'œuvre à laquelle elles sont incorporées, sous réserve, toutefois, du respect des dispositions des articles L 122-10 à L 122-12 du même Code, relatives à la reproduction par reprographie.

Préface

Le domaine des Télécommunications et des Réseaux est en pleine effervescence, chaque semaine qui s'écoule apporte sa moisson de nouvelles offres, d'annonces et de propositions de norme. Confronté à ce flux incessant de nouveautés, le praticien doit faire des choix qui s'avéreront stratégiques pour l'entreprise et structurants pour l'avenir de son système d'information. C'est dire l'importance de disposer de bases solides, seules aptes à évaluer sainement la pertinence des solutions proposées par les constructeurs de matériels et les éditeurs de logiciels. Encore faut-il s'entendre sur la constitution de cette base : il ne s'agit pas d'amasser des connaissances plus ou moins vagues ou plus ou moins utiles, mais de construire un socle sur lequel pourra s'appuyer une réflexion personnelle.

Dans la conjoncture actuelle, il n'est guère de tâche plus utile que de transmettre ces connaissances et d'enseigner les méthodes qui permettent d'en tirer profit. L'évolution technologique imposait une nouvelle édition des ouvrages de Claude Servin. Pour distinguer ce qui, dans cette multitude d'évolutions, est suffisamment assuré pour mériter d'être enseigné, il fallait la pratique du terrain d'un homme de réseaux. Il fallait aussi allier à cette expérience de l'ingénieur qui crée des projets celle de l'enseignant qui transmet les savoirs nécessaires à cette création.

Claude Servin possède assurément l'une et l'autre et c'est ce qui donne à son ouvrage un intérêt tout particulier. Ses lecteurs apprécieront une présentation simple des concepts les plus fondamentaux, débarrassés de tout hermétisme et orientés vers l'action et l'ingénierie, sans céder aux modes passagères ou aux complexités inutiles qui encombrent bien des manuels.

Ce sont ces qualités qui lui ont permis de s'inscrire avec réussite dans les enseignements dispensés au Conservatoire national des Arts et Métiers (CNAM) et de jouer le rôle de pivot vers des enseignements plus spécialisés.

Déjà inséré dans le monde du travail, le public du CNAM est exigeant, il vient y chercher une mise en perspective et une rigueur sans faille. Il ne saurait se satisfaire de l'autorité d'un enseignant qui ne pourrait faire preuve de sa capacité à maîtriser les enjeux technologiques actuels. Claude Servin a su les convaincre et, comme les auditeurs qui se pressent nombreux à ses cours et

y trouvent l'impulsion pour un approfondissement ultérieur, je suis certain que le lecteur trouvera à la lecture de cet ouvrage un intérêt soutenu et qu'il sera son compagnon pendant encore de longues années. Les manuels d'enseignement auxquels on continue de se référer une fois entré dans la vie active ne sont pas si nombreux : ayant personnellement l'expérience de la direction de sociétés dans le domaine des réseaux, je ne saurais faire à cet ouvrage un meilleur compliment que de dire qu'il fait partie de ceux-là.

Jean-Pierre ARNAUD
Professeur au Conservatoire national des Arts et Métiers
Titulaire de la chaire de Réseaux

Table des matières

PRÉFACE V

AVANT-PROPOS XXI

PARTIE I • **CONCEPTS FONDAMENTAUX** 1

CHAPITRE 1 • **L'INFORMATION ET SA REPRÉSENTATION DANS LES SYSTÈMES DE TRANSMISSION** 3

1.1 Généralités 3
1.1.1 Les flux d'information 3
1.1.2 Les caractéristiques des réseaux de transmission 4

1.2 La représentation de l'information 6
1.2.1 Les différents types d'information 6
1.2.2 Le codage des informations 6
1.2.3 La numérisation des informations 12

1.3 La compression de données 21
1.3.1 Généralités 21
1.3.2 La quantification de la compression 21
1.3.3 La compression sans perte 22
1.3.4 Les codages à réduction de bande 22

1.4 La notion de qualité de service 33
1.4.1 Les données et les contraintes de transmission 33
1.4.2 Les classes de service 34
1.4.3 Conclusion 36

EXERCICES 37

CHAPITRE 2 • **LES SUPPORTS DE TRANSMISSION** 39

2.1 Généralités 39

2.2 Les caractéristiques des supports de transmission 40
2.2.1 La bande passante et le système de transmission 40
2.2.2 L'impédance caractéristique 43
2.2.3 Le coefficient de vélocité 45
2.3 Les supports guidés 46
2.3.1 La paire torsadée 46
2.3.2 Le câble coaxial 48
2.3.3 La fibre optique 49
2.3.4 Les liaisons hertziennes 53
2.4 Conclusion 60
EXERCICES 61

CHAPITRE 3 • **ÉLÉMENTS DE BASE DE LA TRANSMISSION DE DONNÉES** 63
3.1 Introduction 63
3.2 L'organisation fonctionnelle et physique des échanges 64
3.2.1 L'organisation des échanges 64
3.2.2 L'organisation physique 65
3.3 Le mode d'adaptation au support 73
3.3.1 Généralités 73
3.3.2 La transmission en bande de base 74
3.3.3 La transmission en large bande 84
3.3.4 Les liaisons *full duplex* 88
3.3.5 Les dispositifs complémentaires 89
3.3.6 Exemples de modem 92
3.3.7 Principaux avis du CCITT 94
3.3.8 Comparaison transmission bande de base et large bande 94
3.4 La jonction DTE/DCE ou interface 96
3.4.1 Nécessité de définir une interface standard 96
3.4.2 Les principales interfaces 97
3.5 Conclusion 105
EXERCICES 105

CHAPITRE 4 • **NOTIONS DE PROTOCOLES** 109
4.1 Généralités 109
4.2 Les type de liaisons et leur contrôle 110
4.2.1 La liaison point à point 110
4.2.2 Les liaisons multipoints 110
4.3 Les fonctions élémentaires 111
4.3.1 La délimitation des données 111
4.3.2 Le contrôle d'intégrité 113
4.3.3 Le contrôle de l'échange 121
4.3.4 Le contrôle de flux 131

4.4 La signalisation 134
4.4.1 Définition 134
4.4.2 La signalisation dans la bande 134
4.4.3 La signalisation hors bande 135
4.5 L'étude succincte d'un protocole de transmission (HDLC) 136
4.5.1 Généralités 136
4.5.2 La structure de la trame HDLC 137
4.5.3 Les différentes fonctions de la trame HDLC 137
4.5.4 Le fonctionnement d'HDLC 139
4.5.5 Les différentes versions du protocole HDLC 143
4.5.6 HDLC et les environnements multiprotocoles 144
4.6 Conclusion 144
EXERCICES 145

CHAPITRE 5 • **MUTUALISATION DES RESSOURCES** 147
5.1 Introduction 147
5.2 La quantification de trafic 147
5.2.1 Généralités 147
5.2.2 L'intensité de trafic et le taux d'activité 148
5.3 Les concentrateurs 151
5.3.1 Principe 151
5.3.2 Les fonctionnalités complémentaires, exemple d'application 152
5.4 Les multiplexeurs 153
5.4.1 Principe 153
5.4.2 Le multiplexage spatial 154
5.4.3 Le multiplexage temporel 156
5.4.4 Comparaison multiplexeur/concentrateur 160
5.5 Le multiplexage et l'accès à l'interface radio 161
5.5.1 Principe 161
5.5.2 Les techniques d'accès multiple 161
5.6 Le concept de réseau à commutation 165
5.6.1 Définitions 165
5.6.2 La classification des réseaux 166
5.6.3 La topologie physique des réseaux 168
5.6.4 Les réseaux à commutation 170
5.7 Conclusion 174
EXERCICES 175

CHAPITRE 6 • **LES RÉSEAUX À COMMUTATION DE PAQUETS** 177
6.1 Généralités 177
6.2 Les performances de la commutation de paquets 178

© Dunod – La photocopie non autorisée est un délit

6.3 Du mode datagramme au mode connecté 179
6.3.1 Principe 179
6.3.2 Les modes de mise en relation 181
6.4 La notion d'adressage 183
6.4.1 Définition 183
6.4.2 L'adressage physique 184
6.5 La notion de nommage 188
6.5.1 Le nommage 188
6.5.2 La notion d'annuaire 188
6.6 L'acheminement dans le réseau 189
6.6.1 Définitions 189
6.6.2 Les protocoles de routage 190
6.7 L'adaptation de la taille des unités de données 201
6.7.1 La notion de MTU 201
6.7.2 La segmentation et le réassemblage 202
6.8 La congestion dans les réseaux 203
6.8.1 Définition 203
6.8.2 Les mécanismes de prévention de la congestion 204
6.8.3 La résolution ou la guérison de la congestion 206
6.9 La voix dans les réseaux en mode paquet 207
6.9.1 Intérêt et contraintes 207
6.9.2 Le principe de la paquétisation de la voix 207
6.10 Conclusion 208
EXERCICES 209

PARTIE II • **L'ARCHITECTURE PROTOCOLAIRE** 211

CHAPITRE 7 • **LES ARCHITECTURES PROTOCOLAIRES** 213
7.1 Introduction 213
7.2 Les concepts de base 214
7.2.1 Principe de fonctionnement d'une architecture en couches 214
7.2.2 La terminologie 215
7.3 L'organisation du modèle de référence 219
7.3.1 Les concepts ayant conduit à la modélisation 219
7.3.2 La description du modèle de référence 220
7.4 L'étude succincte des couches 225
7.4.1 La couche physique 225
7.4.2 La couche liaison de données 226
7.4.3 La couche réseau 227
7.4.4 La couche transport 231
7.4.5 La couche session 235
7.4.6 La couche présentation 236

7.4.7 La couche application 238
7.4.8 Devenir du modèle OSI 241
7.5 Les architectures constructeurs 243
7.5.1 L'architecture physique d'un système de téléinformatique 243
7.5.2 L'origine des architectures constructeurs 243
7.6 Conclusion 244
EXERCICES 245

CHAPITRE 8 • **INTRODUCTION À TCP/IP** 247
8.1 Généralités 247
8.1.1 Origine 247
8.1.2 Principe architectural 247
8.1.3 La description générale de la pile et les applications TCP/IP 249
8.1.4 Les mécanismes de base de TCP/IP 250
8.1.5 Les instances de normalisation 253
8.2 L'adressage dans le réseau logique 253
8.2.1 Principe de l'adressage IP 253
8.2.2 Les techniques d'adressage dans un réseau IP 255
8.3 Le routage dans le réseau IP 264
8.3.1 L'adressage d'interface 264
8.3.2 Le concept d'interface non numérotée 265
8.4 L'adressage dans IPv6 266
8.4.1 Généralités 266
8.4.2 La notation et le type d'adresse 267
8.4.3 Le plan d'adressage 268
8.4.4 L'adressage de transition d'IPv4 vers IPv6 270
8.5 Conclusion 270
EXERCICES 271

CHAPITRE 9 • **L'ARCHITECTURE TCP/IP ET LE NIVEAU LIAISON** 273
9.1 Généralités 273
9.2 Les protocoles de liaison (point à point) 274
9.2.1 Généralités 274
9.2.2 SLIP, *Serial Line Internet Protocol* (RFC 1055) 274
9.2.3 PPP, *Point to Point Protocol* (RFC 1548 et 1661, 1662) 275
EXERCICE 286

CHAPITRE 10 • **LE PROTOCOLE IP ET LES UTILITAIRES RÉSEAUX** 289
10.1 Généralités 289
10.2 La structure du datagramme IP 289
10.3 Le contrôle de la fragmentation sous IP 294

© Dunod – La photocopie non autorisée est un délit

10.4 Les utilitaires de la couche réseau 295
10.4.1 Le protocole ICMP 295
10.4.2 La résolution d'adresses 298
10.4.3 Les utilitaires de configuration 301
10.4.4 Conclusion 304
10.5 D'IPv4 à IPv6 305
10.5.1 Les lacunes d'IPv4 305
10.5.2 Le datagramme IPv6 305
10.6 IP et la mobilité 309
10.6.1 Généralités 309
10.6.2 Le principe de la mobilité sous IPv4 309
10.6.3 La mobilité dans IPv6 314
10.6.4 Conclusion 315
10.7 L'encapsulation GRE 315
10.8 Conclusion 316
EXERCICE 317

CHAPITRE 11 • **LES PROTOCOLES DE TRANSPORT : TCP ET UDP** 319
11.1 Généralités 319
11.2 Les mécanismes de base de TCP 320
11.2.1 La notion de connexion de transport 320
11.2.2 Notion de multiplexage de connexion de transport 320
11.2.3 L'établissement de la connexion de transport 322
11.2.4 Le mécanisme contrôle de l'échange 323
11.2.5 Le contrôle de flux et de congestion 326
11.3 Le message TCP et les mécanismes associés 330
11.3.1 La structure du segment TCP 330
11.3.2 Le contrôle d'erreur 331
11.3.3 La « bufferisation » des données 332
11.4 Les options de TCP 332
11.4.1 La taille des segments 333
11.4.2 L'option d'estampille horaire 333
11.4.3 Le TCP et les réseaux à haut débit 334
11.5 Le mode datagramme (UDP) 335
11.6 Conclusion 335
EXERCICES 337

CHAPITRE 12 • **TCP/IP ET LES APPLICATIONS** 339
12.1 Introduction 339
12.2 Les notions d'annuaire 339
12.2.1 Généralités 339

12.2.2 Le service de noms (DNS) 340
12.2.3 La généralisation de la notion d'annuaire 346
12.3 Le transfert de fichiers 348
12.3.1 TFTP (*Trivial File Transfert Protocol*) 348
12.3.2 FTP (*File Transfert Protocol*) 350
12.4 L'émulation de terminal (Telnet) 351
12.4.1 Principe de Telnet 351
12.4.2 Les commandes et les modes de fonctionnement 352
12.5 Les notions de Middleware 353
12.5.1 Définitions 353
12.5.2 Les exemples d'outils *milddleware* dans TCP/IP 354
12.5.3 Internet et le *middleware* 357
12.6 Conclusion 358
EXERCICES 360

PARTIE III • **MISE EN ŒUVRE** 361

CHAPITRE 13 • **INTRODUCTION AUX RÉSEAUX DE TRANSPORT** 363
13.1 Généralités 363
13.2 Le plan de transmission 364
13.2.1 Généralités 364
13.2.2 La synchronisation des réseaux 364
13.2.3 La hiérarchie plésiochrone (PDH) 368
13.2.4 La hiérarchie synchrone (SDH) 370
13.2.5 La transmission optique 373
13.3 Le plan de service 374
13.3.1 Généralités 374
13.3.2 Introduction aux protocoles réseaux 375
13.3.3 Les réseaux d'opérateurs 381
13.4 L'accès aux réseaux, la boucle locale 383
13.4.1 Définition 383
13.4.2 Organisation de la distribution des accès 383
13.4.3 L'accès aux réseaux par liaison dédiée (ligne spécialisée) 384
13.4.4 La Boucle locale radio (BLR) 387
13.4.5 Les accès hauts débits 388
13.4.6 Les courants porteurs 393
13.5 Conclusion 394
EXERCICES 395

CHAPITRE 14 • **LES PROTOCOLES DE CŒUR DE RÉSEAU** 397
14.1 Le protocole X.25 397
14.1.1 Généralités 397

© Dunod – La photocopie non autorisée est un délit

14.1.2 Le niveau X.25-1 397
14.1.3 Le niveau X.25-2 398
14.2 Le relais de trame ou Frame relay 411
14.2.1 Généralités 411
14.2.2 Le format de l'unité de données 412
14.2.3 Les mécanismes élémentaires 412
14.3 L'ATM (*Asynchronous Transfer Mode*) 421
14.3.1 Généralités 421
14.3.2 La taille des unités de données ou cellules 422
14.3.3 Les mécanismes de base et le format de la cellule ATM 424
14.3.4 Les différentes couches du modèle 427
14.3.5 La qualité de service dans l'ATM 431
14.3.6 Le contrôle de flux et de congestion 433
14.3.7 La signalisation et le routage 434
14.3.8 L'administration des réseaux ATM 437
14.4 Conclusion 438
EXERCICES 439

CHAPITRE 15 • **MPLS, *MULTIPROTOCOL LABEL SWITCHING*** 443
15.1 Généralités 443
15.2 Principe 443
15.3 Le réseau MPLS 444
15.3.1 Le commutateur MPLS 444
15.3.2 Le principe de base d'un réseau MPLS 445
15.3.3 Les mécanismes particuliers 446
15.4 MPLS et les infrastructures existantes 448
15.4.1 Généralités 448
15.4.2 La gestion du TTL 449
15.4.3 MPLS et ATM 449
15.5 La construction des routes dans un réseau MPLS 451
15.5.1 Généralités 451
15.5.2 Le protocole LDP (RFC 3036) 452
15.6 MPLS et l'ingénierie de trafic 454
15.7 Les VPN MPLS 454
15.7.1 Notions de base sur les VPN 454
15.7.2 Principe général des VPN MPLS 457
15.8 Conclusion 459
EXERCICE 460

CHAPITRE 16 • **LES RÉSEAUX LOCAUX ET MÉTROPOLITAINS** 461

16.1 Introduction 461
16.1.1 Définition 461
16.1.2 Distinction entre réseau local et informatique traditionnelle 462
16.1.3 Les réseaux locaux et l'accès aux systèmes traditionnels 462
16.1.4 Les constituants d'un réseau local 463
16.1.5 Les réseaux locaux et la normalisation 465

16.2 Étude succincte des différentes couches 466
16.2.1 La couche physique 466
16.2.2 La sous-couche MAC 469
16.2.3 La couche liaison (LLC) 473

16.3 Étude succincte des principales implémentations 477
16.3.1 L'anneau à jeton, IEEE 802.5 477
16.3.2 Le jeton adressé ou Token Bus, IEEE 802.4 480
16.3.3 Le réseau 100 VG AnyLAN, 802.12 482

16.4 Les réseaux locaux ATM 484
16.4.1 Généralités 484
16.4.2 « *Classical IP* » ou « *IP over ATM* » 485
16.4.3 *LAN Emulation* 487

16.5 Les réseaux métropolitains 492
16.5.1 Généralités 492
16.5.2 FDDI (*Fiber Distributed Data Interface*) 492
16.5.3 DQDB (*Distributed Queue Dual Bus*) 494

16.6 Les canaux hauts débits 496
16.6.1 HiPPI 497
16.6.2 *Fibre Channel Standard* 497

16.7 Conclusion 498

EXERCICES 499

CHAPITRE 17 • **ETHERNET ET SES ÉVOLUTIONS SANS FIL** 501

17.1 Introduction 501

17.2 Les caractéristiques générales des réseaux Ethernet/802.3 501
17.2.1 Le principe du CSMA/CD 501
17.2.2 La fenêtre de collision 503
17.2.3 L'algorithme du BEB 504
17.2.4 Le silence inter-message (IFG, *InterFrame Gap*) 505
17.2.5 Le format des trames Ethernet/IEEE 802.3 505
17.2.6 Les erreurs 506

17.3 Les différentes versions d'Ethernet 506
17.3.1 Présentation 506
17.3.2 L'Ethernet épais, IEEE 802.3 10Base5 507
17.3.3 L'Ethernet fin, IEEE 802.3 10Base2 508

© Dunod – La photocopie non autorisée est un délit

17.3.4 L'Ethernet sur paires torsadées, IEEE 802.3 10BaseT 509
17.3.5 L'Ethernet à 100 Mbit/s 511
17.3.6 Le Gigabit Ethernet 513
17.3.7 Le 10 Gigabit Ethernet 517
17.3.8 Le devenir d'Ethernet 518
17.4 L'Ethernet sans fil 518
17.4.1 Généralités 518
17.4.2 La problématique de l'accès aux réseaux sans fil 519
17.4.3 L'architecture générale des réseaux sans fil 520
17.4.4 Les réseaux 802.11 522
17.4.5 Les réseaux IEEE 802.15-1 (Bluetooth) 536
17.5 Conclusion 541
EXERCICES 542

CHAPITRE 18 • **PONTAGE, COMMUTATION ET VLAN** 545
18.1 Pont ou commutateur ? 545
18.2 Les ponts 546
18.2.1 Généralités 546
18.2.2 Les différents types de ponts 547
18.2.3 Les ponts transparents 547
18.2.4 Le *Spanning Tree Protocol* (STP) ou arbre recouvrant 549
18.2.5 Les ponts à routage par la source 553
18.2.6 Le pontage par translation 555
18.3 La commutation dans les LAN 556
18.3.1 Principe de base 556
18.3.2 Notion d'architecture des commutateurs 557
18.3.3 Les différentes techniques de commutation 559
18.3.4 Les différents modes de commutation 559
18.3.5 Ethernet *full duplex* 560
18.3.6 Pontage, commutation et trafic *multicast* 560
18.4 Les réseaux virtuels ou VLAN (*Virtual Local Area Network*) 562
18.4.1 Principes généraux des VLAN 562
18.4.2 Les différents niveaux de VLAN 563
18.4.3 L'identification des VLAN (802.1Q) 564
18.5 Conclusion 567
EXERCICES 568

CHAPITRE 19 • **INTERCONNEXION DES RÉSEAUX ET QUALITÉ DE SERVICE** 571
19.1 L'interconnexion des réseaux, généralités 571
19.1.1 Définition 571
19.1.2 Les problèmes liés à l'interconnexion 571
19.1.3 Les notions de conversion de service et de protocole 572
19.1.4 L'encapsulation ou *tunneling* 572

19.2 Les éléments d'interconnexion (relais) 576
19.2.1 Définitions 576
19.2.2 Les répéteurs 577
19.2.3 Les ponts 578
19.2.4 Les routeurs 579
19.3 Les techniques de routage 582
19.3.1 Généralités 582
19.3.2 Le routage vecteur-distance, RIP 583
19.3.3 Le routage à état des liens (OSPF) 586
19.3.4 Le routage inter-domaine 595
19.4 Notions de qualité de service 597
19.4.1 Généralités 597
19.4.2 *Integrated Services* 597
19.4.3 *Differentiated Services* 598
19.4.4 Mise en œuvre dans les réseaux d'opérateur 602
19.5 Le *multicast* et le routage *multicast* 603
19.5.1 Introduction au *multicast* 603
19.5.2 Rappel sur l'adressage *multicast* 604
19.5.3 Le protocole local IGMP (RFC 2236) 605
19.5.4 Les protocoles de routage *multicast* 605
19.6 Les fonctions annexes des routeurs 607
19.6.1 Les routeurs multiprotocoles 607
19.6.2 La compression de données 608
19.6.3 Le routage à la demande (*Dial on Demand*) 609
19.6.4 La bande passante à la demande (*Bandwith on Demand*) 609
19.7 Les passerelles applicatives 610
EXERCICES 611

PARTIE IV • **LA VOIX DANS LES RÉSEAUX** 615

CHAPITRE 20 • **INTRODUCTION À LA TÉLÉPHONIE** 617
20.1 Principes généraux de la téléphonie 617
20.2 L'organisation du réseau téléphonique 618
20.2.1 L'architecture traditionnelle 618
20.2.2 La gestion du réseau 619
20.3 L'établissement d'une communication téléphonique 620
20.3.1 Principe d'un poste téléphonique 620
20.3.2 Principe du raccordement d'usager 620
20.3.3 La mise en relation Usager/Usager 621
20.3.4 La numérotation 623
20.3.5 Les modes de signalisation 624

© Dunod – La photocopie non autorisée est un délit

20.4 L'évolution de la téléphonie, le RNIS 625
20.4.1 De l'accès analogique à l'accès numérique 625
20.4.2 Le concept d'intégration de services 626
20.4.3 La structure du réseau 627
20.4.4 Le raccordement d'usager 628
20.4.5 Les services du RNIS 630
20.4.6 La signalisation et le réseau RNIS 632
20.5 La téléphonie et la mobilité 643
20.5.1 Principes généraux 643
20.5.2 La gestion de l'abonné et du terminal 645
20.5.3 L'interface radio 646
20.5.4 Description succincte des différents systèmes en service 649
20.5.5 Le service transport de données sur la téléphonie mobile 649
20.5.6 La mobilité et l'accès à Internet 650
20.5.7 L'évolution des systèmes de téléphonie mobile, l'UMTS 651
20.5.8 La téléphonie satellitaire 652
20.6 Conclusion 653
EXERCICES 654

CHAPITRE 21 • **INSTALLATION D'ABONNÉ ET RÉSEAU PRIVÉ DE TÉLÉPHONIE** 655
21.1 Les autocommutateurs privés 655
21.1.1 Généralités 655
21.1.2 Architecture d'un PABX 656
21.1.3 Les téléservices et applications vocales offerts par les PABX 656
21.1.4 PABX et transmission de données 661
21.2 L'installation d'abonné 662
21.2.1 Généralités 662
21.2.2 Le dimensionnement du raccordement au réseau de l'opérateur 663
21.3 Les réseaux privés de PABX 665
21.3.1 Principes généraux 665
21.3.2 La signalisation et type de liens 667
21.4 Principes des réseaux voix/données 675
21.4.1 Généralités 675
21.4.2 Les réseaux de multiplexeurs 675
21.4.3 La voix paquétisée 676
21.5 La voix sur ATM 683
21.6 La voix sur le Frame Relay 685
21.7 La voix et téléphonie sur IP 687
21.7.1 Généralités 687
21.7.2 TCP/IP et le transport de la voix 688
21.7.3 Les terminaux 691
21.7.4 Les architectures et protocoles de signalisation 693

21.8 Conclusion 703
EXERCICES 704

PARTIE V • **ADMINISTRATION ET INGÉNIERIE** 707

CHAPITRE 22 • **ADMINISTRATION DES RÉSEAUX – PRINCIPES GÉNÉRAUX** 709
22.1 Généralités 709
22.1.1 Définition 709
22.1.2 Principe général 709
22.1.3 Structure d'un système d'administration 710
22.2 L'administration vue par l'ISO 710
22.2.1 Généralités 710
22.2.2 Les différents modèles 711
22.3 L'administration dans l'environnement TCP/IP 714
22.3.1 Principes généraux 714
22.3.2 Les MIB 715
22.3.3 Le protocole SNMP 717
22.4 SNMP et ISO 719
22.5 Les plates-formes d'administration 719
22.5.1 Les outils d'administration des couches basses 719
22.5.2 Les hyperviseurs 719
22.5.3 Les systèmes intégrés au système d'exploitation 720
22.6 Conclusion 720
EXERCICES 721

CHAPITRE 23 • **LA SÉCURITÉ DES SYSTÈMES D'INFORMATION** 723
23.1 Généralités 723
23.2 La sûreté de fonctionnement 723
23.2.1 Principes généraux de la sûreté 723
23.2.2 Les systèmes à tolérance de panne 723
23.2.3 La sûreté environnementale 726
23.2.4 Quantification 728
23.3 La sécurité 730
23.3.1 Généralités 730
23.3.2 La protection des données 730
23.3.3 La protection du réseau 741
23.4 Le commerce électronique 749
23.4.1 Le paiement *off-line* (*e-cash*) 749
23.4.2 Le paiement *on-line* 749
23.5 Conclusion 750
EXERCICES 751

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 24 • **NOTIONS D'INGÉNIERIE DES RÉSEAUX** 755

24.1 Généralités 755

24.2 Les services et la tarification 756

24.3 Les éléments d'architecture réseaux 756
24.3.1 La structure de base des réseaux 756
24.3.2 La conception du réseau de desserte 757
24.3.3 La conception du réseau dorsal 759

24.4 Le dimensionnement et l'évaluation des performances 760
24.4.1 Généralités 760
24.4.2 Les réseaux en mode circuit 760
24.4.3 Les réseaux en mode paquet 763

24.5 Conclusion 768

EXERCICES 769

SOLUTIONS DES EXERCICES 773

SYNTHÈSE DES FONDAMENTAUX 879

GLOSSAIRE 885

ANNEXES 919

A. Normalisation 919

B. Quelques définitions 921

C. Abaques d'Erlang 922

D. Liste des abréviations et sigles utilisés 924

BIBLIOGRAPHIE 931

INDEX 933

Avant-propos

Les télécommunications recouvrent toutes les techniques (filaires, radio, optiques...) de transfert d'information quelle qu'en soit la nature (symboles, écrits, images fixes ou animées, son, ou autres). Ce mot, introduit en 1904 par Édouard Estaunié (polytechnicien, ingénieur général des télégraphes, 1862-1942), fut consacré en 1932 à la conférence de Madrid qui décida de rebaptiser l'Union télégraphique internationale en Union internationale des télécommunications (UIT).

Aujourd'hui, avec la déferlante Internet, les télécommunications ont débordé les domaines de la télégraphie et de la téléphonie. Une ère nouvelle est née, celle de la communication. Cette révolution n'a été rendue possible que par une formidable évolution des technologies. Les progrès réalisés dans le traitement du signal ont permis la banalisation des flux de données et la convergence des techniques. Cette convergence implique de la part des professionnels une adaptation permanente.

Cette dernière ne sera possible que si l'ingénieur ou le technicien possède une base de connaissances suffisamment vaste ; c'est l'objectif de cet ouvrage. À partir de l'information et de sa représentation en machine, *Réseaux et Télécoms* conduit le lecteur des techniques de base des télécommunications à l'ingénierie des réseaux.

Cette nouvelle édition a intégré les nouvelles technologies qui émergentes hier sont une réalité aujourd'hui. Abondamment illustré et avec plus de 130 exercices ou problèmes réseau, cet ouvrage constitue une base de savoir indispensable aux techniciens réseau et aux étudiants.

La première partie est consacrée à l'étude des concepts fondamentaux : la représentation des données, les techniques de base de la transmission de données et la mutualisation des ressources qui trouve sa concrétisation dans le concept de réseau, sont étudiées en détail.

La seconde partie formalise ces concepts en décrivant le principe des architectures protocolaires de réseaux. L'étude de TCP/IP, de son évolution et d'IPv6 y tiennent une place importante.

La troisième partie est consacrée à la mise en œuvre des techniques étudiées précédemment dans la réalisation de réseaux de transport d'information (réseaux longue distance) et de la diffusion de celle-ci (réseaux locaux). L'étude du protocole X.25 a été maintenue, mais une large place a été octroyée à MPLS et au concept de VPN. Les réseaux locaux, notamment dans la version Ethernet, y sont largement détaillés ainsi que la mise en œuvre des réseaux virtuels (VLAN). Enfin, les notions d'interconnexion et de qualité de service concluent cette partie.

La quatrième partie est dédiée à l'étude des réseaux voix et à celle de la convergence de la voix, de la donnée et des images. Après l'étude des solutions de téléphonie traditionnelle, les réseaux voix/données et en particulier l'étude de la voix sur IP font l'objet d'un long développement.

Enfin, la cinquième partie conclut cet ouvrage par l'étude de l'administration des réseaux, de la sécurité et de l'ingénierie des réseaux.

L'étude théorique de chaque chapitre est illustrée ou complétée par de nombreux exercices, problèmes ou études de cas qui pour l'essentiel sont extraits des sujets d'examen de mes enseignements au Conservatoire national des Arts et Métiers de Paris.

Partie **I**

Concepts fondamentaux

1 L'information et sa représentation dans les systèmes de transmission 3
1.1 Généralités 3
1.2 La représentation de l'information 6
1.3 La compression de données 21
1.4 La notion de qualité de service 33
EXERCICES 37

2 Les supports de transmission 39
2.1 Généralités 39
2.2 Les caractéristiques des supports de transmission 40
2.3 Les supports guidés 46
2.4 Conclusion 60
EXERCICES 61

3 Éléments de base de la transmission de données 63
3.1 Introduction 63
3.2 L'organisation fonctionnelle et physique des échanges 64
3.3 Le mode d'adaptation au support 73
3.4 La jonction DTE/DCE ou interface 96
3.5 Conclusion 105
EXERCICES 105

4 Notions de protocoles 109
4.1 Généralités 109
4.2 Les type de liaisons et leur contrôle 110
4.3 Les fonctions élémentaires 111
4.4 La signalisation 134
4.5 L'étude succincte d'un protocole de transmission (HDLC) 136
4.6 Conclusion 144
EXERCICES 145

5 Mutualisation des ressources 147
5.1 Introduction 147
5.2 La quantification de trafic 147
5.3 Les concentrateurs 151
5.4 Les multiplexeurs 153
5.5 Le multiplexage et l'accès à l'interface radio 161
5.6 Le concept de réseau à commutation 165
5.7 Conclusion 174
EXERCICES 175

6 Les réseaux à commutation de paquets 177
6.1 Généralités 177
6.2 Les performances de la commutation de paquets 178
6.3 Du mode datagramme au mode connecté 179
6.4 La notion d'adressage 183
6.5 La notion de nommage 188
6.6 L'acheminement dans le réseau 189
6.7 L'adaptation de la taille des unités de données 201
6.8 La congestion dans les réseaux 203
6.9 La voix dans les réseaux en mode paquet 207
6.10 Conclusion 208
EXERCICES 209

Chapitre **1**

L'information et sa représentation dans les systèmes de transmission

1.1 GÉNÉRALITÉS

1.1.1 Les flux d'information

L'évolution des besoins et des applications informatiques conduit à l'acheminement, dans un même réseau de données informatiques traditionnelles (texte), de la voix et de la vidéo. Transporter sur un même système physique des flux d'information de natures différentes nécessite que chacun d'eux ait une représentation physique identique et que le système de transmission ait la capacité de prendre en compte les contraintes spécifiques à chaque type de flux (figure 1.1).

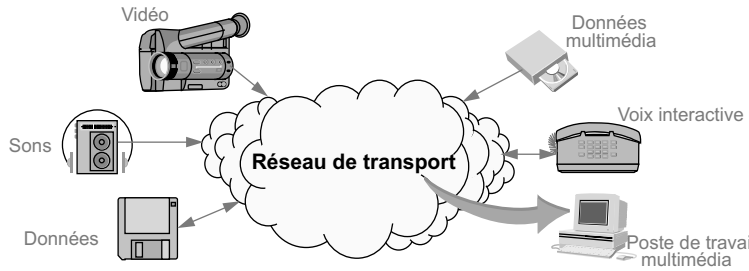


Figure 1.1 Le réseau et les différents flux d'information.

Afin de qualifier ces différents flux vis-à-vis du système de transmission, nous définirons succinctement les caractéristiques essentielles d'un réseau de transmission[1]. Ensuite, nous examinerons le mode de représentation de ces informations. Enfin, nous appliquerons les résultats aux données, à la voix et à l'image pour en déduire les contraintes de transfert spécifiques à chaque type de flux.

1. Ces différentes notions seront revues et approfondies dans la suite de cet ouvrage.

1.1.2 Les caractéristiques des réseaux de transmission

Notion de débit binaire

Les systèmes de traitement de l'information emploient une logique à deux états dite « binaire ». Pour y être traitée, l'information doit être traduite en symboles compréhensibles et manipulables par ces systèmes. Selon le type d'information à transformer, l'opération qui consiste à transformer les données en éléments binaires s'appelle le **codage** ou **numérisation.**

On appelle débit binaire (D) le nombre d'éléments binaires, ou nombre de bits, émis sur le support de transmission pendant une unité de temps. Le débit binaire est généralement la grandeur utilisée en premier pour qualifier un système de transmission ; il s'exprime par la relation :

$$D = \frac{V}{t}$$

avec D (débit) en bits[2] par seconde (bit/s),
V volume à transmettre exprimé en bits,
t durée de la transmission en seconde.

Le débit binaire mesure le nombre d'éléments binaires transitant sur le canal de transmission pendant l'unité de temps (figure 1.2).

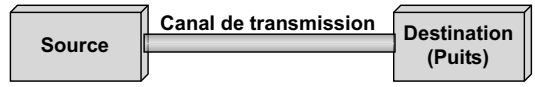


Figure 1.2 La schématisation d'un système de transmission.

Notion de rapport signal sur bruit

Durant la transmission, les signaux électriques peuvent être perturbés par des phénomènes électriques ou électromagnétiques d'origine externe désignés sous le terme générique de **bruit**. Le bruit est un phénomène qui dénature le signal et qui est susceptible d'introduire des erreurs d'interprétation du signal reçu (figure 1.3).

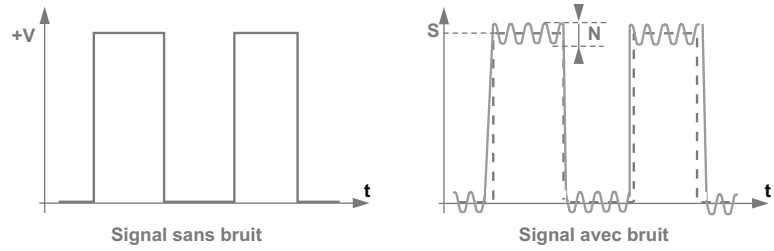


Figure 1.3 Le signal pollué par le bruit.

2. L'unité officielle de débit est le bit/s (invariable). L'abréviation bps pouvant être confondue avec *byte* par seconde ne sera pas utilisée dans cet ouvrage. Rappelons que le terme bit provient de la contraction des termes « *binary digit* ».

Les capacités de transport d'information (débit) sont directement liées au rapport entre la puissance du signal utile et celle du signal de bruit. Ce rapport, appelé rapport signal sur bruit (**SNR**, *Signal Noise Ratio* que nous noterons *S/N*), s'exprime en dB (décibel[3]), formule dans laquelle *S* représente la puissance électrique du signal transmis et *N* la puissance du signal parasite ou bruit affectant le canal de transmission :

$$S/N_{\text{dB}} = 10 \log_{10} (S/N)_{\text{(en puissance)}}$$

Notion d'erreur et de taux d'erreur

Les phénomènes parasites (bruit) perturbent le canal de transmission et peuvent affecter les informations en modifiant un ou plusieurs bits du message transmis, introduisant ainsi des erreurs dans le message (figure 1.4).

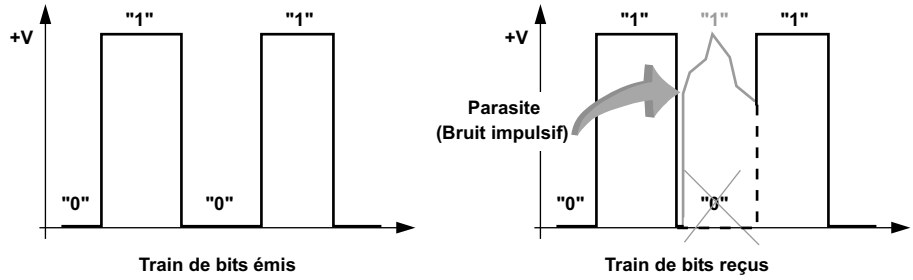


Figure 1.4 L'effet d'une erreur sur le train binaire.

On appelle **taux d'erreur binaire** (*Te* ou **BER**, *Bit Error Rate*) le rapport du nombre de bits reçus en erreur au nombre de bits total transmis.

$$Te = \frac{\text{Nombre de bits en erreur}}{\text{Nombre de bits transmis}}$$

Notion de temps de transfert

Le temps de transfert, appelé aussi temps de transit ou temps de latence, mesure le temps entre l'émission d'un bit, à l'entrée du réseau et sa réception en sortie de ce dernier. Ce temps prend en compte le temps de propagation sur le ou les supports et le temps de traitement par les éléments actifs du réseau (nœuds).

Dans un réseau, le temps de transfert n'est pas une constante, il varie en fonction de la charge du réseau. Cette variation est appelée gigue ou *jitter*. Le temps de transfert conditionne le bon fonctionnement des applications interactives, sa variation le transfert correct d'information comme la voix ou la vidéo.

Notion de spectre du signal

Le mathématicien français Joseph Fourier (1768-1830) a montré que tout signal périodique de forme quelconque pouvait être décomposé en une somme de signaux élémentaires sinusoïdaux

3. Le décibel ou dB (10^{e} du Bel) est une unité logarithmique sans dimension. Elle exprime le rapport entre deux grandeurs de même nature. Le rapport signal/bruit peut aussi s'exprimer par le rapport des tensions, la valeur est alors $S/N_{\text{dB}} = 20 \log_{10} (S/N)_{\text{(en tension)}}$

© Dunod – La photocopie non autorisée est un délit

(fondamental et harmoniques) superposée à une valeur moyenne (composante continue) qui pouvait être nulle. L'ensemble de ces composantes forme le spectre du signal ou bande de fréquence occupée par le signal (largeur de bande).

1.2 LA REPRÉSENTATION DE L'INFORMATION

1.2.1 Les différents types d'information

Les informations peuvent être réparties en deux grandes catégories selon ce qu'elles représentent et les transformations qu'elles subissent pour être traitées dans les systèmes informatiques. On distingue :

- Les **données discrètes**, l'information correspond à l'assemblage d'une suite d'éléments indépendants les uns des autres (suite discontinue de valeurs) et dénombrables (ensemble fini). Par exemple, un texte est une association de mots eux-mêmes composés de lettres (symboles élémentaires).
- Les **données continues ou analogiques** (figure 1.5) résultent de la variation continue d'un phénomène physique : température, voix, image... Un capteur fournit une tension électrique qui varie de manière analogue à l'amplitude du phénomène physique à analyser : signal analogique. Dans un intervalle déterminé (bornes) aussi petit que possible, un signal analogique peut toujours prendre une infinité de valeurs. Par exemple pour passer 10 °C à 11 °C, la température prend, entre ces deux valeurs, une infinité de valeurs sans aucune discontinuité entre elles (fonction continue).

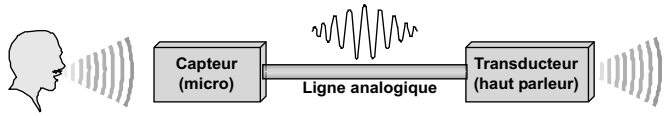


Figure 1.5 Le signal analogique.

Pour être traitées par des équipements informatiques, les informations doivent être représentées par une valeur binaire (**codage à la source**). Le codage à la source est plus spécifiquement appelé codage de l'information pour les informations discrètes et numérisation de l'information pour les informations analogiques.

1.2.2 Le codage des informations

Définition

Coder l'information consiste à faire correspondre (bijection) à chaque symbole d'un alphabet (élément à coder) une représentation binaire (mot code). L'ensemble des mots codes constitue le code (figure 1.6). Ces informations peuvent aussi bien être un ensemble de commandes d'une machine outil, des caractères alphanumériques... Seuls seront traités ici les codages alphanumériques utilisés dans les systèmes de traitement de données. Ces codes peuvent contenir :

- Des chiffres de la numérotation usuelle [0..9] ;
- Des lettres de l'alphabet [a..z, A..Z] ;

– Des symboles nationaux [é, è,...] ;
– Des symboles de ponctuation [, ; : . ? ! ...] ;
– Des symboles semi graphiques [▉ ╠ ╣] ;
– Des commandes nécessaires au système [saut de ligne, saut de page, etc.]

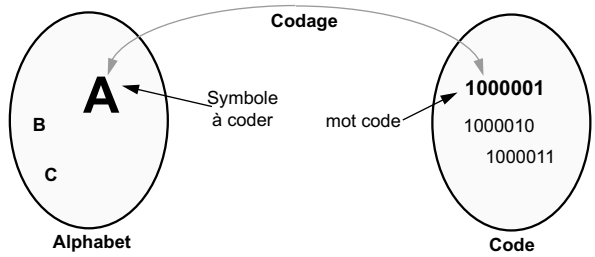


Figure 1.6 Le principe du codage des données.

Les différents types de code

Le codage des différents états d'un système peut s'envisager selon deux approches. La première, la plus simple, considère que chacun des états du système est équiprobable. La seconde prend en compte la fréquence d'apparition d'un état. Ceci nous conduit à définir deux types de code : les codes de longueur fixe et ceux de longueur variable.

➤ Les codes de longueur fixe

Notion de quantité d'information

Chaque état du système est codé par un certain nombre de bits (n), appelé longueur du code, longueur du mot code ou encore code à n moments. Ainsi,

– avec 1 bit, on peut coder 2 états (0,1)
– avec 2 bits 4 états (00, 01, 10, 11)
– avec 3 bits 8 états (000, 001, 010, 011, 100, 101, 110, 111)

D'une manière générale :

– avec n bits, on code 2^n états

Le nombre d'états pouvant être codés par un code de n bits s'appelle puissance lexicographique du code que l'on note :

$$P = 2^n$$

En généralisant, le nombre de bits nécessaires pour coder P états est n, tel que :

$$2^{(n-1)} < P \leqslant 2^n$$

Soit, en se rappelant que le logarithme d'un nombre N est le nombre par lequel il faut élever la base pour retrouver ce nombre (N = base $^{\log N}$), par exemple, le logarithme de 8 à base 2 est 3 car $2^3 = 8$; on peut alors écrire :

$$n = \log_2 P$$

© Dunod – La photocopie non autorisée est un délit

Dans cette formule, le nombre de bits (n) représente la quantité d'information (Q) d'un mot du code. Lorsque dans un système, tous les états sont équiprobables ou considérés comme tel, la quantité d'information apportée par la connaissance d'un état est la même quel que soit l'état connu ; le codage qui en résulte est alors dit à longueur fixe.

L'information élémentaire est représentée par deux valeurs équiprobables (0 ou 1, pile ou face...), la quantité d'information apportée par la connaissance de l'un des états est :

$$Q = \log_2 2 = 1 \text{ shannon ou } 1 \text{ bit.}$$

La quantité d'information Q s'exprime en shannon[4] ou plus simplement en bit. Le bit est la quantité d'information qui correspond au lever de doute entre deux symboles équiprobables. Lorsque tous les états ne sont pas équiprobables, la quantité d'information est d'autant plus grande que la probabilité de réalisation de l'état est faible. Si p est la probabilité de réalisation de l'état P, la quantité d'information apportée par la connaissance de P est :

$$Q = \log_2 1/p$$

Application

En supposant équiprobable l'apparition de chaque lettre, combien de bits sont nécessaires pour coder toutes les lettres de l'alphabet et quelle est la quantité d'information contenue dans la représentation codée d'une lettre ?

Le nombre de bits nécessaires, pour coder P valeurs, est donné par la relation :

$$2^{(n-1)} < P \leqslant 2^n \qquad \text{si } P = 26 \quad \text{on a} \quad 2^4 < 26 \leqslant 2^5$$

soit un code de longueur 5 bits pour coder les 26 éléments. La quantité d'information contenue dans un mot code est de 5 bits.

Cependant, la quantité d'information apportée par la connaissance d'un caractère n'est que de :

$$Q = \log_2 (1/p)$$

où p représente la probabilité d'apparition d'un symbole. Ici $p = 1/26$

$$Q = \log_2 (26) = 3{,}32 \log_{10} (26) = 3{,}32 \cdot 1{,}4149 = 4{,}69 \text{ shannons ou bits}$$

Les principaux codes de longueur fixe

Les codes usuels utilisent cinq éléments (code Baudot), sept éléments (code ASCII appelé aussi CCITT n°5 ou encore IA5) ou huit éléments (EBCDIC).

Le code Baudot, code télégraphique à cinq moments ou alphabet international n°2 ou encore CCITT n°2, est utilisé dans le réseau télex. Le code Baudot autorise 2^5 soit 32 caractères, ce qui est insuffisant pour représenter toutes les lettres de l'alphabet (26), les chiffres (10) et les commandes

4. Les premiers travaux sur la théorie de l'information sont dus à Nyquist (1924). La théorie de l'information fut développée par Shannon en 1949. Les principes établis à cette époque régissent toujours les systèmes de transmission de l'information.

(Fin de ligne...). Deux caractères particuliers permettent la sélection de deux pages de codes soit au total une potentialité de représentation de 60 caractères.

Le code **ASCII** (figure 1.7), *American Standard Code for Information Interchange,* dont la première version date de 1963, est le code générique des télécommunications. Code à sept moments, il autorise 128 caractères (2^7). Les 32 premiers symboles correspondent à des commandes utilisées dans certains protocoles de transmission pour en contrôler l'exécution. La norme de base prévoit des adaptations aux particularités nationales (adaptation à la langue). Ce code, étendu à huit moments, constitue l'alphabet de base des micro-ordinateurs de type PC.

Caractères nationaux

Jeu de commandes

BITS				b_7	0	0	0	0	1	1	1	1
				b_6	0	0	1	1	0	0	1	1
				b_5	0	1	0	1	0	1	0	1
b_4	b_3	b_2	b_1		0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	à	P		p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	£	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	'	6	F	V	f	v
0	1	1	1	7	BEL	ETB	(	7	G	W	g	w
1	0	0	0	8	BS	CAN	)	8	H	X	h	x
1	0	0	1	9	HT	EM	.	9	I	Y	i	y
1	0	1	0	A	LF	SUB		:	J	Z	j	z
1	0	1	1	B	VT	ESC	,	;	K		k	é
1	1	0	0	C	FF	ES		<	L	ç	l	ù
1	1	0	1	D	CR	GS		¨	M	§	m	è
1	1	1	0	E	SO	RS		>	N	^	n	¨
1	1	1	1	F	SI	US	/	?	O	–	o	DEL

Symbole	Signification	
ACK	Acknowledge	Accusé de réception
BEL	Bell	Sonnerie
BS	Backspace	Retour arrière
CAN	Cancel	Annulation
CR	Carriage Return	Retour chariot
DC	Device control	Commande d'appareil auxiliaire
DEL	Delete	Oblitération
DLE	Data Link Escape	Caractère d'échappement
EM	End Medium	Fin de support
ENQ	Enquiry	Demande
EOT	End Of Transmission	Fin de communication
ESC	Escape	Échappement
ETB	End of Transmission Block	Fin de bloc de transmission
ETX	End Of Text	Fin de texte
FE	Format Effector	Commande de mise en page
FF	Form Feed	Présentation de formule

Figure 1.7 Le code ASCII.

© Dunod – La photocopie non autorisée est un délit

Symbole	Signification	Symbole
FS	File Separator	Séparateur de fichiers
GS	Group Separator	Séparateur de groupes
HT	Horizontal Tabulation	Tabulation horizontale
LF	Line Feed	Interligne
NAK	Negative Acknowledge	Accusé de réception négatif
NUL	Null	Nul
RS	Record Separator	Séparateur d'articles
SI	Shift IN	En code
SO	Shift Out	Hors code
SOH	Start Of Heading	Début d'en-tête
SP	Space	Espace
STX	Start Of Text	Début du texte
SYN	Synchronous idle	Synchronisation
TC	Transmission Control	Commande de transmission
US	Unit Separator	Séparateur de sous-article
VT	Vertical Tabulation	Tabulation verticale

Figure 1.7 Le code ASCII. (suite)

Le code **EBCDIC**, *Extended Binary Coded Decimal Interchange Code*, code à huit moments, d'origine IBM, est utilisé dans les ordinateurs du constructeur. Le code EBCDIC a, aussi, été adopté par d'autres constructeurs (notamment Bull) pour leurs calculateurs.

➤ Les codes de longueur variable

Lorsque les états du système ne sont pas équiprobables, la quantité d'information apportée par la connaissance d'un état est d'autant plus grande que cet état a une faible probabilité de se réaliser. La quantité moyenne d'information apportée par la connaissance d'un état, appelée **entropie**, est donnée par la relation :

$$H = \sum_{i=1}^{i=n} p_i \log_2 \frac{1}{p_i}$$

où p_i représente la probabilité d'apparition du symbole de rang i.

L'entropie représente la longueur optimale du codage des symboles du système. Déterminons la longueur optimale du code (entropie) pour le système décrit par le tableau suivant. À des fins de simplicité, chaque état est identifié par une lettre.

État	Probabilité
E	0,48
A	0,21
S	0,12
T	0,08
U	0,06
Y	0,05

La longueur optimale du mot code est :

$$H = -(0{,}48 \log_2 0{,}48 + 0{,}21 \log_2 0{,}21 + 0{,}12 \log_2 0{,}12 + 0{,}08 \log_2 0{,}08 + 0{,}06 \log_2 0{,}06 + 0{,}05 \log_2 0{,}05)$$

$$H = -3{,}32\ [(0{,}48 \log_{10} 0{,}48 + 0{,}21 \log_{10} 0{,}21 + 0{,}12 \log_{10} 0{,}12 + 0{,}08 \log_{10} 0{,}08 + 0{,}06 \log_{10} 0{,}06 + 0{,}05 \log_{10} 0{,}05)]$$

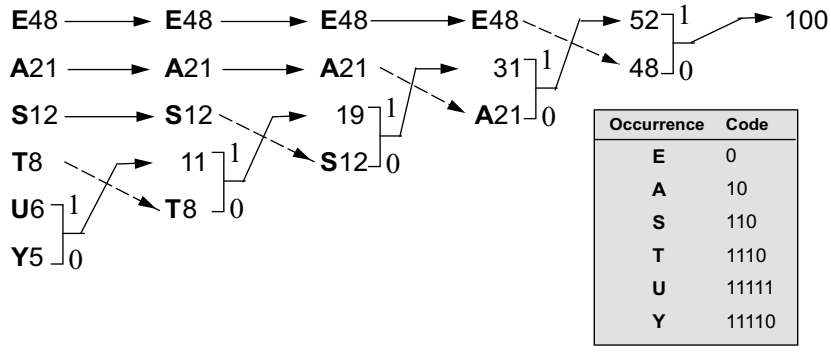
$$H = 2{,}09 \text{ bits}$$

Le codage optimal devrait conduire à construire un code dont la longueur moyenne serait de 2,09 bit, alors que l'utilisation d'un code à longueur fixe nécessite 3 bits pour coder les six états de ce système ($2^2 < 6 \leqslant 2^3$).

Il n'existe pas de code qui permette d'atteindre cette limite théorique. Cependant, Huffman introduit en 1952 une méthode de codage (codage d'entropie) qui prend en compte la fréquence d'occurrence des états et qui se rapproche de cette limite théorique.

À partir du tableau précédent, construisons le code de Huffman correspondant (figure 1.8) :

1. Dénombrez les différents états du système et créez la table des symboles.
2. Classez ces symboles par ordre des fréquences décroissantes (occurrence).
3. Réalisez des réductions successives en rassemblant les deux occurrences de plus petite fréquence en une nouvelle occurrence.
4. Insérez la nouvelle occurrence obtenue dans la table et trier celle-ci à nouveau par ordre décroissant.
5. Poursuivez les réductions jusqu'à ce qu'il n'y ait plus d'élément (répétition des étapes 3, 4, 5).
6. Construisez l'arbre binaire en reliant chaque occurrence à la racine.
7. Établissez le code en lisant l'arbre construit du sommet aux feuilles et en attribuant par exemple la valeur 0 aux branches basses et 1 aux branches hautes.



Occurrence	Code
E	0
A	10
S	110
T	1110
U	11111
Y	11110

Figure 1.8 L'arbre d'Huffman.

La longueur moyenne (Lmoy) du code est de :

$$\text{Lmoy} = 0{,}48 \cdot 1 + 0{,}21 \cdot 2 + 0{,}12 \cdot 3 + 0{,}08 \cdot 4 + 0{,}06 \cdot 5 + 0{,}05 \cdot 5 = 2{,}13$$

© Dunod – La photocopie non autorisée est un délit

Dans cet exemple, on peut remarquer qu'aucun des mots codes obtenus ne peut être confondu avec le début d'un autre. Le codage est dit préfixé. Le codage de Huffman permet de réduire le nombre de bits utilisés pour coder l'information. Dépendant du contexte, il impose, avant la transmission, d'établir une convention (Huffman modifié, utilisé en télécopie groupe 3) ou de transmettre, avant les données, le contenu de la table construite par l'émetteur sur un échantillon ou sur la totalité des données à transférer.

Du code ASCII à l'Unicode

Le codage ASCII (7 bits) ou ISO-646 ne permet de coder que 128 symboles ; il ne réserve que sept valeurs pour prendre en compte les particularités nationales. L'internationalisation des communications, notamment avec Internet, a mis au premier plan les problèmes de codage des textes et a révélé les insuffisances du codage ASCII.

Une première extension a été réalisée par la norme ISO-8859-*x* (8 bits). ISO-8859-*x* utilise les 128 premiers caractères du code ASCII (32 codes de commandes et 96 codes de caractères), le symbole *x* renvoie vers des tables qui complètent le jeu originel autorisant ainsi les écritures à base de caractères latins, cyrilliques, arabes, grecs et hébraïques. Le codage ISO-8859-*x* doit être préféré, sur Internet, à tout autre code chaque fois que cela est possible.

Le décodage d'un texte nécessite que le destinataire connaisse et identifie le code utilisé. Ceci a conduit à définir un code unique sur 16 ou 32 bits permettant la représentation de pratiquement toutes les langues écrites du monde : l'Unicode (16 bits) qui reprend les spécifications du code ISO 10646 UCS-2 (*Universal Character Set*).

1.2.3 La numérisation des informations

Principe

Numériser une grandeur analogique consiste à transformer la suite continue de valeurs de la grandeur analogique en une suite de valeurs discrètes finies. À cet effet, on prélève, à des instants significatifs, un échantillon du signal et on exprime son amplitude par rapport à une échelle finie (quantification).

À partir des valeurs transmises, le récepteur reconstitue le signal d'origine. Une restitution fidèle du signal nécessite que soient définis :

- un intervalle d'échantillonnage qui doit être une constante du système (fréquence d'échantillonnage) ;
- une amplitude de l'échelle de quantification, celle-ci doit être suffisante pour reproduire la dynamique du signal (différence d'amplitude entre la valeur la plus faible et la valeur la plus forte) ;
- des mécanismes pour garantir que le système de transmission respecte les intervalles temporels entre chaque échantillon.

La figure 1.9 représente les différentes étapes de la numérisation du signal. À intervalle régulier (période d'échantillonnage), on prélève une fraction du signal (échantillon). Puis, on fait correspondre à l'amplitude de chaque échantillon une valeur discrète (quantification dite **quantification scalaire**) ; cette valeur est ensuite transformée en valeur binaire (codification).

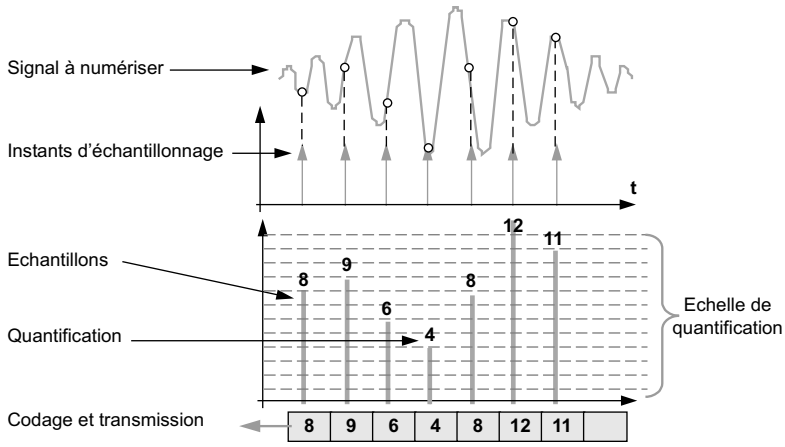


Figure 1.9 La numérisation d'un signal analogique.

Alors que le phénomène à quantifier varie de façon continue, la quantification définit des valeurs en escalier dites « **pas de quantification** ». Aussi, quel que soit le nombre de niveaux utilisés, une approximation est nécessaire ; celle-ci introduit une erreur dite erreur de quantification ou bruit de quantification correspondant à la différence entre la valeur réelle de l'échantillon et la valeur quantifiée[5].

Pour reproduire correctement le signal à l'arrivée, le récepteur doit disposer d'un minimum d'échantillons. Il existe donc une relation étroite entre la fréquence maximale des variations du signal à discrétiser et le nombre d'échantillons à prélever.

Soit un signal dont le spectre (largeur de bande) est limité et dont la borne supérieure vaut $F_{\max}$, Shannon a montré que si F_e est la fréquence d'échantillonnage, le spectre du signal échantillonné est le double de $F_{\max}$ et est centré autour de F_e, $2F_e$... nF_e. Par conséquent, pour éviter tout recouvrement de spectre (interférence), le signal à échantillonner doit être borné (filtré) à une fréquence supérieure telle que $F_{\max}$ soit inférieure à la moitié de l'intervalle d'écartement des spectres (F_e). La figure 1.10 illustre cette relation appelée **relation de Shannon**.

On en déduit que la fréquence minimale d'échantillonnage (fréquence de Nyquist) d'un signal doit être le double de la fréquence maximale du signal à échantillonner. Pour répondre à cette

5. La qualité du signal restitué peut être appréciée par la mesure de l'erreur quadratique moyenne (EQM) dont la valeur est :

$$EQM = \frac{1}{n}\sum_{i=1}^{n}\Delta_i^2$$

Avec n nombre d'échantillons et Δ l'erreur sur l'échantillon i.
On utilise aussi une valeur dérivée, le PSNR (*Peak Signal Noise Ratio*) ou rapport signal sur bruit de crête :

$$PSNR = 10\log_{10}\frac{N-1}{EQM}$$

où N est le nombre de niveaux de quantification.
On estime que la restitution est correcte lorsque le PSNR > 30 dB.

© Dunod – La photocopie non autorisée est un délit

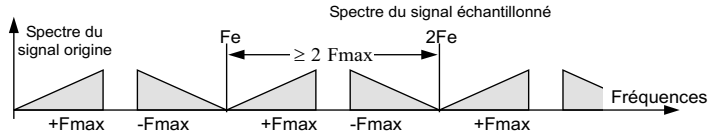


Figure 1.10 Le spectre d'échantillonnage.

contrainte, la numérisation du signal sera toujours précédée d'une calibration du spectre de fréquences. Cette opération est réalisée par un filtre qui élimine les fréquences hautes (figure 1.11).

$$F_{\text{échantillon}} \geqslant 2 \cdot F_{\text{max du signal}}$$

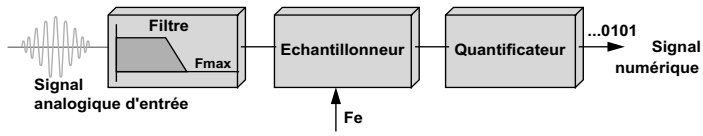


Figure 1.11 La structure élémentaire d'un convertisseur analogique/numérique.

Une reproduction correcte nécessite aussi que le système de transmission respecte les intervalles temporels entre chaque échantillon. Si le temps de transfert ou temps de latence varie dans le réseau, le signal restitué n'est plus conforme au signal d'origine (figure 1.12).

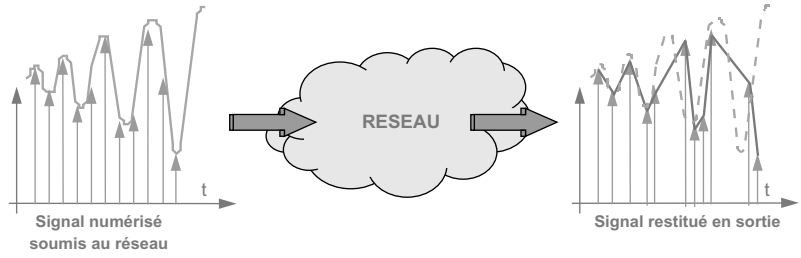


Figure 1.12 Influence de la gigue sur la restitution du signal.

Les flux de données qui nécessitent une récurrence temporelle stricte (gigue nulle) sont dits isochrones et également, par abus de langage, flux ou données temps réel.

Application à la voix

Un canal téléphonique utilise une plage de fréquence ou largeur de bande s'étendant de 300 Hz à 3 400 Hz. Si, pour garantir un espace suffisant entre les différents sous-ensembles du spectre (figure 1.10), on prend 4 000 Hz comme fréquence de coupure du filtre d'entrée, la fréquence d'échantillonnage minimale est de :

$$F_e \geqslant 2 \cdot F_{\max} = 2 \cdot 4\,000 = 8\,000 \text{ Hz}$$

Soit 8 000 échantillons par seconde, ce qui correspond à prélever un échantillon toutes les 125 μs (1/8 000). Pour une restitution correcte (dynamique[6] et rapport signal sur bruit), la voix devrait être quantifiée sur 12 bits (4 096 niveaux). Des contraintes de transmission en rapport avec le débit conduisent à réduire cette bande. L'utilisation d'une loi de quantification logarithmique permet de ramener la représentation numérique de la voix à 8 bits (7 bits pour l'amplitude et un bit de signe), tout en conservant une qualité de reproduction similaire à celle obtenue avec une quantification linéaire sur 12 bits. Cette opération dite de compression est différente en Europe (loi A) et en Amérique du Nord (loi μ). En codant chaque échantillon sur 8 bits, il est nécessaire d'écouler :

$$8\,000 \cdot 8 = 64\,000 \text{ bits par seconde sur le lien,}$$

Ce qui correspond à un débit de 64 000 bit/s. Le transport de la voix ayant été le premier transfert d'information réalisé, c'est naturellement lors de la numérisation des réseaux que le débit de 64 kbit/s est devenu le débit unitaire de référence. Les débits offerts par les réseaux numériques vont de 64 kbit/s à un multiple entier de 64 kbit/s.

Application à l'image vidéo

La voix est un phénomène vibratoire, l'oreille perçoit et interprète les variations de pression successives. L'image est analysée globalement par l'œil alors qu'elle ne peut être transmise et reproduite que séquentiellement. La discrétisation de l'image nécessite deux étapes : d'abord une transformation espace/temps qui se concrétise par une analyse de celle-ci, ligne par ligne, puis une décomposition de chaque ligne en points (pixel), enfin, la quantification de la valeur lumineuse du point, valeur qui est transmise.

➤ L'image monochrome

La reproduction d'une image nécessite l'analyse et la quantification de l'intensité lumineuse, ou luminance, de chacun des points constituant l'image (échantillon). La figure 1.13 schématise l'analyse de l'image et présente le signal électrique analogique résultant dit « signal de luminance » et noté Y(t).

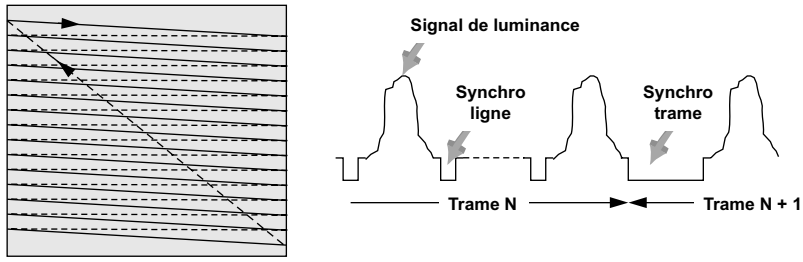


Figure 1.13 Le principe de l'analyse d'image.

L'image est analysée de gauche à droite ligne par ligne (balayage horizontal) et de haut en bas (balayage vertical). Pour garantir le synchronisme entre le système d'analyse de l'émetteur et le système de reproduction du récepteur, une impulsion de synchronisation (synchronisation

6. La dynamique exprime le rapport entre les puissances maximale et minimale du signal.

© Dunod – La photocopie non autorisée est un délit

ligne) est insérée entre deux lignes successives. À l'instar de la synchronisation ligne, un signal (synchronisation verticale ou trame) réinitialise le positionnement du système de balayage pour l'analyse d'une nouvelle image. Les commandes de déplacement, horizontal et vertical, s'exécutent simultanément, de ce fait les lignes sont légèrement inclinées. L'ensemble des lignes constituant une image constitue une trame. Lorsque l'analyse des lignes est réalisée de façon continue l'image est dite progressive. Les paramètres de base d'un système de télévision sont donc :

– le format de l'image ;
– le nombre de lignes analysées par seconde, généralement appelée définition verticale de l'image ;
– le nombre d'images analysées par seconde.

À l'origine, l'image de télévision a adopté le même format que l'image du cinéma, ce format s'exprimant par le rapport entre la largeur de l'image et sa hauteur (image 4:3 ou 1,33). Plus le nombre de lignes d'analyse est important, plus l'image restituée est fidèle. Cependant, l'augmentation du nombre de lignes accroît la bande passante (débit) nécessaire à la transmission de l'image. Le nombre de lignes est donc un compromis entre la qualité de l'image et les contraintes de transmission. Le nombre de lignes a été défini pour qu'à distance normale de l'écran deux lignes successives soient vues sous un angle inférieur à 1 minute d'angle[7]. Actuellement, ce nombre est de 625 lignes en Europe (576 lignes utiles ou visibles) et de 525 lignes en Amérique du Nord et au Japon (480 lignes visibles).

La persistance rétinienne moyenne est d'environ 0,1 seconde. Dans ces conditions, si le temps entre l'illumination du premier point en haut à gauche et celle du dernier point en bas à droite est inférieure à 0,1 seconde, l'œil verra une image et non pas un point. En conséquence, le nombre d'images doit être d'au moins 10 images/s. Cependant, l'impression de mouvement fluide n'est obtenue qu'à partir de 16 images/secondes (cinéma muet). Pour avoir une reproduction du son correcte, le cinéma sonore a nécessité d'augmenter le nombre d'images et de le porter à 24 images/seconde (longueur physique du film pour l'empreinte sonore). Pour tenir compte d'éventuels phénomènes stroboscopiques entre l'affichage de l'image et la tension dite de ronflement des alimentations, en télévision, ce nombre a été fixé à 25 images/seconde en Europe et 30 images/seconde en Amérique. En télévision, compte tenu du système spécifique de reproduction continue d'un point et non de l'affichage d'une image complète comme le cinéma, une reproduction à 25 images/seconde provoque un effet de papillotement de l'image. Afin d'augmenter le nombre d'images affichées sans augmenter la bande passante, l'image est analysée et reproduite en deux trames successives. En Europe, la fréquence image est donc de 25 images/seconde et la fréquence trames de 50 Hz (50 $\frac{1}{2}$ images par seconde), la première trame analyse les lignes impaires, la seconde les lignes paires. Ce système est dit à **trames entrelacées** (figure 1.14).

➤ L'image colorée

Une image colorée peut être analysée selon trois couleurs dites **primaires** de longueur d'onde (λ) déterminée. Pour reconstituer l'image d'origine, il suffit de superposer les trois images, c'est la synthèse additive. La figure 1.15 représente le principe de la synthèse additive. Le dosage de chacune des sources lumineuses permet de reproduire toutes les couleurs.

7. Une personne dotée d'une vision de dix dixièmes ne perçoit deux objets distincts que si l'écart qui les sépare est vu sous un angle d'au moins une minute d'angle.

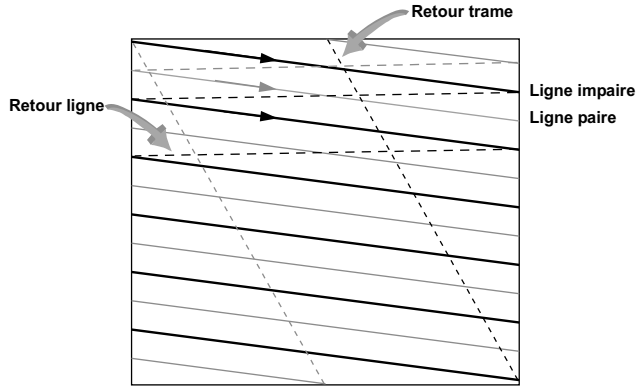


Figure 1.14 Le principe de l'analyse entrelacée.

Chaque point de l'image est représenté par deux grandeurs, la **luminance** et la **chrominance**. Ces grandeurs sont reliées entre elles par la relation :

$$Y = 0{,}3\ R + 0{,}59\ V + 0{,}11\ B$$

où Y est la luminance (échelle des gris),
R l'intensité de la composante de lumière rouge,
V celle de la composante de lumière verte,
B celle de la composante de lumière bleue.

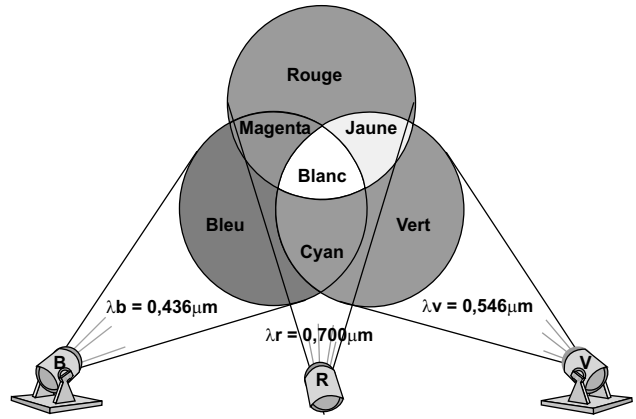


Figure 1.15 La synthèse additive.

L'image est dite **RVB** ou **RGB** (*Red, Green, Blue*), du nom des trois couleurs primaires rouge, vert, bleu. En télévision, pour assurer la compatibilité avec les téléviseurs monochromes, il faut transmettre non seulement les informations de chrominance mais aussi celles de luminance (**échelle des gris**).

Par conséquent, l'information de luminance (Y) est transmise sans modification. Compte tenu qu'il existe une relation mathématique entre la luminance et les trois fondamentales, seules les

© Dunod – La photocopie non autorisée est un délit

informations de couleur rouge (R) et bleue (B) sont transmises ; l'information de couleur verte[8] (V) sera calculée par le récepteur :

$$Y = 0{,}3\ R + 0{,}59\ V + 0{,}11\ B$$

d'où

$$V = [Y - (0{,}3\ R + 0{,}11\ B)] / 0{,}59$$

Les travaux de Bedford (mires de Bedford) ont mis en évidence que l'œil ne percevait pas la couleur dans les détails. Dès lors, on peut se contenter d'une définition moindre pour l'information couleur que pour l'information monochrome (noir et blanc). Plusieurs schémas de réduction de la bande chrominance ont été adoptés, ceux-ci sont illustrés par la figure 1.16.

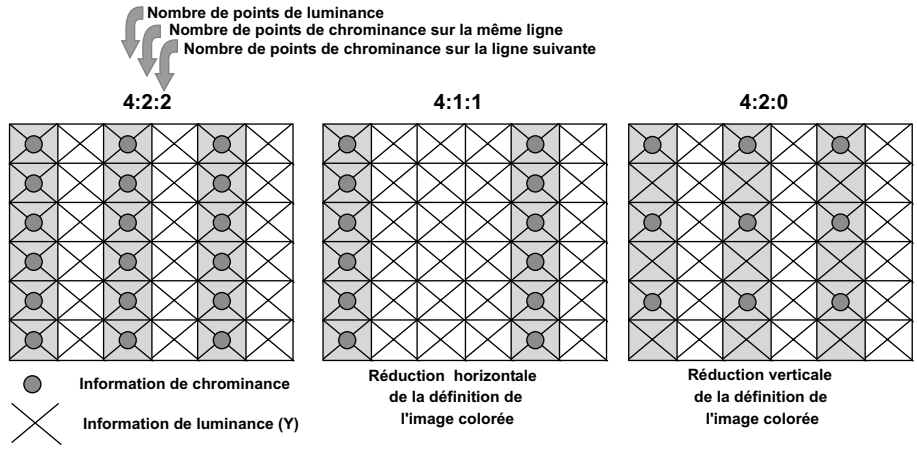


Figure 1.16 Le format de réduction de bande.

Le format de base adoptée pour la télévision est le 4:2:2 (quatre échantillons de luminance pour deux échantillons de chrominance horizontal et vertical). Le format 4:1:1 est plus réducteur puisque la définition horizontale n'est que le quart de la définition verticale. Enfin, dans le format dit 4:2:0, à l'instar du format 4:2:2 la définition horizontale de la chrominance est réduite de moitié, mais aussi celle de chrominance verticale, puisque l'information de chrominance de la ligne N et réutilisée pour la ligne N+1 (une seule ligne d'analyse de chrominance pour deux lignes reproduites).

Application à la télévision numérique

Le standard d'une image de télévision numérique au format européen (625 lignes, 25 Hz) est caractérisé par :

– le nombre de lignes utiles (visibles) par image fixé à 576 ;

8. On ne transmet pas directement les informations de chrominance, mais les signaux dits de différence de couleur $Dr = R–Y$, $Db = B–Y$, $Dv = V–Y$. Dans ces conditions, l'amplitude du signal V étant la plus importante, la valeur Dv est la plus faible, donc la plus sensible aux bruits de transmission. C'est cette analyse qui a conduit au choix de Dr et Db comme signaux à transmettre. Ce format est souvent désigné sous le terme de format YUV ou YCbCr.

– le nombre de points par ligne défini à 720[9] ;
– le nombre d'images par seconde déterminé à 25 images (25 Hz).

Ainsi, on transmet :

– 720 points par ligne pour le signal Y ;
– 360 points pour chacune des couleurs B et R.

Au total 1 440 échantillons élémentaires par ligne sont analysés. En se satisfaisant d'une quantification sur 255 niveaux (8 bits, soit 16 millions de couleurs, plus que l'œil n'est capable d'en discerner), le nombre de bits nécessaires à la reconstitution d'une image (576 lignes) est donc de :

$$N(\text{bits}) = 1\,440 \cdot 8 \cdot 576 = 6\,635\,520 \text{ bits}$$

À raison de 25 images par seconde (50 demi-images), il faut, pour transmettre une image animée, un débit minimal de :

$$D_{\min} = 6\,635\,520 \cdot 25 = 166 \text{ Mbit/s.}$$

Ce débit, relativement important, a conduit à rechercher des méthodes de codage particulières. Un groupe de travail commun à l'ISO et à la CEI (Commission électrotechnique internationale), le *Motion Picture Expert Group* (**MPEG**), est chargé de définir les algorithmes normalisés de compression d'images vidéo et du son associé.

➤ Le codage de l'information de couleur

Les différents procédés de télévision couleur diffèrent essentiellement par le codage adopté pour transmettre les informations de couleur. Le premier système public de télévision a été mis au point aux États-Unis par le *National Television Comitee* d'où son nom de **NTSC** (*National Television System Comitee*)

Dans le système NTSC, les informations de couleur modulent en amplitude deux sous-porteuses en quadrature. Le signal réellement émis est donc un vecteur dit vecteur de chrominance (Uc) (figure 1.17).

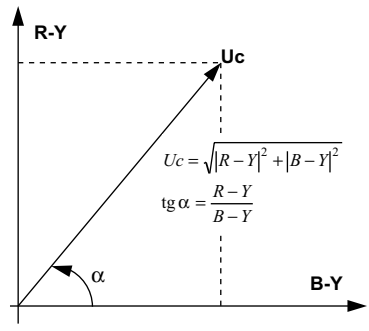


Figure 1.17 Le codage de l'information de chrominance dans le système NTSC.

9. À titre de comparaison : le magnétoscope VHS (*Video Home System*) 250 points/ligne ; le magnétoscope SVHS 400 points/ligne.

© Dunod – La photocopie non autorisée est un délit

Ce signal correspond à une modulation d'amplitude et à une modulation de phase. Toute altération de la phase du signal durant la transmission altère les nuances de couleur. C'est le principal défaut du système NTSC.

Le système **PAL** (*Phase Alternance Line*), d'origine allemande utilise le même procédé que le système NTSC, mais en corrige le principal défaut en alternant à chaque ligne la phase des signaux de chrominance. De ce fait, les erreurs de couleur dues à l'erreur de phase sur une ligne sont compensées par une erreur de couleur inverse sur la ligne suivante.

Le système de télévision couleur français, dû à Henri de France, procède différemment. Les signaux de couleur sont émis successivement. Ainsi, par exemple, la ligne N correspond à l'émission des signaux Dr, et la ligne $N + 1$ à celle des signaux Db. Les signaux Dr et Db étant nécessaires simultanément pour reconstituer le signal Dv, lors de la réception de la ligne N, le signal est mis en mémoire durant l'intervalle de temps d'une ligne, puis lors de la réception de la ligne suivante le signal Dv est reconstitué à partir du signal reçu et du signal mémorisé précédemment et ainsi de suite. Le procédé est séquentiel, il nécessite la mise en mémoire de l'information ligne d'où le nom de **SECAM** pour *SEquentiel Couleur A Mémoire*. La figure 1.18 résume les caractéristiques des différents standards de télévision.

Standard CCIR 601	Définition analogique	Définition luminance	Définition chrominance	Format couleur	Entrelacé	Trames/s
NTSC	525/60	720x480	360x480	4:2:2	Oui	59,94[a]
PAL	625/50	720x576	360x576	4:2:2	Oui	50
SECAM	625/50	720x576	720x288	4:2:2	Oui	50

a. À l'origine, la fréquence trame du système de télévision américain était de 60 Hz. Lors de la définition d'un système couleur, cette fréquence a été légèrement modifiée pour tenir compte de la fréquence de la sous-porteuse chrominance.

Figure 1.18 Synthèse des standards de télévision couleur.

Application à la vidéoconférence

La vidéoconférence permet à un groupe de personnes d'entrer en communication. Selon le type de moniteur vidéo utilisé, on distingue la visioconférence (écran d'ordinateur), la vidéoconférence (moniteur dédié) ou la téléconférence (téléviseur). Le système assure la transmission de l'image (vidéo) et du son. Les principaux standards sont :

– H.320 ou p*64 qui utilise le réseau téléphonique numérique en associant p canaux téléphoniques, avec $1 \leqslant p \leqslant 30$. Le codage de la vidéo y est défini selon les recommandations de l'avis H.261 et H.263 (plus efficace).
– H.323, pour la diffusion de flux multimédia sur des réseaux de transmission de données sans qualité de service comme Internet.

Ces standards définissent la pile protocolaire et les modes de codage de l'image et du son. Le codage vidéo est celui défini par le CCIR 4:2:2 YUV non entrelacé (progressif). Ce codage est un compromis entre les formats de télévision NTSC et PAL. Pour s'adapter au débit du réseau, plusieurs formats dérivés de deux formats de base ont été définis :

– **CIF** (*Common Intermediate Format*).
– **QCIF** (Quart-CIF).

De même, en début de communication, le nombre d'images par seconde est négocié entre les différents agents. La fréquence image est un sous-multiple de 30 : 30 Hz, 15 Hz, 10 Hz et 7,5 Hz. La figure 1.19 fournit les relations entre les formats d'image et leurs implémentations dans les normes de vidéoconférence.

	sub-QCIF	QCIF	CIF	4CIF	16CIF
Format image	128x96	176x144	352x288	704x576	1408x1152
H.261	Optionnel	Obligatoire	Optionnel	Non prévu	Non prévu
H.263	Obligatoire	Obligatoire	Optionnel	Optionnel	Optionnel

Figure 1.19 Synthèse des caractéristiques CIF et QCIF.

Les informations vidéos représentent un volume de données important à transférer. Ainsi hors la définition des formats d'image que nous venons d'étudier, les différents systèmes mettent en œuvre des techniques de compression.

1.3 LA COMPRESSION DE DONNÉES

1.3.1 Généralités

Si on néglige le temps de propagation du message sur le support, le temps de transmission ou temps de transfert d'un message a pour expression :

$$T_t = \text{Longueur du message en bits / débit de la liaison}$$

Pour un même contenu sémantique, ce temps sera d'autant plus faible que la longueur du message sera petite ou que le débit sera élevé. L'augmentation du débit se heurte à des problèmes technologiques et de coûts. Il peut donc être intéressant de réduire la longueur du message sans en altérer le contenu (la sémantique) : c'est la compression de données.

Les techniques de compression se répartissent en deux familles : les algorithmes réversibles ou sans perte, dits aussi sans bruit, et les algorithmes irréversibles, dits avec perte. Les premiers restituent à l'identique les données originelles. Ils s'appliquent aux données informatiques. Le taux de compression obtenu est voisin de 2. Les seconds, dits aussi codes à réduction de bande, autorisent des taux de compression pouvant atteindre plusieurs centaines au détriment de la fidélité de restitution. Utilisés pour la voix, l'image et la vidéo, ils s'apparentent plus à des procédés de codage qu'à des techniques de compression.

1.3.2 La quantification de la compression

La compression se quantifie selon trois grandeurs[10] : le quotient de compression, le taux de compression et le gain de compression.

10. En toute rigueur, les grandeurs définies ci-après ne sont valables que pour les algorithmes de compression sans perte. En effet, pour les algorithmes avec perte, il y a réduction d'information et non compression. Cependant, l'usage étend ces quantifications aux deux types de compression.

© Dunod – La photocopie non autorisée est un délit

Le quotient de compression (Q) exprime le rapport entre la taille des données non compressées à la taille des données compressées.

$$Q = \frac{\text{Taille avant compression}}{\text{Taille après compression}}$$

Le taux de compression (T) est l'inverse du quotient de compression.

$$T = 1/Q$$

Enfin, le gain de compression, exprime en % la réduction de la taille des données.

$$G = (1 - T) \times 100$$

1.3.3 La compression sans perte

Compression d'un ensemble fini de symboles équiprobables

Quand le nombre de symboles appartient à un ensemble fini, par exemple un catalogue de produits, on peut substituer au symbole un code (référence du produit, code d'erreur...). Cette technique qui appartient à l'organisation des données ne sera pas étudiée ici.

Compression de symboles non équiprobables

De nombreuses techniques permettent de réduire la taille de données quelconques. Les trois principales sont :

- Le **codage en longueur de plage** comme le *Run Length Encoding* (**RLE**) qui consiste à remplacer une suite de caractères identiques par le nombre d'occurrences de ce caractère. On obtient des séquences du type : échappement/nombre/caractère, par exemple la séquence @10A peut signifier, 10 A consécutifs. Ce codage, peu efficace, pour le texte est utilisé pour compresser les images et les fichiers binaires, notamment par MacPaint (Apple). Ce codage n'est efficace que lorsqu'une séquence de caractères comporte plus de deux caractères consécutifs différents. Aussi, si le nombre de caractères similaires consécutifs est inférieur à trois, la suite de caractères différents est identifiée (caractère de contrôle) et ne fait l'objet d'aucune compression.
- Le **codage par substitution** remplace une séquence de caractères prédéfinie par un code. Le dictionnaire nécessaire au codage et au décodage est construit dynamiquement. Non transmis, il est reconstitué en réception. Connu sous le nom de Lempel-Ziv-Welch (**LZW**), il est utilisé dans les utilitaires de compression PKZIP, ARJ et dans les modems (V.42bis).
- Le **codage d'entropie** ou codage statistique attribue un mot code d'autant plus petit que la probabilité d'apparition du symbole à coder dans le fichier est grande (exemple : le codage d'Huffman). Nécessitant une lecture préalable du fichier et l'envoi du dictionnaire de codage, le code de Huffman est peu efficace. Utilisé en télécopie G3, le code de Huffman modifié (HM) associe, à partir d'un dictionnaire préconstitué, un mot binaire à une séquence de points.

1.3.4 Les codages à réduction de bande

Le codage à réduction de bande concerne le codage de la voix et de l'image. Il met à profit les imperfections des organes d'interprétation humains pour réduire la quantité d'information transmise tout

en garantissant une reproduction correcte pour l'utilisateur final. Plus la réduction de bande sera élevée, plus la restitution sera dégradée. L'objectif des procédés de codage consiste donc en un compromis entre la réduction de bande passante nécessaire à la transmission et la qualité de restitution. La réduction de bande envisageable ne dépend pas de la source, mais des imperfections du système d'interprétation. L'homme étant plus sensible aux altérations du son qu'à celles de l'image, les méthodes de codification de l'image autoriseront des réductions de bande plus importantes que celles adoptées pour le son.

Le codage de la voix

Les procédés de codage et de compression de la voix déclinent trois techniques :

- Le codage **MIC** (Modulation par Impulsion et Codage ou **PCM**, *Pulse Code Modulation*) qui utilise une quantification logarithmique.
- Les codages différentiels, codant non plus l'échantillon mais son écart par rapport à l'échantillon précédent comme l'**ADPCM**[11] (*Adaptative Differential Pulse Code Modulation*).
- Des techniques plus élaborées reconstituent la voix par synthèse (**CELP**, *Code Excited Linear Prediction*).

➤ Le codage MIC ou PCM

La numérisation de la voix selon le procédé **MIC** (Modulation par impulsion et codage ou **PCM**, *Pulse Code Modulation*) est adoptée dans tous les réseaux téléphoniques. Cependant, une reproduction correcte de la voix (dynamique et rapport signal sur bruit) nécessite au minimum une quantification sur 12 bits (voir dans le § 1.2.3, *Application à la voix*). Cette quantification dite linéaire introduit un rapport signal sur bruit d'autant plus défavorable que la valeur du signal est faible (figure 1.20). Maintenir un rapport signal sur bruit acceptable quels que soient le niveau de quantification et la nécessité de réduire la bande ont conduit à adopter des lois de quantification non linéaires. Ces lois attribuent pour une même variation d'amplitude du signal un nombre de niveaux de quantification plus important aux faibles valeurs du signal qu'aux fortes (quantification logarithmique).

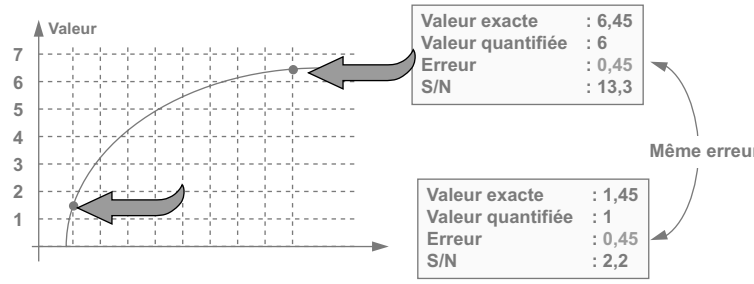


Figure 1.20 Amplitude du signal de voix et rapport signal sur bruit.

11. L'ADPCM64 autorise une bande de 7 kHz pour un débit de 64 kbit/s ; il peut être mis en œuvre dans la téléphonie numérique sur RNIS (Réseau numérique à intégration de service).

© Dunod – La photocopie non autorisée est un délit

Deux lois de quantification non linéaires sont utilisées :

– La loi μ utilisée en Amérique du Nord, Japon et Australie quantifie les échantillons sur un espace linéaire de 14 bits, réduit à 8 bits.
– La loi A mise en œuvre dans le reste du monde correspond à une quantification linéaire sur 12 bits et à une réduction à 8 bits.

Ces lois autorisent un codage sur 8 bits avec un rapport signal sur bruit de 33 dB. La figure 1.21 représente la partie positive de la loi A. Celle-ci divise l'espace de quantification en huit intervalles. Chaque intervalle de quantification (sauf les deux premiers) est le double du précédent. À l'intérieur de chaque intervalle, on opère une quantification linéaire sur 16 niveaux. Un échantillon est représenté par 8 bits (figure 1.21) :

– le premier indique la polarité du signal (P) ;
– les trois suivants identifient le segment de quantification (S) ;
– enfin, les quatre derniers représentent la valeur dans le segment (V).

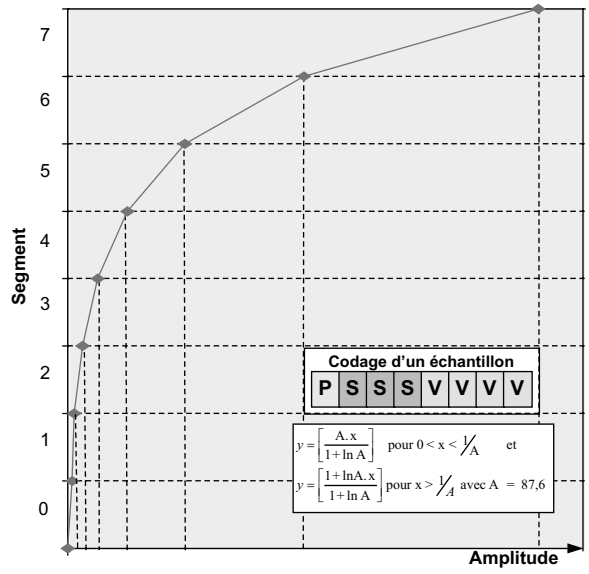


Figure 1.21 La loi de codage A.

➤ Le codage différentiel

Le MIC différentiel appelé aussi codage *Delta Modulation* (**DM**) ne code pas la valeur de l'échantillon, mais sa différence par rapport au précédent. La figure 1.22 schématise le principe d'un codeur différentiel à quantification linéaire constante.

Le signal quantifié (i) est la différence entre le signal d'entrée (x) et une valeur prédite. En effet, les différents échantillons étant fortement corrélés, il est possible à partir de la variation des échantillons précédents ($n - 1$, $n - 2$...) de prédire la valeur de l'échantillon n. Dans le principe de base de la figure 1.22, la prédiction n'est que de 1, la référence est le seul échantillon précédent.

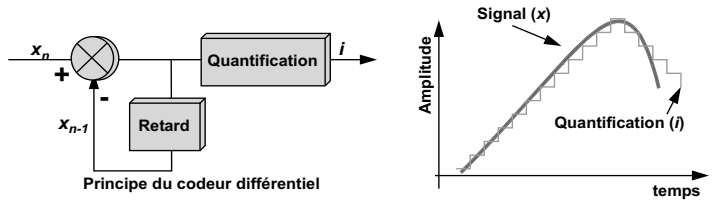


Figure 1.22 Principe du codage différentiel.

Si cette technique permet de réduire la bande nécessaire, on note figure 1.22 que lorsque le pas de quantification est fixe, le système ne peut suivre les variations rapides du signal. **ADPCM** (*Adaptative Differential Pulse Code Modulation*) ou **MICDA** (Modulation par impulsion et codage différentiel et adaptatif) utilise une technique de quantification à pas variable proportionnel à la variance du signal. Cette quantification est estimée, non pas sur la différence de valeur entre l'échantillon précédent et l'échantillon courant, mais sur l'écart entre la valeur réelle de l'échantillon et celle résultant de la prédiction de cette valeur par rapport à la variation de *n* échantillons précédents. La figure 1.23 illustre ce principe.

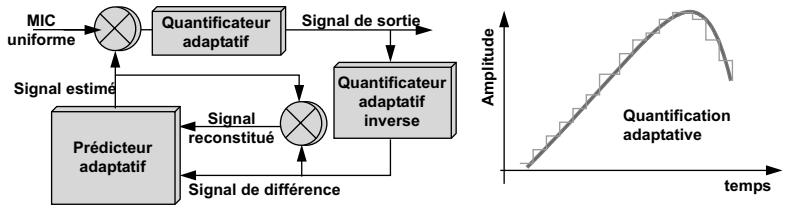


Figure 1.23 Principe du codage ADPCM.

Une variante de l'ADPCM, le SB-MICDA (Sous-bande - MICDA) permet d'augmenter la bande passante du signal à numériser sans augmenter le débit d'un canal téléphonique. Le SB-MICDA autorise une bande passante de 50 à 7 000 Hz. Cette bande est séparée en deux sous-bandes 50 à 4 000 Hz et 4 000 à 7 000 Hz. La bande inférieure, la plus riche en composante est quantifiée sur 4, 5 ou 6 bits et la bande supérieure sur 2 bits.

➤ Les codages par synthèse

Ce n'est pas le signal compressé qui est transmis mais la valeur des coefficients qui permettront au décodeur, à partir d'un dictionnaire de sons, de reconstituer la voix par synthèse vocale. À l'instar d'un instrument de musique à vent, le système vocal humain peut être assimilé à un ensemble de tubes, évidemment plus complexe, excités par une onde sonore. Le principe de base des algorithmes à excitation (**CELP**, *Code Excited Linear Prediction*) consiste à transmettre les paramètres mathématiques qui permettront au récepteur de modéliser le système vocal de celui qui parle et un index qui pointe dans un dictionnaire de séquences de voix préétablies appelées vecteurs. Ce dictionnaire est commun à l'émetteur et au récepteur.

Le dictionnaire comporte un ensemble de vecteurs qui modélise le signal de parole. Le mécanisme consiste en une recherche en boucle fermée le vecteur contenu dans le dictionnaire le plus proche du vecteur courant, le vecteur courant étant prédit à partir de *n* échantillons précédents. La figure 1.24 illustre le principe, très simplifié, d'un codeur CELP.

© Dunod – La photocopie non autorisée est un délit

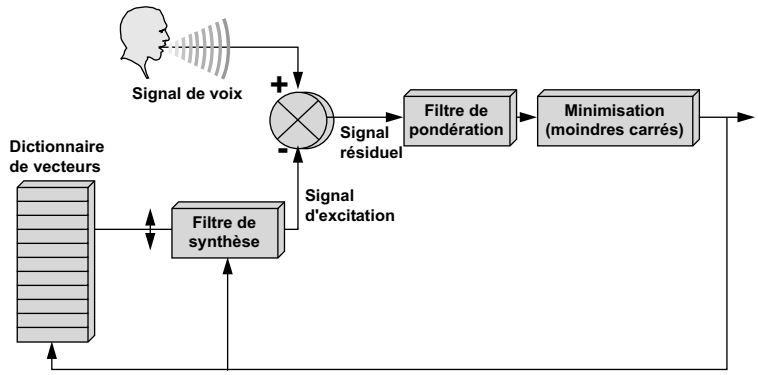


Figure 1.24 Principe d'un codeur CELP.

Le CELP nécessite une puissance de calcul importante de l'ordre de 10 MIPS et introduit un délai important, de l'ordre de 50 à 100 ms. Le CELP modélise la voix, il n'est donc pas adapté aux autres transferts (fax, modem, signaux de numérotation DTMF[12]...).

La première variante, **LD-CELP** (*Low Delay - CELP*) a pour principal objectif de minimiser le délai, celui-ci n'est plus que de 2 ms. Le débit obtenu est de 16 kbit/s. Le **CS-ACELP** (*Conjugate Structure - Algebric CELP*) conçu à l'origine pour le transport de la voix en mode paquet (réseau IP, GSM...) opère sur des trames de parole de 10 ms (80 échantillons à 8 000 Hz). La durée de codage est de 15 ms en tenant compte du temps de prétraitement de la trame suivante (*look ahead*).

La figure 1.25 résume les principales normes fondées sur la technique CELP.

Codage	Commentaires
ACELP	*Algebraic Code Excited Linear Prediction* (G.723 à 5,3 kbit/s)
CELP	*Code Excited Linear Prediction*
CS-ACELP	*Conjugate Structure - Algebraic Code Excited Linear Prediction*, utilisé dans le G.729
LC-CELP	*Low Complexity - CELP*
LD-CELP	*Low Delay* - CELP utilisé dans G.728
LPC	*Linear Productive Coding*
MP-MLQ	*Multipulse Maximum Likelihood Quantization* utilisé dans G.723 à 6,4 kbit/s
RPE-LTP	*Regular Pulse Excitation Long-Term Preditor*, utilisé dans le GSM (variante du CELP), utilise une prédiction à long terme.

Figure 1.25 Tableau récapitulatif des principaux modes de codage.

Mesure de la qualité sonore

Les algorithmes de compression sont destructifs. En l'absence d'instrument de mesure pour évaluer la qualité de la restitution sonore celle-ci est directement appréciée par des observateurs humains.

12. **DTMF** (*Dual Tone Multi-Frequency*) est une technique de numérotation de la téléphonie traditionnelle dans laquelle chaque chiffre du clavier est identifié par deux fréquences.

L'appréciation donnée est donc très subjective. La qualité est exprimée en **MOS** (*Mean Opinion Score*) sur une échelle de notes de 1 à 5 :

1 : mauvais, quelques problèmes d'intelligibilité ;
2 : médiocre, dégradation considérable, la voix à une tonalité de voix synthétique ;
3 : passable, dégradation perceptible, mais on reconnaît son interlocuteur ;
4 : bon, dégradation à peine perceptible ;
5 : excellent, pas de déformation perceptible.

La figure 1.26 compare les différents algorithmes de compression en fonction du débit qu'ils autorisent et de la qualité de restitution de la parole. La norme G.711 est utilisée dans la téléphonie fixe traditionnelle. La norme G.729 est mise en œuvre dans la voix sur IP, elle modélise la voix humaine par l'utilisation de filtres.

Codec	Technique	Débit	Délai	MOS	Commentaire
G.711	PCM	64 kbit/s	0,125 ms	4,2	Compression logarithmique. Téléphonie et H.320.
G.721	ADPCM	32 kbit/s	0,125 ms	4,4	Échantillon codé sur 4 bits.
G.722	ADPCM	48, 56, 64 kbit/s	< 3 ms		Spectre sonore de 50 à 7 000 Hz. Utilisation visioconférence (H.320).
G.722-1	ADPCM	16, 24, 32 kbit/s			Version 16 kbit/s supportée par Windows Messenger.
G.723	ACELP	5,3 et 6,4 kbit/s	30 ms	3,9	
G.723-1	ACELP, MP-MLQ		30 ms	3,9	H.323 et H.324M (UMTS).
G.726	ADPCM	16, 24, 32, 40 kbit/s	< 3 ms	4,5 à 2,0	Décomposition du spectre en sous-bande. Remplace G.721.
G.727	ADPCM	16, 24, 32, 40 kbits		3,9	Complète G.726. Changement du nombre de bit (débit) en cours de conversation.
G.728	LD-CELP	16 kbit/s	3 ms	4,1	Trame courte de 2,5 ms
G.729	CS-ACELP	8 kbit/s	15 ms	3,9	Concurrent de G.723.1, recommandé pour voix sur Frame Relay et H.323.
G.729 a	CS-ACELP	8 kbit/s	15 ms	3,7	G.729 + récupération des silences.
GSM	RPE-LTP	13, 13,2 kbit/s	20 ms	3,9	

Figure 1.26 Synthèse des principaux algorithmes de compression du son.

Le codage de l'image[13]

➤ Généralités

Le développement d'applications multimédia, la télévision numérique et la vidéo conférence sont autant d'utilisation de l'image qui nécessitent une forte compression pour mettre le volume de données en adéquation avec les capacités de transfert des réseaux et celles de stockage des calculateurs.

Ceci conduit à rechercher des méthodes de codage autorisant des taux de compression élevés tout en conservant une qualité d'image acceptable. Les méthodes définies prennent en compte

13. Le codage d'images fixes ou animées est extrêmement complexe ; ce paragraphe a pour objet de démystifier ce codage. Pour plus de précision, le lecteur se reportera à des ouvrages spécialisés.

© Dunod – La photocopie non autorisée est un délit

les spécificités de l'information transmise (forte corrélation spatiale et temporelle des séquences vidéo), et mettent à profit les imperfections de la vision pour réduire la quantité d'information à transmettre. Différentes techniques peuvent être mises en œuvre :

- la quantification scalaire qui n'attribue pas la même importance à chaque niveau du signal transmis. En recherchant une répartition optimale des niveaux de quantification, on peut réduire la bande nécessaire ;
- la quantification vectorielle (extension de la méthode précédente) qui opère une quantification sur des blocs (redondance spatiale) ;
- les méthodes prédictives qui tentent, à partir de la valeur des points voisins, de déterminer la valeur du point courant ;
- les méthodes à compensation de mouvements qui ne transmettent au temps t que la différence entre l'image actuelle et l'image précédente $(t - 1)$;
- la croissance rapide des puissances de calcul des machines modernes qui laisse prévoir un avenir aux méthodes mathématiques (fractales, ondelettes).

Le codage d'images fixes a été défini par un groupe d'experts de la photographie le *Joint Photographic Expert Group* (**JPEG**) en 1982. Leurs travaux ont servi de base au *Moving Picture Expert Group* (**MPEG**) pour définir les normes de compression d'images animées (**MPEG-1** novembre 1992, **MPEG-2** mars 1994, **MPEG-4** fin 1998). Ces procédés de codage procèdent des principes précédents et autorisent des images de qualité **VHS** (MPEG-1) et de qualité Télévision (720×480 à 30 images/seconde pour le système NTSC[14] et 720×576 à 25 images/seconde pour le système PAL[15]) pour la norme MPEG-2. MPEG-2[16] dit de qualité *broadcast* est utilisé pour la diffusion d'émissions de télévision numérique avec un débit compris entre 4 et 6 Mbit/s. MPEG-4 est essentiellement destiné à la vidéoconférence, il autorise des débits inférieurs à 64 kbit/s. MPEG-4 sera utilisé dans la TNT haute définition.

➤ Le codage d'images fixes (JPEG)

Le codage JPEG met à profit la forte redondance spatiale de l'image. L'image (figure 1.27) est décomposée en blocs de 8×8 pixels, chaque pixel de ce bloc présentant entre eux une forte corrélation. Une réduction de bande importante est envisageable à condition de préserver un pixel (en haut à gauche) qui servira de référence pour le décodage du bloc.

La figure 1.28 illustre le schéma de codage d'un bloc. Le signal d'entrée est transformé en blocs de 8×8 dans lequel chaque pixel a été quantifié (quantification scalaire). À cette matrice (quantification vectorielle) est appliquée une opération de transformation linéaire (DCT) permettant de réduire l'écart entre les coefficients, voire d'en annuler certains sans que cette opération n'entraîne de distorsion significative de l'image. La transformée en cosinus discrète (**DCT**, *Discret Cosinus Transform*) est une opération mathématique, elle ne correspond nullement à une quelconque compression mais prépare les données à une compression efficace en transformant l'information sur les pixels en une information de variation d'un pixel à l'autre.

14. NTSC (*National Television System Committee*). Premier grand système de télévision couleur (1950) utilisé aux États-Unis et au Japon.

15. PAL (*Phase Alternance Line*) : système de télévision couleur d'origine allemande.

16. Le forum européen **DVB** (*Digital Video Broadcasting*) a défini, sur les bases de MPEG2, les principes de la télévision numérique.

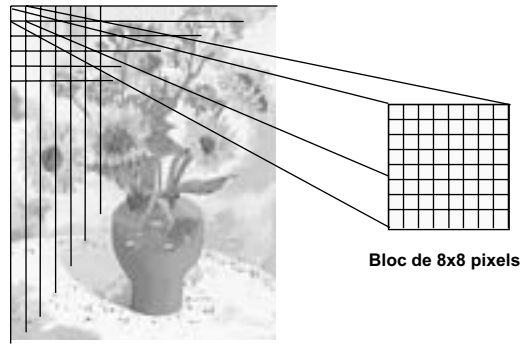


Figure 1.27 La décomposition de l'image en blocs.

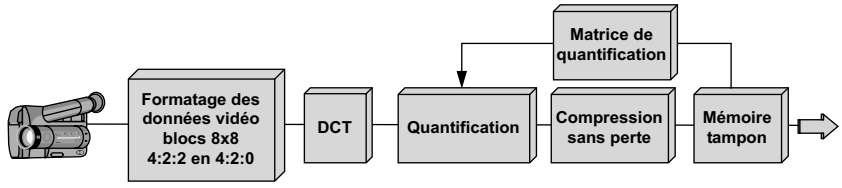


Figure 1.28 Le schéma fonctionnel d'un codage JPEG.

Le signal d'entrée vidéo est mis au format 4:2:0 et l'image est décomposée en blocs de 8×8 pixels. Chaque pixel est alors quantifié sur 8 bits. À chaque bloc est appliqué la fonction DCT, puis les coefficients sont réduits par division de chaque terme par le terme de même indice d'une matrice dite matrice de quantification. Les coefficients ainsi réduits sont lus en zigzag puis subissent une compression sans perte du type longueur de plage (RLE) suivi d'un codage Huffman (figure 1.29). La matrice de quantification peut être prédéterminée (système à débit variable) ou déterminée en fonction d'un débit à atteindre (système à débit fixe).

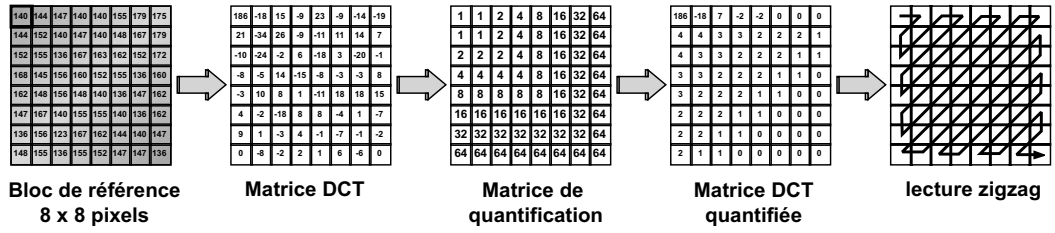


Figure 1.29 L'illustration de la compression spatiale JPEG.

La scrutation en zigzag accroît la probabilité d'obtenir une suite de coefficients identiques et donc un meilleur taux de compression. Le schéma de lecture de la figure 1.29 est adapté à la lecture d'une image progressive ; il est différent pour une image entrelacée.

© Dunod – La photocopie non autorisée est un délit

➤ Le codage d'images animées (MPEG)

Image I ou image de référence

En cinématographie, le mouvement est restitué par la projection d'images successives. Compte tenu du volume de données, même compressé, d'une image, ce schéma ne peut être reproduit pour transmettre des images vidéo. Cependant, d'une image à l'autre les données ont peu varié (redondance temporelle), il est donc envisageable de ne transmettre que la différence avec l'image précédente. Ce principe, s'il semble simple, ne peut être appliqué strictement. En effet une erreur dans l'image de référence se propagerait dans les images suivantes. Il est donc nécessaire périodiquement de transmettre une image complète (compression JPEG). MPEG définit le codage des images comprises entre deux images de références appelées images **I** (*Intra Picture*). Ces images sont codées indépendamment du contexte, seul intervient leur contenu. Elles constituent des points de référence à partir desquels les autres images sont construites (figure 1.30).

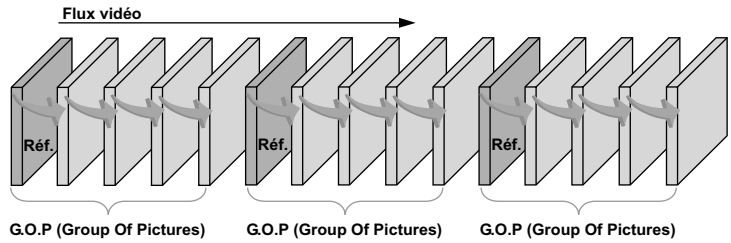


Figure 1.30 Principe d'un groupement d'images.

Principe de la compensation de mouvement

Dans une séquence vidéo animée, si la vitesse de déplacement est faible vis-à-vis de la fréquence des images, il y a peu de différence entre deux images successives. Il est alors envisageable d'envoyer la différence entre l'image actuelle et l'image précédente (figure 1.31).

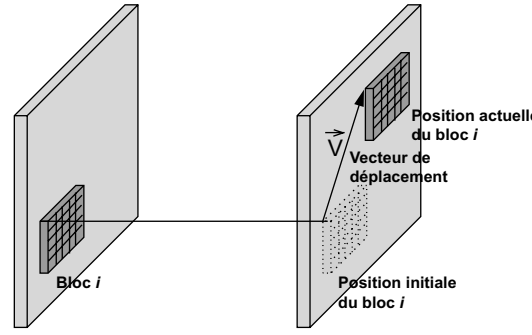


Figure 1.31 Principe du codage des images P (prédites).

Ainsi, le système décompose l'image en macroblocs et recherche dans l'image suivante la position d'un macrobloc identique qui minimise les informations d'erreurs (vecteurs de déplacement). Pour être valable, la différence ne doit pas être codée à partir de l'image réelle précédente, mais à partir de l'image précédente telle que la reconstituera le décodeur. Cette approche implique qu'un

codeur vidéo comporte aussi un décodeur pour coder valablement la compensation de mouvement. Les images ainsi construites sont dites images **P** (prédites, *Predicted Pictures*). Le déplacement est évalué non pas sur un bloc mais sur un macrobloc (16×16 pixels). Les données d'une image P constituent un ensemble de vecteurs décrivant la localisation des macroblocs dans l'image de référence et la correction à apporter. La réduction de bande par rapport à une image I est d'environ 50 %.

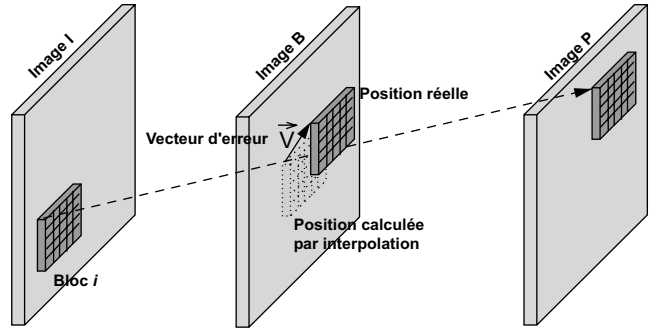


Figure 1.32 Principe du codage des images B (bidirectionnelles).

Une réduction plus importante peut être obtenue, en déduisant une image par interpolation de la position d'un bloc entre deux images successives. Cependant, quand un objet se déplace, il est possible de coder dans l'image suivante le déplacement de l'objet, mais il est impossible de deviner la partie masquée qu'il a découverte en se déplaçant. Pour cela, MPEG utilise un codage bidirectionnel. Les images bidirectionnelles ou *Bidirectional Pictures* (images **B**) sont déduites non seulement de la précédente, mais aussi de la suivante (prédiction arrière et avant). Le décodage correct d'une séquence vidéo nécessite donc plusieurs images. Cet ensemble unitaire d'images forme un groupe d'images (**GOP**, *Group Of Pictures*). La figure 1.33 représente un groupe d'images et les liens de codage entre les différentes images. Un GOP comprend entre dix et quinze images.

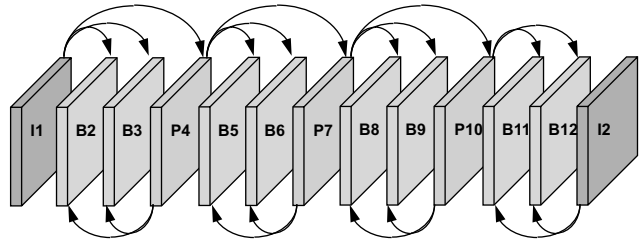


Figure 1.33 Exemple de structure d'un groupement d'images (GOP).

Ce mode de codage implique un déséquencement dans la transmission des images et donc un retard à la transmission et au décodage. Ce retard est sans importance, l'image vidéo n'ayant aucune interactivité avec le spectateur.

Structure du flux vidéo

La figure 1.34 représente le flux vidéo associé à une séquence complète. On y remarquera particulièrement l'ordre de présentation des images qui diffère de celui d'affichage.

© Dunod – La photocopie non autorisée est un délit

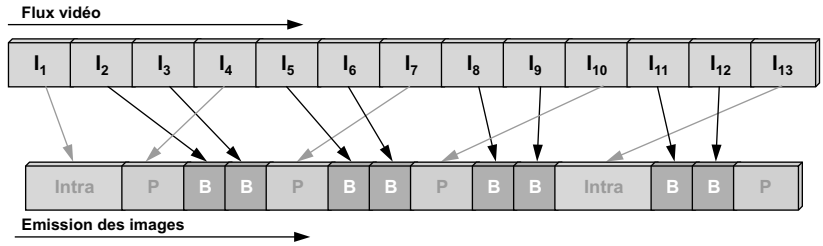


Figure 1.34 La description du flux vidéo.

La figure 1.35 illustre la structure hiérarchique des informations d'image. Le GOP correspond à une unité de codage, l'en-tête contient les informations d'horloge nécessaires à la restitution des images (fréquence image, taille, débit binaire, matrices de quantification...). Le champ image est une unité d'affichage ; son en-tête contient un numéro de séquence utilisé pour l'affichage des images dans l'ordre de visualisation. La tranche (*slice*) est une unité de codage et de resynchronisation du codeur ; l'en-tête précise la position de la tranche dans l'image et le nombre de macroblocs contenus. La structure macrobloc correspond à une unité de traitement de la compensation de mouvement. Le type de codage, les vecteurs déplacements... sont contenus dans l'en-tête. Enfin le bloc, unité élémentaire correspond à l'unité de traitement de la DCT.

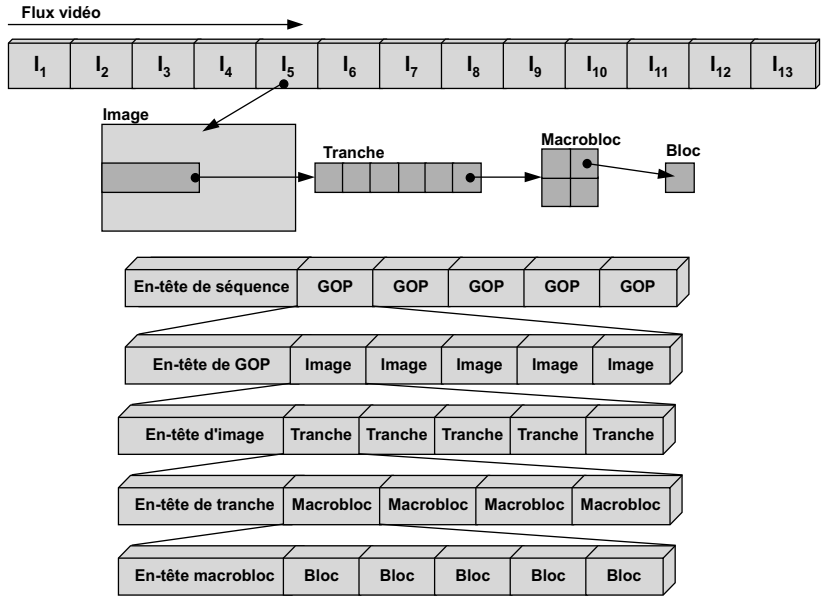


Figure 1.35 La structure hiérarchique d'un flux vidéo.

Structure simplifiée d'un décodeur MPEG

Les informations contenues dans un flux MPEG permettent de reconstituer complètement une séquence vidéo. La figure 1.36 représente la structure fonctionnelle d'un décodeur MPEG. Après décodage et séparation des informations, le décodeur MPEG comporte trois sous-systèmes :

le sous-système de traitement des images, le sous-système de traitement du son associé et enfin le sous-système de synchronisation.

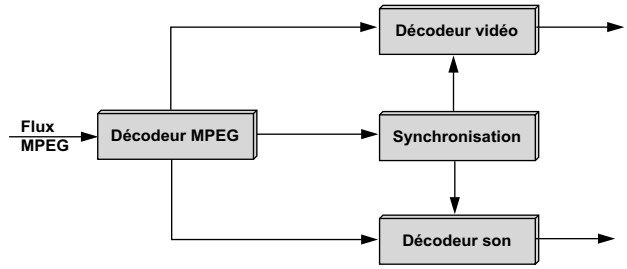


Figure 1.36 La structure fonctionnelle d'un décodeur MPEG.

Le standard MPEG assure la synchronisation entre les flux vidéo et audio. Deux paramètres sont définis : l'horloge de référence du système (**SCR**, *System Clock Reference*) et le marquage temporel (**PTS**, *Presentation Time Stamp*). Une horloge système à 90 kHz assure le marquage temporel ; elle est transmise dans le flux et codée sur 33 bits modulo 24 heures.

Le marquage temporel associé à chaque image vidéo (PTS) indique à quel moment celle-ci doit être affichée. En cas de décalage, le système peut ignorer certaines images pour rattraper un retard temporel.

1.4 LA NOTION DE QUALITÉ DE SERVICE

1.4.1 Les données et les contraintes de transmission

Les réseaux transportent des flux numériques et non des informations. Selon le type de données les exigences en termes de débit (volume), de temporalité (temps de transfert et variation de celui-ci) et fiabilité (taux d'erreur) diffèrent. Un système de transmission multimédia doit être capable de garantir à chaque type de flux le respect de ses contraintes spécifiques.

Ainsi, un transfert de fichiers correspond à un flux binaire constant. Il requiert un débit relativement important mais est très peu sensible au temps de transmission. Plus exigeantes en termes de temps de transfert (interactivité), les applications informatiques de type conversationnel sont caractérisées par la sporadicité des flux qu'elles soumettent au système de transmission.

Moins sensibles aux erreurs, la voix et la vidéo ont des exigences strictes en matière de débit (débit minimal garanti), de temps de transfert et surtout de récurrence temporelle (gigue), elles sont qualifiées de données isochrones[17]. La compression opérée sur ces types de données engendre des flux variables. La figure 1.37 résume ces différentes caractéristiques.

17. Isochrone : se dit des flux de données dans lesquels l'écart de temps entre deux informations successives doit être constant. Au cas où le réseau de transmission introduirait un décalage, un mécanisme spécifique doit être mis en œuvre par le récepteur.

© Dunod – La photocopie non autorisée est un délit

Type de transfert	Type de débit	Débit requis	Sensibilité à la variation du temps de transfert	Sensibilité aux erreurs
Voix	Constant	Faible	Élevée (isochrone)	Faible
Voix compressée	Variable	Faible	Élevée (isochrone)	Faible
Vidéo non compressée	Constant	Élevé	Élevée (isochrone)	Faible
Vidéo compressée	Variable	Élevé	Élevée (isochrone)	Faible
Transactionnel et transfert de fichiers	En rafale (*bursty*)	Moyen à élevé	Faible	Élevée
Interconnexion de réseaux locaux	En rafale, débit de la source élevé.	Élevé	Faible	Élevée

Figure 1.37 Types de données et contraintes de transmission.

1.4.2 Les classes de service

Garantir un transfert de données qui respecte les contraintes spécifiques à chaque type de flux de données (transparence sémantique et/ou la transparence temporelle), c'est assurer à celui-ci une certaine qualité de service ou **QoS** (*Quality of Service*).

Il existe essentiellement deux modes d'approche de la qualité de service. La première se contente d'augmenter la bande passante du réseau, la seconde plus pragmatique consiste à gérer la bande passante en allouant à chaque flux ce dont il a besoin. La qualité de service dans un réseau ne crée pas de bande passante, elle assure un traitement différencié à un flux donné.

La QoS et la réservation de ressource

Dans un système à bande passante limitée, les solutions adoptées sont toutes du deuxième type. Deux techniques s'opposent, la première consiste à rechercher un chemin dans le réseau (circuit virtuel) qui satisfasse les exigences du flux transmis (figure 1.38).

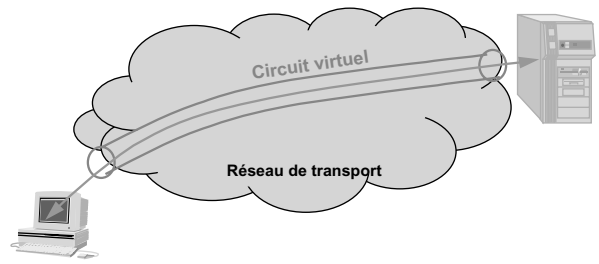


Figure 1.38 Principe de la réservation des ressources dans un réseau.

C'est l'approche traditionnelle des protocoles réseaux comme le *Frame Relay*[18] et l'ATM[18] (*Asynchronous Transfer Mode*).

Compte tenu de la combinatoire possible entre les différents éléments de qualité de service, ces derniers ont été regroupés en profils. C'est la notion de classe de service (**CoS**, *Classe of Service*). Plusieurs classifications de CoS ont été définies. La classification formulée par l'ATM Forum est la plus utilisée. Les classes de service se répartissent en deux catégories, celles qui requièrent une qualité de service multiple (multiservice) comme les applications voix et vidéo et celles de la qualité « données » dont les exigences sont moindres. Les classes de service permettent à l'utilisateur de spécifier ses besoins (contrat de service). La figure 1.39 fournit une description succincte des différentes classes de service.

Services	Noms	Caractéristiques	Application type
CBR	*Constant Bit Rate*	Débit constant Flux isochrone	Voix, vidéo non compressée
VBR-rt	*Variable Bit Rate* real time	Débit variable Flux isochrone	Applications audio et vidéo compressées
VBR-nrt	*Variable Bit Rate* non real time	Débit variable mais prévisible	Application de type transactionnel
ABR	*Available Bit Rate*	Débit sporadique Sans contrainte temporelle	Interconnexion de réseaux locaux
UBR	*Unspecified Bit Rate*	Trafic non spécifié *Best Effort*	Messagerie, sauvegarde à distance (*remote backup*)

Figure 1.39 Les classes de service de l'ATM Forum.

Dans les réseaux ATM et *Frame Relay*, la réservation des ressources par application est peu utilisée dans les réseaux, elle nécessite des protocoles d'établissement de route complexes. On préfère attribuer globalement une certaine QoS à une route, toutes les données transitant sur la route établie subissant le même traitement (figure 1.40).

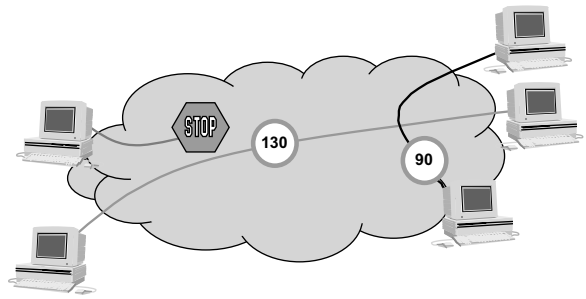


Figure 1.40 La schématisation du traitement de la priorité dans un réseau.

La QoS et la prioritisation des données

La notion de priorité consiste à marquer les flux en fonction d'un traitement à lui appliquer. Chaque application se voit attribuer dynamiquement une partie de la bande passante en fonction d'un niveau

18. Voir chapitre 14.

© Dunod – La photocopie non autorisée est un délit

de priorité indiqué dans chaque élément de données. Si ce système a la faveur des opérateurs car il simplifie la gestion du réseau, il présente l'inconvénient majeur de ne pas préserver les flux déjà établis dans le réseau ce qui conduit généralement à un surdimensionnement de ce dernier.

1.4.3 Conclusion

La notion de qualité de service est au cœur de la recherche de nouveaux protocoles et des développements réseaux. Des solutions ont été apportées à ce problème dans les protocoles de dernières générations tels qu'**ATM**, tandis que les protocoles plus anciens comme **TCP/IP** (*Transmission Control Protocol/Internet Protocol*) ont été adaptés et enrichis pour en tenir compte.

EXERCICES

Exercice 1.1 Code ASCII, algorithme de changement de casse

Donnez l'algorithme qui transforme la chaîne (*String*) codée en ASCII `Chaine = "IL FAIT BEAU"`, en chaîne ASCII `Chaine = "il fait beau"`, en pseudo-code et dans le langage de votre choix (Pascal, C).

Exercice 1.2 Codage de Huffman

Deux terminaux informatiques s'échangent des messages de longueur moyenne égale à 2 000 caractères. Ces caractères, clairement identifiés (A, F, O, R, U, W), apparaissent avec les probabilités respectives suivantes : 0,23 - 0,09 - 0,30 - 0,19 - 0,14 - 0,05.

1. Déterminez la longueur du code idéal.
2. Construisez l'arbre d'Huffman, puis donnez le code correspondant pour chacun des caractères ainsi que le nombre de bits du message ainsi codé.
3. Calculez la longueur moyenne du code établi.
4. Évaluez le taux de compression obtenu par rapport au code Baudot.
5. Donnez le temps de transmission du message codé en ASCII selon le code que vous avez établi, sachant que le signal est transmis sur un support dont le débit est de 4 800 bit/s.

Exercice 1.3 Télécopieur

Dans un télécopieur, un scanner analyse l'image ligne par ligne (balayage horizontal). Chaque ligne est découpée en un certain nombre de points (pixel). L'analyse de la ligne se traduit par une suite, plus ou moins longue, de zones blanches ou noires (séquence). La redondance d'information peut être réduite en ne transmettant que les informations de longueur et non les séquences elles-mêmes. Le codage des informations, en télécopie groupe 3, utilise le principe du code Huffman (code à longueur variable) appelé : code **Huffman modifié** (HM). À chaque longueur de séquence de blancs ou de noirs est associé un mot binaire unique. Sur ce principe, codez en Huffman le texte suivant (figure 1.41).

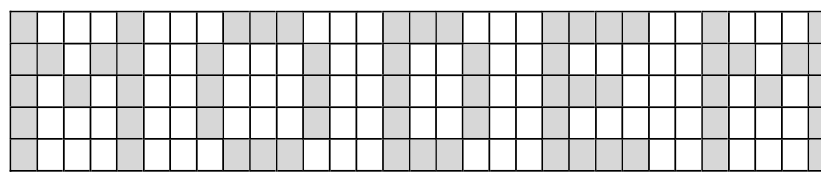


Figure 1.41 Page à coder en Huffman.

© Dunod – La photocopie non autorisée est un délit

Exercice 1.4 Numérisation du son

Les CD audio utilisent la technique MIC mais échantillonnent le son à 44,1 kHz (bande passante 20 Hz à 20 000 Hz, S/N = 96 dB) et le quantifient sur 16 bits. Pour améliorer la qualité de restitution, deux nouvelles technologies s'affrontent. À l'instar du CD audio, le DVD audio utilise aussi la technique MIC mais échantillonne à 192 kHz et quantifie sur 24 bits, tandis que le SACD (*Super Audio CD*) analyse le son à raison de 2,8224 MHz (technique *differential mode* dite ici *Direct Stream Digital*, bande passante 100 kHz et S/N 120 dB) et quantifie la variation de l'échantillon par rapport à son précédent sur un bit (1 valeur croissante, 0 valeur décroissante).

1. Calculez le débit nécessaire pour qu'une ligne transmette en temps réel les flux audios.
2. Calculez le volume à stocker pour une œuvre musicale d'une durée d'une heure en négligeant les données de service (correction d'erreur, index...).

Exercice 1.5 Numérisation et débit binaire

La télévision analogique occupe une largeur de bande de 6,75 MHz pour l'information de luminance et une bande réduite de moitié pour les informations de chrominance. Chaque signal étant quantifié sur 8 bits :

1. Déterminez le débit binaire nécessaire pour transmettre ces images numérisées.
2. Déterminez le nombre de couleurs d'une image ainsi numérisée.

Exercice 1.6 Rapport signal sur bruit et loi de quantification A

La loi de quantification logarithmique A permet d'obtenir un rapport signal sur bruit pratiquement constant sur tout l'espace de quantification. En établissant pour chaque segment de quantification la valeur maximale du bruit de quantification, vérifiez, de manière simple, cette assertion.

Exercice 1.7 Image RVB

Deux solutions étaient envisageables pour la télévision numérique, transmettre une image RVB ou une image *Y*, *Db* et *Dr*. Quel est l'avantage de la deuxième solution en matière d'efficacité de la transmission ?

Exercice 1.8 Type de flux voix et données (data)

En cas d'erreur dans un réseau, le système source peut éventuellement procéder à une réémission des données. Comparez vis-à-vis du traitement des erreurs les flux dits de données informatiques (*data*) et ceux de la voix.

Chapitre **2**

Les supports de transmission

2.1 GÉNÉRALITÉS

L'infrastructure d'un réseau, la qualité de service offerte, les solutions logicielles à mettre en œuvre dépendent largement des supports de transmission utilisés. Les supports de transmission exploitent les propriétés de conductibilité des métaux (paires torsadées, câble coaxial), celles des ondes électromagnétiques (faisceaux hertziens, guides d'onde, satellites) ou encore celles du spectre visible de la lumière (fibre optique). Généralement on classe les supports en deux catégories :

- les supports guidés (supports cuivre et supports optiques) ;
- les supports libres (faisceaux hertziens et liaisons satellites).

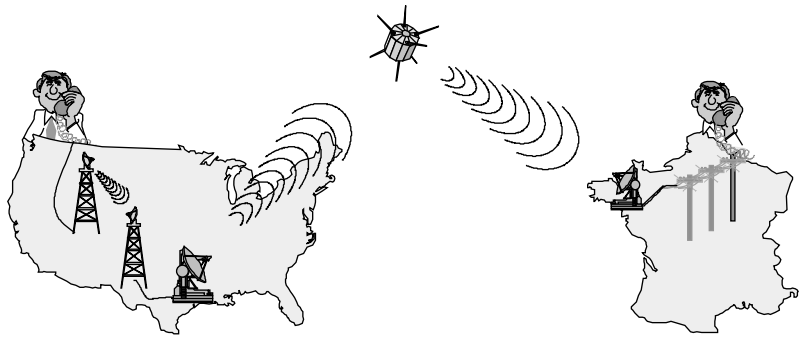


Figure 2.1 Une liaison informatique peut mettre en œuvre plusieurs types de support.

La complexité des systèmes provient généralement du fait qu'une liaison peut emprunter différents supports (figure 2.1). Le système de transmission devra alors réaliser l'adaptation du signal à transmettre à chaque type de support utilisé. Les caractéristiques des supports diffèrent selon la nature physique de celui-ci et du mode de propagation choisi. Cependant, certaines caractéristiques sont communes à tous les types de support (bande passante...), d'autres sont spécifiques (impédance caractéristique...). Les supports sont à l'origine de nombreux problèmes de transmission, aussi il

est important de bien en connaître les caractéristiques pour en comprendre l'utilisation et prévenir les différents problèmes d'exploitation pouvant survenir.

2.2 LES CARACTÉRISTIQUES DES SUPPORTS DE TRANSMISSION

2.2.1 La bande passante et le système de transmission

Généralités

L'impulsion électrique représentative d'un élément binaire est affaiblie (atténuation) et déformée (distorsion) par le système de transmission (figure 2.2).

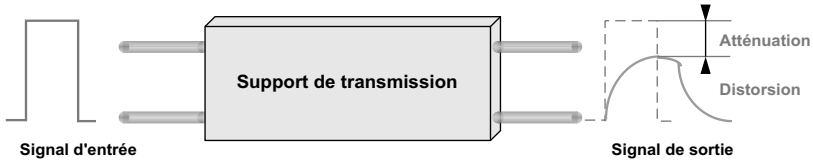


Figure 2.2 La déformation du signal par le support de transmission.

À l'extrémité de la ligne, le récepteur doit identifier et décoder le signal. Cette fonction ne peut valablement être réalisée que si le signal n'a pas été exagérément modifié durant la transmission. Ces modifications dépendent d'une part de la nature du signal (spectre du signal) et, d'autre part, de la réponse en fréquence du système (bande passante).

Notion d'analyse spectrale

L'impulsion électrique est un phénomène discontinu qui ne peut être modélisé. L'étude du comportement des circuits en régime impulsionnel est essentiellement due aux travaux du mathématicien et physicien Fourier qui a montré que tout signal périodique non sinusoïdal peut être considéré comme la somme d'une composante continue (A_0) et d'une infinité de signaux sinusoïdaux d'amplitude de fréquence et de phase convenablement choisies. Le théorème de Fourier peut s'exprimer simplement sous la forme de :

$$u(t) = A_0 + \sum_{i=1}^{i=\infty} U_i \cos(i\omega t + \varphi_i)$$

La composante de même fréquence que le signal d'origine est appelée **fondamental**. Les autres composantes, multiples de la fréquence du signal fondamental, sont appelées **harmoniques**. La figure 2.3 illustre la décomposition d'un signal carré.



u(t) = 4 U / π (sin ωt + 1/3 sin 3ωt + 1/5 sin 5ωt + ...)

Figure 2.3 La décomposition d'un signal carré symétrique par rapport au 0 volt.

Un signal périodique quelconque peut donc être considéré comme une infinité de signaux sinusoïdaux. Chaque composante peut être représentée par l'énergie qu'elle contient. Cette représentation est appelée **raie de fréquence** (transformation de l'espace temps en espace fréquence). L'ensemble des raies de fréquence constitue le spectre de fréquences (spectre de raies) du signal. L'espace de fréquence occupé par le spectre se nomme largeur de bande (figure 2.4). En théorie, la largeur de bande d'un signal non sinusoïdal est infinie.

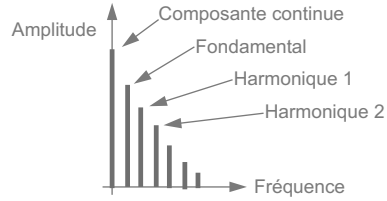


Figure 2.4 La notion de spectre du signal.

La figure 2.5 illustre la reconstitution du signal de la figure 2.3 à partir de ces trois premières composantes. En 1, le fondamental et la première composante donne un signal différent du signal d'origine. En 2, on additionne, au signal obtenu en 1, la troisième composante : le signal est plus proche du signal d'origine. En pratique, les cinq premières harmoniques sont suffisantes pour reconstituer un signal satisfaisant.

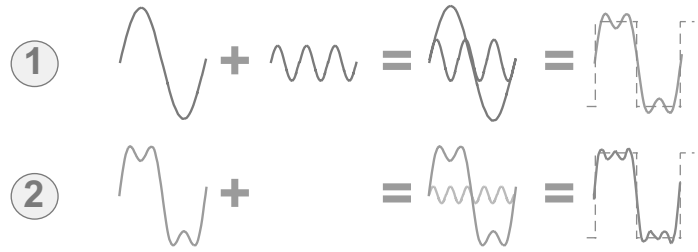


Figure 2.5 La reconstitution du signal d'origine.

Notion de bande passante

Dès lors, pour étudier le comportement d'un système en régime non sinusoïdal, on peut étudier celui-ci pour chacune des composantes du signal d'origine auquel il sera soumis. Cette étude est réalisée en utilisant une source de courant sinusoïdal dont on fait varier la fréquence (générateur de fréquences). La mesure de la puissance en sortie du système permet de tracer une courbe, dite **courbe de réponse en fréquence** (figure 2.6).

La courbe de la figure 2.6 montre que le système de transmission n'atténue pas toutes les composantes de la même manière. Dans ces conditions, le signal en sortie du système n'est plus l'image de celui en entrée, on dit qu'il y a distorsion (figure 2.2), cette distorsion est dite d'amplitude. De même, on constate que toutes les harmoniques ne sont pas transmises dans les mêmes délais, la déformation qui en résulte est dite distorsion de phase. Les distorsions d'amplitude et de phase sont indissociables, cependant la distorsion d'amplitude est plus importante que la distorsion de phase.

© Dunod – La photocopie non autorisée est un délit

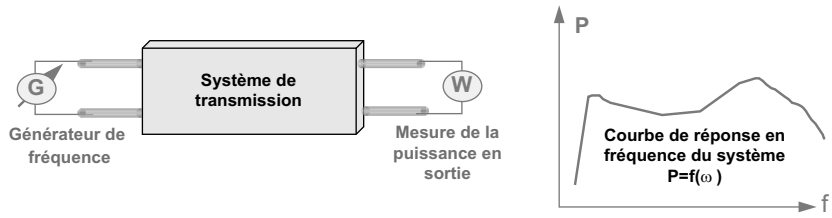


Figure 2.6 Principe du relevé de la bande passante d'un système.

Par conséquent, les systèmes de transmission (lignes, amplificateurs...) ne transmettent pas toutes les composantes du signal de façon identique. Les signaux sont transmis avec une distorsion faible jusqu'à une certaine fréquence appelée **fréquence de coupure**. Au-delà de cette fréquence, toutes les composantes sont fortement atténuées. On appelle **bande passante** (figure 2.7) l'espace de fréquences tel que tout signal appartenant à cet intervalle, ne subisse, au plus, qu'un affaiblissement déterminé par rapport à un niveau de référence prédéfini. L'affaiblissement, exprimé en décibel (dB), est donné par la relation :

$$A = 10 \log_{10} P_1 / P_0$$

où P_1 est la puissance du signal en sortie,
P_0 est la puissance du signal de référence

La bande passante est définie pour une atténuation en puissance de moitié, ce qui correspond à –3 dB (figure 2.7).

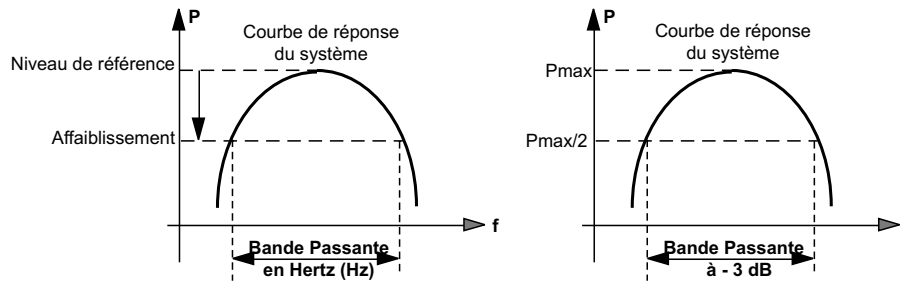


Figure 2.7 La bande passante à –3 dB.

La **largeur de bande** d'un signal correspond à la bande passante minimale que le système doit posséder pour restituer correctement l'information. Ainsi, la bande passante qualifie le système, et la largeur de bande qualifie le signal. Notons que le terme de bande passante est utilisé non seulement pour désigner un espace fréquentiel (bande passante ou BP en Hz), mais aussi pour qualifier le débit binaire d'un système (bande passante exprimée en bit/s).

Notion de filtre

Un système ne restitue pas les différentes composantes du signal de manière identique, il agit comme un filtre. Deux données caractérisent un filtre :

– La fréquence de coupure (*fc*), ou fréquence à partir de laquelle on considère que toutes les fréquences supérieures et (ou) inférieures sont atténuées d'une valeur donnée (généralement –3 dB).
– La pente de la courbe d'affaiblissement qui s'exprime en dB par octave[1].

En fonction de l'espace de fréquence que le système retransmet, on distingue trois types de filtres (figure 2.8).

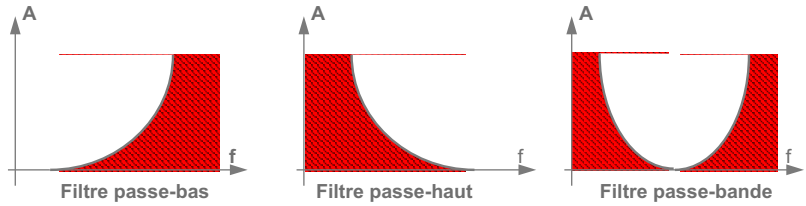


Figure 2.8 L'atténuation en fonction de la fréquence.

Le filtre passe-bas ne se laisse « traverser » que par les fréquences basses, il atténue les fréquences élevées. À l'inverse, le filtre passe-haut atténue les fréquences basses. En principe un système de transmission se présente à la fois comme un filtre passe-bas et un filtre passe-haut, il laisse passer une certaine bande de fréquence, c'est un filtre passe-bande (figure 2.9). Le signal à transmettre devra tenir compte de ces caractéristiques. L'adaptation du signal aux caractéristiques du support est réalisée par un équipement particulier dénommé ETCD (Équipement terminal de circuit de données).

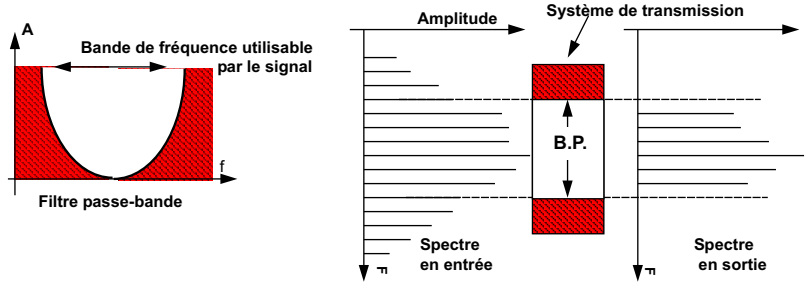


Figure 2.9 Le spectre du signal et le système de transmission.

2.2.2 L'impédance caractéristique

Définition

Une ligne de transmission est constituée de deux conducteurs de cuivre séparés par un isolant. La figure 2.10 modélise un élément d'une ligne en matérialisant ses composantes physiques. Elle présente au courant électrique un effet résistif (*R*) responsable de l'atténuation du signal, des effets

1. Une octave correspond à une variation de fréquence dans un rapport de 1 à 2.

© Dunod – La photocopie non autorisée est un délit

réactifs qui se décomposent en effet selfique (L) et en effet capacitif (C), et enfin la conductance (G) qui exprime la perte par effet résistif entre les deux conducteurs (généralement négligeable).

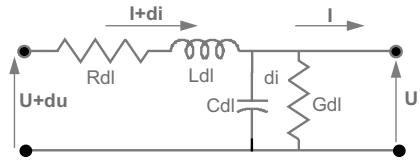


Figure 2.10 Le schéma équivalent d'un élément (dl) d'une ligne de transmission.

On appelle impédance (Z) de l'élément de ligne de longueur dl, le rapport du/di. La notion d'impédance en courant alternatif recouvre une notion similaire à celle de résistance en courant continu, elle s'exprime en ohm (Ω). Le rapport du/di pour une ligne supposée de longueur infinie s'appelle **impédance caractéristique** notée Zc :

$$Zc = \sqrt{\frac{R + jL\omega}{G + jC\omega}} \approx \sqrt{\frac{L}{C}}$$

avec $\omega = 2\,\pi\,.\,f$,
où ω est la pulsation du courant exprimée en radian/s,
et f, en Hz, la fréquence du signal.

On montre (figure 2.11) qu'une ligne de longueur finie refermée sur un récepteur, dont l'impédance Zr est telle que $Zr = Zc$, se comporte comme une ligne de longueur infinie. Le transfert de puissance est alors maximal entre le générateur et le récepteur. La ligne est dite adaptée (**adaptation d'impédance**).

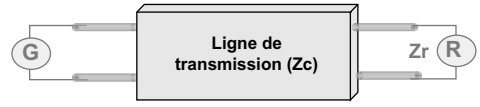


Figure 2.11 La notion d'adaptation d'impédance.

Conséquence de la désadaptation d'impédance : l'écho

À chaque rupture d'impédance ($Zr \# Zc$), le transfert de puissance n'est pas optimal, une partie de l'énergie incidente est réfléchie. Cette énergie (onde réfléchie ou **écho**) se combine à l'énergie incidente pour former des ondes stationnaires. En transmission numérique, l'écho a pour conséquence de générer des « bits fantômes », introduisant ainsi des erreurs de transmission. La figure 2.12 illustre un système complètement désadapté. À chaque point de raccordement, une partie de l'énergie est réfléchie. La source reçoit deux fois le signal d'écho. Le premier dû à la rupture d'impédance locale (écho local) est peu gênant. Le second dû à la rupture d'impédance distante (écho distant) est plus perturbant, des dispositifs spécifiques (annuleurs d'écho) ont en charge de supprimer les effets de cet écho.

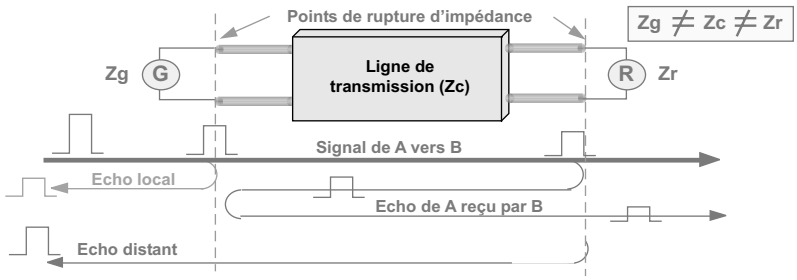


Figure 2.12 La notion d'écho.

Pour éviter ces réflexions parasites, il est nécessaire, tout au long de la ligne et à chaque raccordement d'un nouvel élément à la liaison, de réaliser la continuité de l'impédance : c'est l'adaptation d'impédance. Cependant, celle-ci n'est pas toujours réalisable. Par exemple, la ligne qui raccorde un usager à un réseau peut être en 2 fils, alors que la transmission dans le réseau de l'opérateur s'effectue en 4 fils (2 fils par sens de transmission), le passage de 2 à 4 fils provoque une rupture d'impédance et des échos. L'emploi d'annuleur d'écho est alors indispensable (figure 2.13).

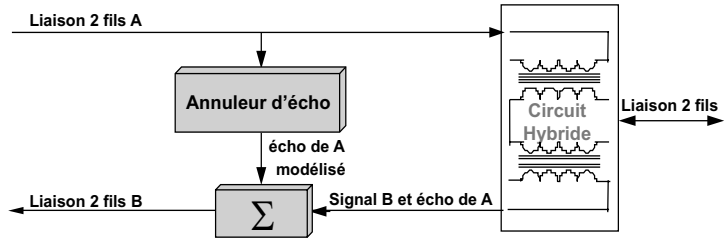


Figure 2.13 Principe de l'annulation d'écho.

Le filtre annuleur d'écho de la figure 2.13 réalise une estimation du signal d'écho en amplitude et phase (modélisation mathématique). Ce signal est ajouté en opposition de phase au signal de l'autre canal. Le système est symétrique pour les deux canaux de communication (injection d'une partie du signal B dans A). Le *Return Loss* mesure le rapport entre l'énergie transmise et l'énergie réfléchie.

2.2.3 Le coefficient de vélocité

Le **coefficient de vélocité** est une grandeur qui informe sur la vitesse de propagation du signal dans un support. C'est le rapport entre la vitesse de propagation réelle et la vitesse de la lumière ($c = 3 \cdot 10^8$ m/s). Pour les câbles cuivre, il vaut environ 0,7. Notons que la vitesse de propagation dans un support est une fonction inverse de la racine carrée de la fréquence.

$$V = v.c$$

avec V vitesse de propagation réelle du courant en m/s,
v coefficient de vélocité,
c célérité ou vitesse de la lumière.

© Dunod – La photocopie non autorisée est un délit

Le temps de propagation d'un signal entre sa source et sa destination est fonction de la distance. Lorsque la transmission a lieu sur un seul support, ce facteur est peu important. Dans les systèmes où les données sont transmises simultanément sur plusieurs supports, comme dans le Gigabit Ethernet, les parcours n'étant pas strictement identiques, les temps de propagation diffèrent (*delay skew*) et impliquent l'utilisation de système de retard pour réaligner les signaux.

2.3 LES SUPPORTS GUIDÉS

2.3.1 La paire torsadée



Figure 2.14 Paire torsadée ou paire symétrique.

La paire torsadée ou symétrique est constituée de deux conducteurs identiques torsadés. Les torsades réduisent l'inductance de la ligne (L). Généralement plusieurs paires sont regroupées sous une enveloppe protectrice appelée gaine pour former un câble. Les câbles contiennent une paire (desserte téléphonique), quatre paires (réseaux locaux), ou plusieurs dizaines de paires (câble téléphonique).

Caractéristiques

Impédance caractéristique, bande passante et atténuation sont les caractéristiques essentielles des paires torsadées. Cependant, compte tenu de la proximité des différentes paires dans un câble, un phénomène spécifique apparaît : la **diaphonie** (figure 2.15). La diaphonie, due au couplage inductif entre paires voisines, correspond au transfert du signal d'un câble à un autre. Elle limite l'utilisation de la paire symétrique à de faibles distances.

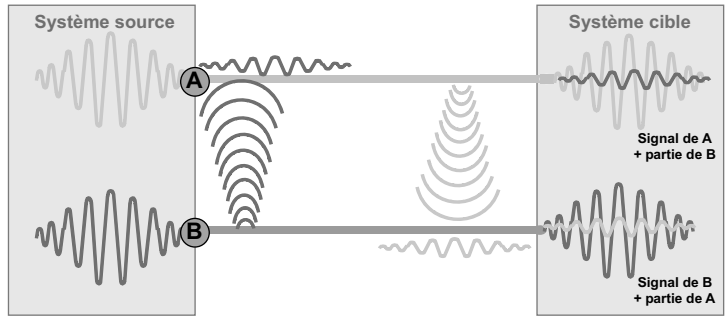
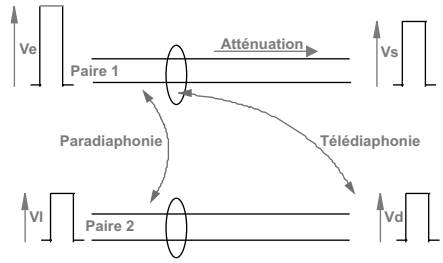


Figure 2.15 Le couplage inductif entre paires : la diaphonie.

Deux grandeurs ont été introduites pour mesurer ce phénomène : la paradiaphonie et la télédiaphonie. La paradiaphonie (**Next** ou *Near end crosstalk*) et la télédiaphonie (**Fext** ou *Far end crosstalk*) indiquent l'affaiblissement du signal transmis sur les paires avoisinantes par rapport au signal d'entrée, l'une est mesurée près de la source (*Near*), l'autre à l'extrémité (*Far*). Ces rapports sont exprimés en dB ; plus grande est la valeur, meilleur est le câble utilisé (figure 2.16).



Atténuation A = 20 $\log_{10}$ *Vs* / *Ve* où *Vs* est la tension en sortie, *Ve* est la tension du signal d'entrée.

Paradiaphonie Next = 20 $\log_{10}$ *Vl* / *Ve* où *Vl* est la tension locale induite, *Ve* est la tension du signal d'entrée.

Télédiaphonie Fext = 20 $\log_{10}$ *Vd* / *Ve* où *Vd* est la tension distante induite, *Ve* est la tension du signal d'entrée.

Figure 2.16 La paradiaphonie et la télédiaphonie.

La paire torsadée « ordinaire » (paire symétrique, **UTP** *Unshielded Twisted Pairs*) est sensible à l'environnement électromagnétique (parasites industriels, proximité de câbles à courant fort...). L'utilisation de tels câbles est soumise à des contraintes d'installation. Pour ces raisons, la paire symétrique est généralement utilisée sans référence à la terre (transmission différentielle) ce qui améliore sa résistance aux parasites (voir le sous-paragraphe 3.2.2 *Mode de transmission électrique*).

L'immunité aux parasites peut être améliorée en protégeant le faisceau par un écran (câble écranté). L'écran est constitué d'un ruban d'aluminium qui entoure les paires et les protège des perturbations électromagnétiques. Un conducteur de cuivre nu étamé (drain) permet la mise à la terre de l'écran (paires écrantées, **FTP** *Foiled Twisted Pairs*). Une meilleure protection peut être obtenue en réalisant, autour de chacune des paires, un véritable blindage (paires blindées, **STP** *Shielded Twisted Pairs*).

La paire symétrique est actuellement le conducteur le plus utilisé : desserte locale des raccordements téléphoniques, liaisons d'accès aux réseaux de données et surtout les réseaux locaux où les faibles distances autorisent l'utilisation de débits élevés : 100 Mbit/s sur 100 m, voire 10 Gbit/s sur 100 m avec de la paire UTP.

Les systèmes de précâblage

Le développement intensif des postes de travail connectés, en réseau local ou autre, a révélé des problèmes liés au câblage. Les réseaux locaux ont tous, aujourd'hui, une topologie physique en étoile, d'où l'idée de réaliser, dans les immeubles de bureaux, un précâblage (figure 2.17). Un système de précâblage doit :

– assurer que tout poste de travail ne sera qu'à quelques mètres d'une prise informatique ou téléphonique ;
– être indépendant du type de réseau et de la topologie réseau choisis.

© Dunod – La photocopie non autorisée est un délit

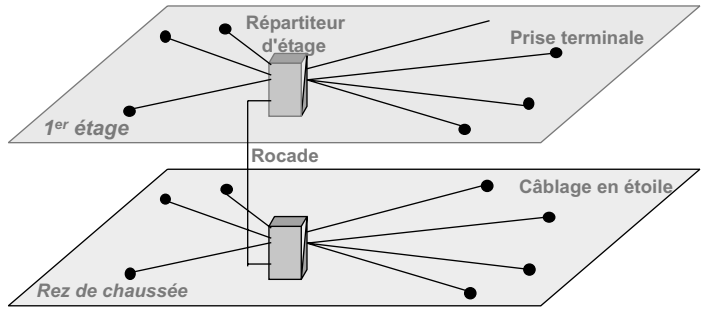


Figure 2.17 Principe d'un précâblage d'immeuble.

Les principaux systèmes sont l'ICS (*IBM Cabling System*), le BCS (*BULL Cabling System*), *l'Open Link* de DEC et le PDS Systimax. Ces systèmes ont en commun l'utilisation de la paire torsadée et une topologie physique en étoile. Le cœur du câblage est constitué de panneaux, dit **panneaux de brassage**, qui permettent, à l'aide de jarretières, de réaliser la connexion des postes de travail selon la topologie requise par le réseau. Ces systèmes diffèrent essentiellement par le type de câble utilisé (UTP, FTP).

Les câbles ont été répartis en différentes catégories selon les spécifications auxquelles ils répondent (atténuation, bande passante, Next...). La figure 2.18 classe les différents types de câble et indique leur utilisation.

Catégorie	Classe	Bande passante	Exemples d'utilisation
1 & 2	A, B		Voix (600 Ω)
3	C	16 MHz	Voix numérique, réseaux locaux de type Ethernet et AnyLan
4	D	20 MHz	Réseaux locaux de type Token Ring
5	D	100 MHz	Réseaux locaux Ethernet 10 et 100 Mbit/s, Token Ring, AnyLAN
6	E	250 MHz	Câble UTP et FTP, Ethernet 1 Gigabit/s
7		600 MHz	Câble SFTP

Figure 2.18 Les catégories de paires torsadées.

Le câble de catégorie 7 cumule une protection paire par paire par un écran (protection contre les hautes fréquences) et une protection de l'ensemble des paires par un véritable blindage (protection contre les basses fréquences).

La catégorie distingue les équipements, la notion de classe de câblage qualifie un câblage de bout en bout. Notons que les câbles 120 Ω catégorie 6, très utilisés en France jusqu'à ces derniers temps, ont été relégués en classe C dans la dernière version de la norme ISO/IEC (ISO 11801 du 23 octobre 2002).

2.3.2 Le câble coaxial

Une paire coaxiale ou câble coaxial (figure 2.19) est constituée de deux conducteurs concentriques maintenus à distance constante par un diélectrique. Le conducteur extérieur, tresse métallique en cuivre recuit appelée **blindage**, est mis à la terre. L'ensemble est protégé par une gaine isolante.

Le câble coaxial possède des caractéristiques électriques supérieures à celles de la paire torsadée. Il autorise des débits plus élevés et est peu sensible aux perturbations électromagnétiques extérieures. Le taux d'erreur sur un tel câble est d'environ 10^{-9}.

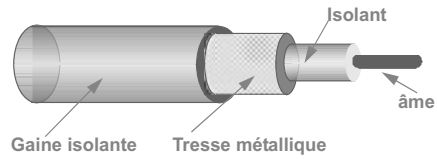


Figure 2.19 Le câble coaxial.

En transmission numérique, notamment dans les réseaux locaux, on utilise des câbles d'impédance 50 Ω à des débits pouvant atteindre 10 Mbit/s sur des distances de l'ordre du kilomètre. En transmission analogique, le câble coaxial est utilisé pour réaliser des liaisons longues distances. Son impédance est de 75 Ω. Ce câble, similaire au câble coaxial utilisé en télévision, est souvent dénommé câble CATV. La bande passante est d'environ 300 MHz à 1 GHz.

Le CATV présente une bonne immunité aux parasites, mais cher et exigeant en contraintes d'installation (rayon de courbure...), il n'est plus utilisé que dans des environnements perturbés ou dans les systèmes sécurisés (rayonnement). Dans les réseaux locaux, il est remplacé par la paire torsadée et dans les liaisons longues distances par la fibre optique.

2.3.3 La fibre optique

Principe

Un faisceau de lumière (figure 2.20), au passage d'un milieu 1 vers un milieu 2 (dioptre), est réfléchi (retour au milieu d'origine) et est réfracté avec une déviation (passage dans le milieu 2).

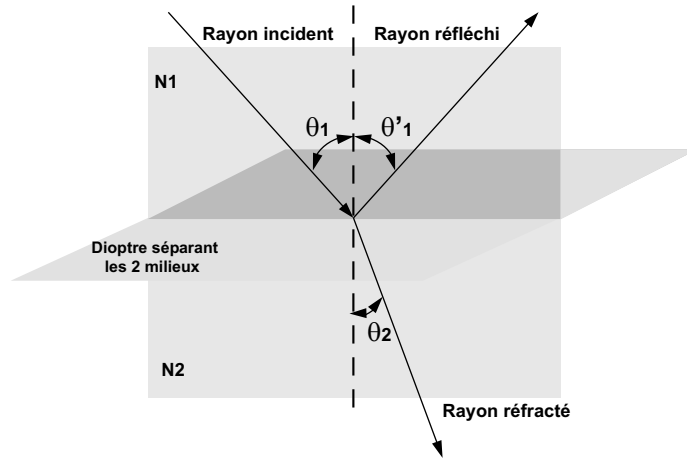


Figure 2.20 La loi de Descartes ($N_1 \sin \theta_1 = N_2 \sin \theta_2$).

© Dunod – La photocopie non autorisée est un délit

L'indice de réfraction (n_1, n_2) mesure le rapport entre la vitesse de propagation du rayon lumineux dans le vide et celle dans le milieu considéré, soit :

$$n = c / v$$

où n est l'indice de réfraction absolu du milieu considéré,
c la vitesse de la lumière dans le vide ($3 \cdot 10^8$ m/s),
v vitesse de propagation de la lumière dans le milieu considéré.

L'indice de réfraction du vide est évidemment de 1, celui de l'air 1,003, du verre ordinaire d'environ 1,5 et de l'eau de 1,33.

Lorsque l'angle d'incidence augmente (θ_1), l'énergie réfractée diminue et l'énergie réfléchie augmente. Si on augmente encore l'angle, la réfraction devient nulle ($\theta_2 = \pi/2$, condition limite de la réfraction) toute l'énergie est réfléchie (réflexion totale). Cette propriété est utilisée pour réaliser des guides de lumière : la fibre optique. Une fibre optique (figure 2.21) est composée d'un « fil » de silice étiré de telle manière que l'on distingue deux structures d'indice de réflexion différent, l'une appelée **cœur**, l'autre qui « l'entoure » appelée gaine optique ou **manteau**, l'ensemble étant protégé par une enveloppe dite de protection. La réflexion totale est assurée par des valeurs d'indices proches, tel que $n_1 > n_2$ où n_1 est l'indice du cœur et n_2 celui de la gaine.

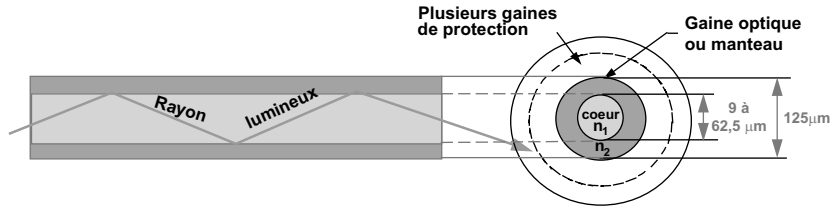


Figure 2.21 La fibre optique : guide de lumière.

Un système de transmission par fibre optique met en œuvre (figure 2.22) :

- un émetteur de lumière (transmetteur), constitué d'une diode électroluminescente **LED** (*Light Emitting Diode*) ou d'une diode **LASER** (*Light Amplification by Stimulated Emission of Radiation*), qui transforme les impulsions électriques en impulsions lumineuses ;
- un récepteur de lumière, constitué d'une photodiode de type **PIN** (*Positive Intrinsic Négative*) ou de type PDA (à effet d'avalanche) qui traduit les impulsions lumineuses en signaux électriques ;
- une fibre optique.

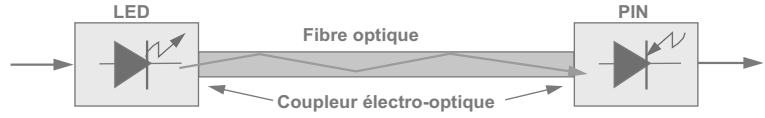


Figure 2.22 Principe d'une liaison optique.

La puissance émise par une LED est peu élevée ($\cong$ 1 mW) et, seul un faible pourcentage de cette puissance est récupéré dans la fibre. Pour les liaisons à haut débit, on lui préfère les diodes laser. Ces dernières autorisent une puissance à l'émission voisine de 5 mW avec un rendement de couplage d'environ 50 %. Une LED a une bande passante de 100 MHz, une diode laser permet une largeur de bande de 800 MHz.

La fibre est en principe un système de transmission unidirectionnel, une liaison optique nécessite l'utilisation de deux fibres. La figure 2.23 montre la réalisation de coupleurs optiques pour interconnecter deux réseaux locaux.

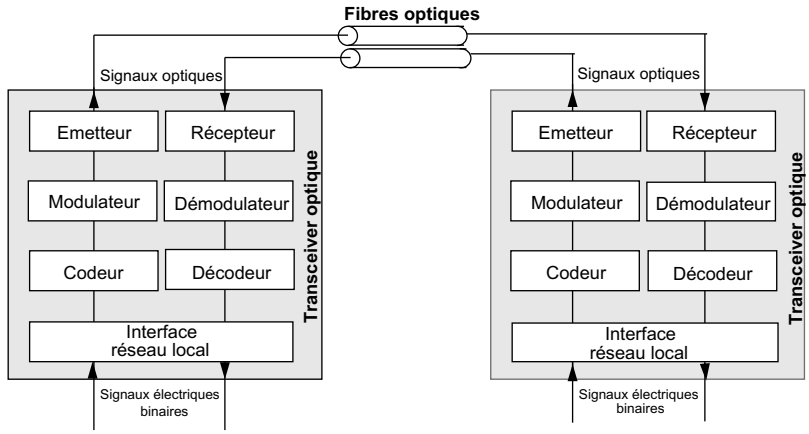


Figure 2.23 L'interconnexion de deux réseaux locaux par fibre optique.

Les différents types de fibres

Les rayons lumineux introduits dans la fibre qui remplissent la condition de réflexion (angle d'incidence) sont acheminés dans le cœur de la fibre. L'ensemble des rayons ainsi admis forme un cône dit cône d'acceptance dont l'ouverture ou angle d'incidence maximal est $\theta_{\max}$ (figure 2.24). L'ouverture numérique (*ON*) de la fibre est la grandeur qui qualifie le cône d'acceptance ($ON = \sin \theta_{\max}$). Les fibres optiques sont distinguées en fonction du mode de propagation, de leur ouverture numérique et du mode de variation des indices entre le cœur et le manteau.

➤ Les fibres à saut d'indice

Dans les fibres à saut d'indice, le cœur d'indice n_1 est entouré d'une gaine d'indice n_2. La variation d'indice entre le cœur et la gaine est brutale (saut d'indice). La propagation s'y fait par réflexion totale à l'interface cœur/gaine.

Quand le diamètre du cœur de la fibre est grand devant la longueur d'onde de la lumière, l'ouverture numérique est importante et permet un bon couplage optique. Ce type de fibre autorise l'utilisation de sources de faible puissance (LED). Cependant, la fibre admet plusieurs rayons qui se propagent sur des chemins différents ou modes de propagation. Ces différents trajets provoquent un étalement du signal (dispersion modale ou **DMD**, *Differential Mode Delay*), la fibre est alors dite multimode (**MMF**, *MultiMode optical Fiber*, figure 2.24). La dispersion modale provoque un étalement du signal, ce qui limite la bande passante de la fibre et la distance franchissable.

© Dunod – La photocopie non autorisée est un délit

En réduisant le diamètre du cœur, on réduit l'ouverture numérique. Cette réduction, peut être telle que, pour une longueur d'onde donnée, la fibre n'admette plus qu'un seul rayon. La fibre est alors dite monomode (**SMF**, *Single Mode optical Fiber*), le diamètre du cœur est compris entre 8 et 9 μm et le diamètre du manteau 125 μm. La fibre n'est monomode qu'au-delà d'une certaine longueur d'onde appelée **longueur d'onde de coupure** ($\approx$1 200 nm). La bande passante est importante, elle autorise des débits conséquents (plusieurs gigabits) et des distances franchissables d'une centaine de kilomètres. Si la fibre monomode autorise des liaisons de grande distance, le couplage optique est faible et demande une source lumineuse de puissance supérieure. La fibre monomode utilise des sources laser (*Light Amplification by Stimulated Emission of Radiation*), d'un coût plus élevé et d'une longévité réduite.

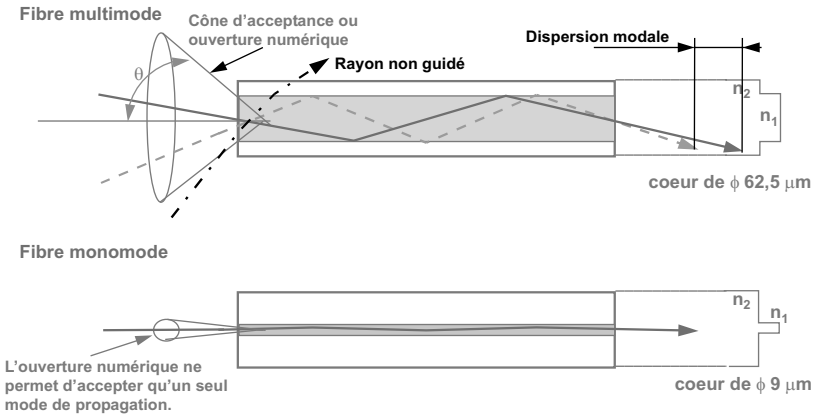


Figure 2.24 Les fibres à saut d'indice.

➤ Les fibres à gradient d'indice

Un compromis a été trouvé avec les fibres à gradient d'indice (figure 2.25), l'indice du cœur décroît de façon continue, depuis le centre du cœur jusqu'à l'interface cœur/gaine suivant une loi parabolique. Tous les rayons sont focalisés au centre de la fibre, ils ont une trajectoire proche de la sinusoïde. La vitesse de propagation est d'autant plus élevée que l'indice de réfraction est faible. Cette différence de vitesse tend à compenser les différences de trajet, elle réduit la dispersion modale et autorise une portée plus grande que les fibres multimodes à saut d'indice. La bande passante, pour une fibre d'un kilomètre est de plusieurs gigabits et l'affaiblissement inférieur au dB/km, ce qui autorise des portées d'environ 50 kilomètres.

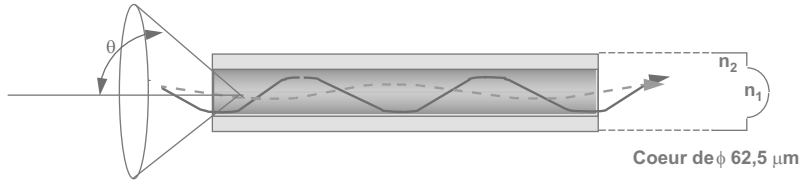


Figure 2.25 Les fibres à gradient d'indice.

La performance des fibres optiques

Dans une fibre optique, on montre que le produit bande passante par la distance est une constante. De ce fait, on exprime la bande passante par km. Compte tenu de la réponse en fréquence des fibres (figure 2.26) et des coupleurs optoélectroniques, on définit trois plages d'utilisation appelées fenêtres optiques proches de l'infrarouge.

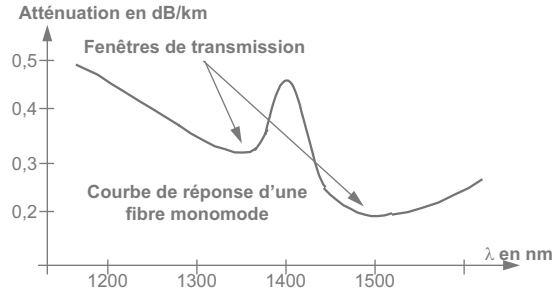


Figure 2.26 La notion de fenêtre optique.

La première fenêtre à 850 nm ($3{,}53 \cdot 10^5$ GHz) correspond à l'utilisation de coupleurs à coût minimal. Ce n'est pas l'optimum d'utilisation des fibres, mais dans des liaisons à faible distance, comme dans les réseaux locaux, cette fenêtre est parfaitement adaptée. Généralement, on lui préfère la fenêtre de 1 300 nm ($2{,}3 \cdot 10^5$ GHz), l'atténuation n'est alors que d'environ 0,5 dB/km. La fenêtre située à 1 550 nm ($1{,}93 \cdot 10^5$ GHz) a l'avantage de ne présenter qu'une atténuation d'environ 0,2 dB/km, mais les coupleurs sont plus coûteux. Les performances des fibres optiques sont :

- bande passante importante,
- immunité électromagnétique,
- faible taux d'erreur 10^{-12},
- faible affaiblissement (0,2 à 0,5 dB/km),
- faible encombrement et poids,
- vitesse de propagation élevée (monomode),
- sécurité (absence de rayonnement à l'extérieur et difficulté de se mettre à l'écoute),
- légèreté.

Ces caractéristiques font des fibres optiques le support privilégié dans le domaine des télécommunications à haut débit et grande distance, dans les applications aéronautiques et navales (sous-marin) et dans les transmissions de données en milieu perturbé.

Si la pose de la fibre optique est aisée (pas de contraintes particulières), la connectique est assez délicate, elle nécessite un outillage particulier et un savoir-faire certain.

2.3.4 Les liaisons hertziennes

Principe

Un conducteur rectiligne alimenté en courant haute fréquence ou radiofréquence peut être assimilé à un circuit oscillant ouvert. Un tel circuit ou antenne d'émission rayonne une énergie, ou onde

© Dunod – La photocopie non autorisée est un délit

électromagnétique, qui résulte de la combinaison d'un champ magnétique et électrostatique. Cette énergie électromagnétique se propage sans support matériel ; recueillie par un autre conducteur distant ou antenne de réception, elle est transformée en un courant électrique similaire à celui d'excitation de l'antenne d'émission (théorème de réciprocité). La figure 2.27 illustre le principe d'une liaison radioélectrique.

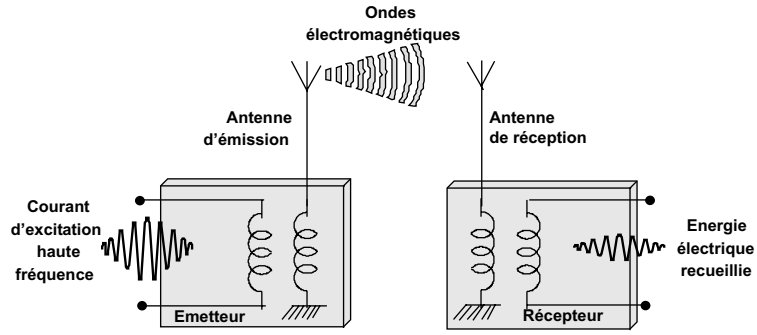


Figure 2.27 Principe d'une liaison radioélectrique.

Contrairement aux supports étudiés dans les paragraphes précédents, la liaison entre les deux entités émetteur et récepteur s'effectue sans support physique. Les ondes électromagnétiques (**OEM**) ou ondes hertziennes[2] se propagent dans le vide à la vitesse de la lumière (c). On appelle longueur d'onde (λ), la distance parcourue par l'onde pendant une période du phénomène vibratoire. La longueur d'onde varie avec la vitesse de propagation. Dans le vide, son expression est :

$$\lambda = c\ T$$

avec λ longueur d'onde exprimée en mètres,
c vitesse de propagation dans le vide ($3 \cdot 10^8$ m/s),
T période du phénomène vibratoire exprimée en secondes.

Une antenne est un conducteur dont la longueur est un sous-multiple entier de la longueur d'onde. Le rayonnement d'une source ponctuelle est omnidirectionnel, l'énergie se diffuse selon une sphère. Le rayonnement d'un conducteur rectiligne s'effectue selon un demi-tore. Afin d'utiliser au mieux l'énergie rayonnée, on réalise des réflecteurs. Les réflecteurs peuvent être actifs (rideaux d'antennes) ou passifs (brins, réflecteur plan ou parabolique).

La transmission de données utilise des systèmes d'antenne passifs à émission directive (faisceaux hertziens) ou à diffusion (liaisons satellitaires, mobiles en téléphonie mobile...).

Les ondes électromagnétiques subissent peu d'affaiblissement, leur mise en œuvre est assez aisée et le coût d'infrastructure généralement faible devant les coûts de génie civil engendrés par le passage de câbles physiques. Les transmissions par ondes électromagnétiques sont utilisées chaque fois qu'il est nécessaire :

– de diffuser une même information vers plusieurs utilisateurs (réseaux de diffusion),

2. Les ondes hertziennes ont été découvertes par le physicien allemand Heinrich Hertz en 1888.

– de mettre en relation des stations mobiles (réseaux de messagerie),
– de relier, à haut débit, deux entités éloignées (faisceaux hertziens) ou très éloignées (satellites de communication).

La propagation des ondes électromagnétiques

Les ondes électromagnétiques (OEM) sont sensibles aux perturbations atmosphériques et leur propagation s'effectue selon plusieurs modes qui dépendent de la fréquence (figure 2.28).

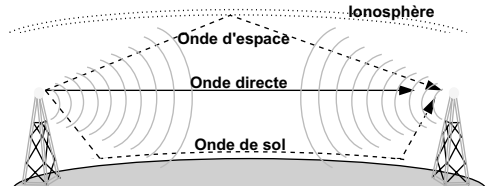


Figure 2.28 Les différents modes de propagation des OEM.

Les systèmes de transmission de données basés sur des systèmes radio utilisent des fréquences dont le mode de propagation principal est la propagation par l'onde directe, c'est-à-dire que l'antenne de réception doit être visible de l'antenne d'émission (figure 2.29). La portée (P en km) de tels systèmes est donc limitée par la rotondité de la terre et la hauteur des antennes (*he* et *hr* exprimées en m).

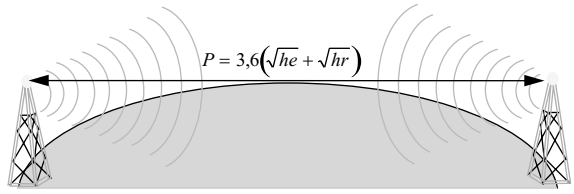


Figure 2.29 La portée optique d'une liaison hertzienne.

La portée pratique est légèrement plus élevée que la portée théorique. Le trajet de l'onde est modifié par un phénomène de réfraction qui incurve légèrement le faisceau qui suit un peu la rotondité de la Terre. D'autres phénomènes perturbateurs, illustrés par la figure 2.30, influent sur la réception.

Les ondes électromagnétiques subissent peu d'affaiblissement dans l'atmosphère, sauf par temps de brouillard ou de pluie où les particules d'eau absorbent l'énergie des ondes. Selon la longueur d'onde, certaines matières absorbent toute l'énergie de l'onde, créant ainsi de véritables zones d'ombre. D'autres matériaux réfléchissent les ondes, ainsi un récepteur peut recevoir plusieurs fois l'information, une fois par le trajet direct et une ou plusieurs fois par des trajets réfléchis. L'onde reçue est alors la composition de l'onde directe et des ondes réfléchies. Du fait de la différence de trajet (temps de parcours), ces ondes ne sont plus en phase, l'onde reçue résultante est la composition des différentes ondes reçues (figure 2.31). Selon l'écart de phase entre ces différentes ondes, l'évanouissement du signal peut être plus ou moins élevé, voire nul (*fading*). De même un obstacle peut modifier le trajet de l'onde (diffraction), la diffraction dépend de la longueur d'onde, elle étale le spectre (dispersion) et perturbe la réception (*fading* sélectif).

© Dunod – La photocopie non autorisée est un délit

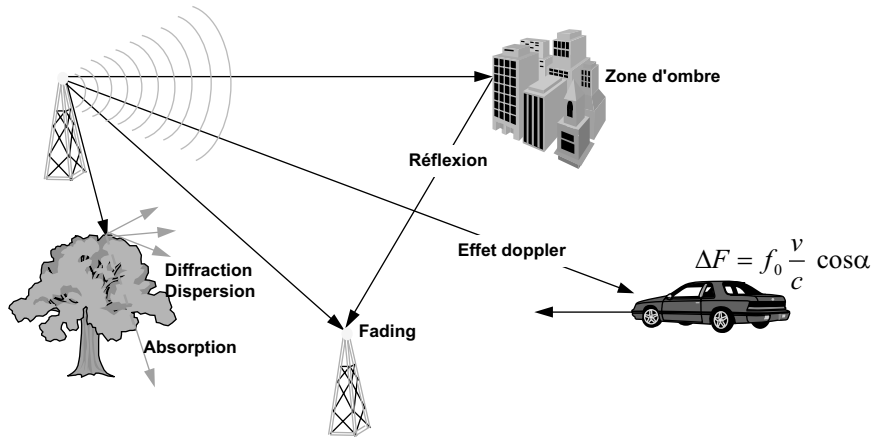


Figure 2.30 Synthèse des phénomènes agissant sur la transmission des OEM.

Lorsque l'émetteur ou le récepteur n'est pas fixe, l'onde subit une modification apparente de sa fréquence. Si le mobile se rapproche de la source, la période semble plus courte donc la fréquence plus grande ; inversement, en éloignement la fréquence reçue est plus faible que celle émise (effet Doppler). L'écart de fréquence (Δf) est directement fonction de la vitesse de déplacement relative entre les deux systèmes (v), de la fréquence du signal (f_0) et de l'angle (α) entre le faisceau émis et le déplacement du mobile (figure 2.30).



Figure 2.31 La notion de fading.

Chaque type de liaison ou d'application utilise des bandes de fréquences différentes. L'espace de fréquences utilisables est limité. On appelle canal radio ou canal de transmission la bande de fréquences réservée à une communication. La figure 2.32 décrit le spectre de fréquences. Les ondes radioélectriques s'étendent de quelques dizaines de kilohertz (ondes longues ou grandes ondes) à plus du térahertz (ondes quasi optiques).

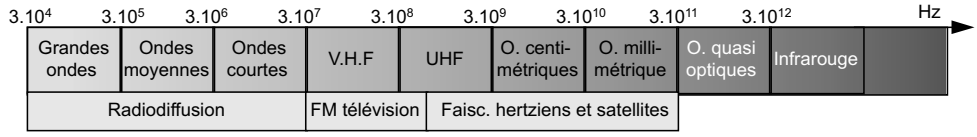


Figure 2.32 Le spectre des fréquences.

L'usage en est réglementé. Au niveau international, les fréquences sont gérées par l'UIT-TS (Union internationale des télécommunications – *Telecommunication Standardization*, ex-CCITT et CCIR). Les différents domaines d'utilisation se voient attribuer une bande de fréquences elle-même divisée en canaux. L'attribution locale des fréquences est généralement le fait d'organismes

nationaux, en France l'ANF (Agence nationale des fréquences) et ARCEP (Autorité de régulation des communications électroniques et des postes).

Les faisceaux hertziens

Les ondes radioélectriques peuvent, dans certains cas, remplacer avantageusement les liaisons filaires (cuivre ou optique). Les faisceaux hertziens ou câbles hertziens, par analogie avec les réseaux câblés peuvent être analogiques ou numériques. Les débits peuvent atteindre 140 Mbit/s. Ils sont principalement utilisés pour des réseaux :

- de téléphonie (multiplexage fréquentiel ou temporel),
- de transmission de données,
- de diffusion d'émissions télévisées.

Pour diminuer les puissances d'émission, la technique des faisceaux hertziens utilise des antennes très directives. L'antenne réelle est placée au foyer optique d'une parabole qui réfléchit les ondes en un faisceau d'ondes parallèles très concentré, limitant ainsi la dispersion de l'énergie radioélectrique. En réception, l'antenne est aussi placée au foyer optique de la parabole. Tous les rayons reçus parallèlement à l'axe optique de la parabole sont réfléchis vers le foyer optique, on recueille ainsi, un maximum d'énergie (figure 2.33).

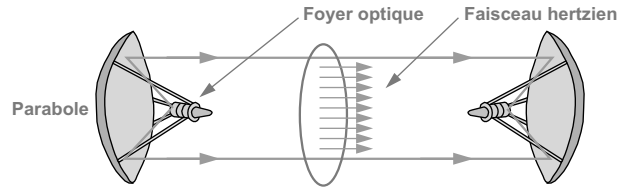


Figure 2.33 Principe des faisceaux hertziens.

Les distances franchissables, par les systèmes de transmission hertzienne, peuvent atteindre 100 km. Pour couvrir des distances plus importantes, il faut disposer de relais, passifs ou actifs. Les relais passifs sont utilisés dans les zones où le relief est important ; il s'agit de simples réflecteurs utilisés pour guider l'onde, par exemple pour suivre une vallée. Les relais actifs nécessitent une infrastructure plus complexe, le signal recueilli est remis en forme, amplifié puis retransmis. Les faisceaux hertziens utilisent les bandes de 2 à 15 GHz et autorisent des débits de 140 Mbit/s.

Les faisceaux hertziens sont sensibles aux perturbations atmosphériques et aux interférences électromagnétiques. La fiabilité d'une infrastructure hertzienne repose sur l'existence de canaux de secours qu'ils soient hertziens ou filaires.

Les liaisons infrarouges et lasers constituent un cas particulier des liaisons hertziennes. Elles sont généralement utilisées pour interconnecter des réseaux privés, sur de courtes distances, de l'ordre de quelques centaines de mètres.

Les liaisons satellitaires

La nécessité de disposer de stations relais rend difficile la réalisation de liaisons hertziennes à très grande distance, notamment pour les liaisons transocéaniques. C'est pourquoi, dès les années

© Dunod – La photocopie non autorisée est un délit

1960, on s'est orienté vers l'utilisation de satellites relais. Ce n'est qu'avec l'apparition de porteurs capables de satelliser sur des orbites d'environ 36 000 km qu'il a été possible de réaliser des liaisons permanentes avec des satellites fixes par rapport à un observateur terrestre (satellite géostationnaire). Ces satellites ont une vitesse angulaire de rotation identique à celle de la Terre sur elle-même, ce qui correspond à une période de révolution de 23 h 56', ils sont dits **géosynchrones**. L'orbite équatoriale est de 42 164 km, soit une altitude exacte au-dessus de la Terre de 35 800 km.

➤ Principe

Une station terrestre émet vers le satellite un flux d'information (voie montante). Le satellite n'est qu'un simple répéteur, il régénère les signaux reçus et les réémet en direction de la Terre (voie descendante). La figure 2.34 illustre le principe d'une liaison satellitaire.

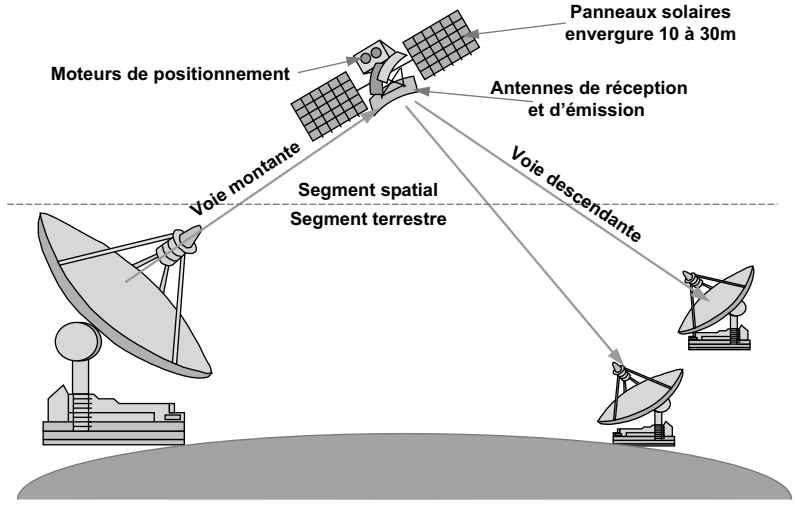


Figure 2.34 Principe d'une liaison satellitaire.

Pour utiliser un satellite comme point nodal d'un réseau terrestre et, non comme simple relais de télécommunication, il est nécessaire d'admettre plusieurs voies montantes. Celles-ci sont alors en compétition pour l'accès au satellite. Plusieurs techniques peuvent être utilisées :

– L'**AMRF** (Accès multiple à répartition de fréquences), elle consiste à diviser la bande de fréquence du satellite en sous-bandes, chacune réservée à une voie de communication.
– L'**AMRT** (Accès multiple à répartition de temps), la porteuse est commune à tous les canaux de communication, mais chaque canal n'en dispose que durant un intervalle de temps limité. Ce mode d'accès nécessite une synchronisation entre les stations.
– L'**AMRC** (Accès multiple à répartition par code), dans cette technique on attribue à chaque voie de communication un code. Les informations codées sont envoyées simultanément, elles sont extraites du flux par décodage.

➤ Les différents types de systèmes satellitaires

Compte tenu des temps de propagation des satellites géostationnaires, des systèmes à orbites plus basses ont été définis. Selon leur orbite, les systèmes satellitaires sont regroupés en trois familles.

On distingue : les orbites stationnaires (GEO), moyennes (MEO) et basses (LEO). La figure 2.35 résume les caractéristiques de ces satellites.

	GEO Geostationary Earth Orbit	MEO Medium Earth Orbit	LEO Low Earth Orbit
Altitude	36 000 km	2 000 à 12 000 km	800 à 2 000 km
Type d'orbite	Circulaire	Elliptique ou circulaire	Elliptique ou circulaire
Plan de rotation	Équatorial	Quelconque	Quelconque
Temps de transmission Terre-satellite	240 ms	110 à 150 ms	Environ 50 ms
Permanence spatiale et temporelle (spatiale : communiquer en tout point ; temporelle : en un point à tout moment)	OUI Trois satellites couvrent la Terre (sauf les pôles)	NON (orbite défilante) Constellation de satellites	NON (orbite défilante) Constellation de satellites
Applications	Téléphonie fixe, télévision, transmission de données	Téléphonie mobile, transmission de données	Téléphonie mobile, transmission de données
Débit	Jusqu'à 155 Mbit/s	De 9,6 à 38 kbit/s	De 2,4 kbit/s à 155 Mbit/s

Figure 2.35 Synthèse des caractéristiques des différents systèmes de satellites.

La figure 2.36 représente les deux modes orbitaux des systèmes de satellites.

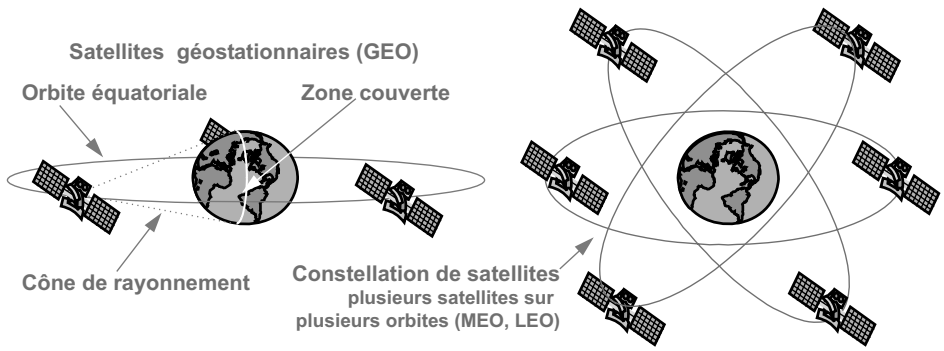


Figure 2.36 Les différents systèmes satellitaires.

La partie de droite illustre un système GEO. En orbite équatoriale, avec un cône de rayonnement de 120°, trois satellites suffisent pour couvrir la Terre, sauf les pôles. Les satellites géostationnaires permettent de réaliser :

– des réseaux de diffusion (radiodiffusion, télévision) ;
– des liaisons point à point ;
– des liaisons à haut débit (bande passante de 500 MHz).

© Dunod – La photocopie non autorisée est un délit

Ces satellites ont un temps de propagation important (environ 240 ms). En raison de la consommation d'énergie nécessaire à leur maintien sur leur orbite, leur temps de vie est limité de 10 à 15 ans. L'énergie motrice est embarquée, donc limitée, tandis que l'énergie nécessaire au système de télécommunication est fournie par des batteries et panneaux solaires.

La partie de droite de la figure illustre les systèmes MEO et LEO qui, pour assurer une couverture spatiale et temporelle totale, impliquent l'utilisation d'une constellation de satellites, c'est-à-dire plusieurs orbites (permanence spatiale) et sur chaque orbite plusieurs satellites (permanence temporelle).

2.4 CONCLUSION

Les caractéristiques intrinsèques des supports conditionnent leur limite d'utilisation. Cependant, les progrès importants réalisés par l'électronique numérique reculent de plus en plus ces limites. Les modes de transformation des informations numériques en signal électrique destiné à être acheminé par le support constituent une voie de recherche importante. Ces différents modes de transformation et d'adaptation de l'information au support font l'objet de l'étude du chapitre suivant.

EXERCICES

Exercice 2.1 Notion de décibels

Utilisé dans tous les domaines de la physique, le décibel[3] est une unité logarithmique qui exprime le rapport d'une grandeur (A) par rapport à une autre grandeur de même nature prise comme référence (B). La relation est de la forme :

$$A/B_{\text{dB}} = 10 \log_{10} (A/B)$$

Compte tenu de cette définition, quel est le rapport en vraie grandeur des rapports A/B exprimés en dB ?

Valeur en décibel	Rapport en nombre naturel
3 dB	
10 dB	
100 dB	
103 dB	
77 dB	

Exercice 2.2 Portée d'une liaison hertzienne

La propagation des ondes électromagnétiques s'effectue selon plusieurs modes qui dépendent de la fréquence (figure 2.37). L'onde d'espace se propage par réflexion sur la Terre et l'ionosphère. L'onde de sol se propage le long de l'écorce terrestre. L'onde directe se propage à vue en ligne droite (la trajectoire est cependant légèrement incurvée).

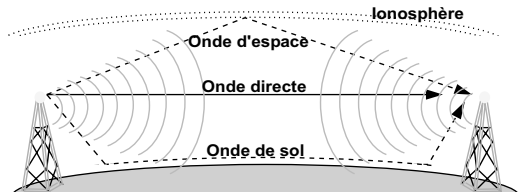


Figure 2.37 La propagation des ondes électromagnétiques (OEM).

Les faisceaux hertziens utilisent la propagation par onde directe ou propagation à vue. Déterminez, en fonction des hauteurs respectives des antennes émission et réception, la portée d'une liaison hertzienne (on supposera la liaison sans obstacle). On vous demande d'en déduire la portée théorique des émetteurs de télévision situés au sommet de la tour Eiffel, pour une antenne de réception située à 8 m du sol (cheminée d'une maison basse).

La tour Eiffel et l'antenne distante seront supposées avoir leur assise à la même altitude.

3. Le décibel, dixième du BEL est à l'origine une unité d'acoustique. La puissance sonore perçue par l'oreille suit une loi logarithme (loi de Fechner). Aussi compte tenu de la dynamique des sons perçus (relation entre le plus faible et plus fort sons perçus) de l'ordre de 10^{13} (13 BEL), il a été convenu de représenter l'intensité sonore par une unité logarithmique le BEL (A. Graham Bell). Le décibel correspond à peu près à la plus petite variation d'intensité sonore perçue par l'oreille.

© Dunod – La photocopie non autorisée est un délit

Exercice 2.3 Puissance de réception

L'antenne supposée ponctuelle d'une borne 802.11 émet avec une puissance de 100 mW (**PIRE**, Puissance isotrope rayonnée équivalente). L'énergie émise étant supposée se répartir sans perte uniformément à la surface d'une sphère dont le rayon correspond à la distance entre la source d'émission et l'antenne de réception, quelle est :

1. la densité de puissance à 10 m (puissance/m^2) ?
2. la puissance reçue par une antenne de réception de surface équivalente supposée de 1 dm^2 ?

Exercice 2.4 Bande passante d'une fibre optique

Une fibre optique multimode à saut d'indice a une ouverture numérique de 0,22 (l'ouverture numérique correspond au sinus de l'angle d'ouverture) et un indice de réfraction du cœur de n_1 = 1,465. Déterminez :

1. la bande passante en bit/s de cette fibre pour une longueur de un km (BP/km) ;
2. $n_{2,}$ sachant que l'ouverture numérique et les indices de réfraction sont liés par la relation :

$$ON = \sqrt{n_1^2 - n_2^2}$$

Exercice 2.5 Conversion de l'expression d'une puissance

Un poste téléphonique émet avec un niveau de puissance de 2 dBmW. Quelle est la puissance émise en mW ?

Exercice 2.6 Caractéristique d'une ligne

Une ligne de communication a une impédance caractéristique Zc = 600 Ω à 800 Hz. Déterminez :

1. le niveau minimal du signal (en volt) à l'extrémité de la ligne si celle-ci est reliée à un modem dont le niveau minimal requis est de – 43 dBmW.
2. l'affaiblissement entre deux points A et B de cette ligne, si l'on mesure entre ces points respectivement 90 mV et 9 mV.

Exercice 2.7 Effet Doppler

La téléphonie mobile utilise une porteuse dans la bande des 1 800 MHz. En supposant que le mobile se déplace dans l'axe du faisceau radio, quelle est l'influence de l'effet Doppler sur la fréquence reçue et quelle sera la déformation de la voix supposée à 10 kHz dans les deux cas suivants :

1. le mobile est embarqué dans une voiture roulant à 100 km/h ;
2. le mobile est embarqué dans un TGV roulant à 300 km/h.

Chapitre 3

Éléments de base de la transmission de données

3.1 INTRODUCTION

Une transmission de données met en œuvre les calculateurs d'extrémité et des éléments d'interconnexion dont les appellations et fonctions sont codifiées (figure 3.1) :

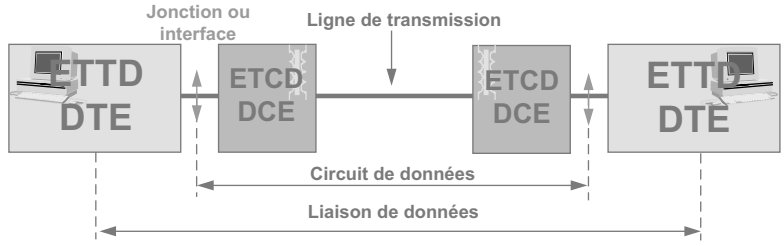


Figure 3.1 Constituant de base d'une liaison de données.

On distingue :

– Les équipements terminaux (*End system*) ou **ETTD** (Équipement terminal de traitement de données), appelés aussi **DTE** (*Data Terminal Equipment*), ce sont les calculateurs d'extrémité. Ces calculateurs sont dotés de circuits particuliers pour contrôler les communications (contrôleur de transmission). L'ETTD réalise la fonction de contrôle du dialogue.

– Des équipements d'adaptation ou **ETCD** (Équipement terminal de circuit de données), ou **DCE** (*Data Circuit Equipment*), qui réalisent l'adaptation entre les calculateurs d'extrémité et le support de transmission. Ces éléments remplissent essentiellement des fonctions électroniques, ils assurent un meilleur transport sur la ligne de transmission. Ils modifient la nature du signal, mais pas sa signification.

– La jonction qui constitue l'interface entre ETTD (DTE) et ETCD (DCE) permet à l'ETTD de gérer l'ETCD afin d'assurer le déroulement des communications (établissement du circuit, initialisation de la transmission, échange de données et libération du circuit).
– Le support ou ligne de transmission, élément passif mais essentiel de la liaison, dont l'étude a fait l'objet du chapitre précédent.

Ce chapitre est consacré à l'étude des bases théoriques de la transmission de données. Les caractéristiques des adaptateurs (ETCD) sont liées à l'organisation fonctionnelle et physique des échanges. Après l'étude de ces différentes organisations, nous examinerons comment est réalisée l'adaptation du signal aux supports. Ce dernier point nous conduira à distinguer deux modes physiques de transmission : la transmission dite en bande de base (*Baseband Transmission*) et la transmission par transposition de fréquence ou large bande (*Broadband Transmission*).

3.2 L'ORGANISATION FONCTIONNELLE ET PHYSIQUE DES ÉCHANGES

3.2.1 L'organisation des échanges

La transmission d'information entre deux correspondants peut être unidirectionnelle (l'échange n'a lieu que dans une seule direction), on parle alors de **liaison simplex** (figure 3.2). Chaque correspondant ne remplit qu'une fonction, il est émetteur (source) ou récepteur (puits ou collecteur).

Si les correspondants peuvent, alternativement, remplir les fonctions d'émetteur et de récepteur, la liaison est dite : liaison à l'**alternat** ou *half duplex*. Le temps mis par les systèmes pour passer d'une fonction à l'autre est appelé temps de retournement. Ce temps peut être important, de l'ordre de quelques dixièmes de seconde.

Lorsque l'échange peut s'effectuer simultanément dans les deux sens, sur des voies distinctes ou sur la même voie par utilisation de techniques spécifiques comme le multiplexage fréquentiel[1], la liaison est appelée **bidirectionnelle intégrale** ou *full duplex*.

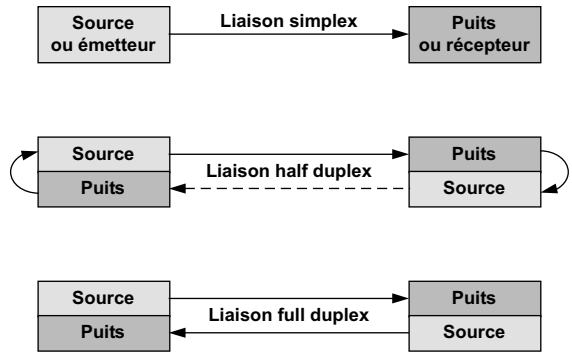


Figure 3.2 L'organisation fonctionnelle des échanges.

1. Le multiplexage fréquentiel consiste à utiliser une fréquence différente pour chaque voie de communication (voir chapitre 5).

3.2.2 L'organisation physique

Transmission parallèle, transmission série

L'information élémentaire à transmettre est le mot (8, 16, 32 ... *n* bits). En interne, les calculateurs transfèrent les données via un bus : un fil par bit. Un bus transmet simultanément tous les bits d'un même mot machine, la transmission est dite transmission parallèle. La communication entre machines peut se réaliser de même. Cependant, la transmission parallèle soulève de nombreux problèmes techniques ; pour des distances importantes, on lui préfère la transmission série : les bits sont transmis successivement sur un support unique.

➤ Transmission parallèle

La transmission parallèle (figure 3.3) est caractérisée par un transfert simultané de tous les bits d'un même mot. Elle nécessite autant de conducteurs qu'il y a de bits à transmettre et un conducteur commun (liaison asymétrique) ou autant de paires de conducteurs si la masse n'est pas commune (liaison symétrique).

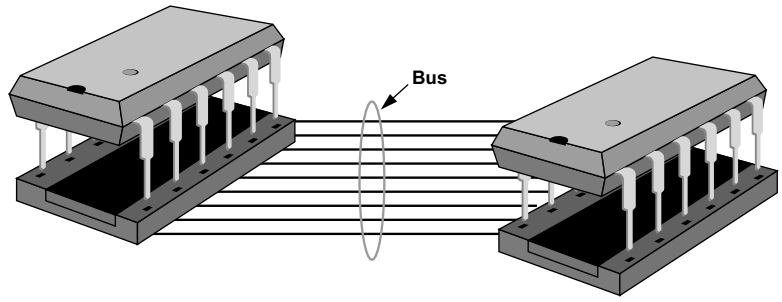


Figure 3.3 La transmission parallèle.

La transmission parallèle est très performante en terme de débit. Elle est utilisée pour des liaisons entre un calculateur, ses périphériques et ses unités de calcul esclaves. Par exemple, l'interface **HiPPI** (*High Performance Parallel Interface*) définit un mode de transmission entre un calculateur et ses périphériques, elle offre un débit de 800 Mbits/s. Elle utilise un câble de 50 paires dont 32 sont utilisées pour la transmission de données (transmission parallèle par mot de 32 bits). HiPPI est limitée à 25 m.

La transmission parallèle pose de nombreuses difficultés dont les principales sont le rayonnement des conducteurs l'un sur l'autre (diaphonie[2]) et la différence de vitesse de propagation entre les différents conducteurs (*Delay Skew*) qui nécessitent la réalisation d'une électronique coûteuse.

Un coût élevé (nombre de conducteurs) et une distance franchissable limitée par la désynchronisation du train de bits (*Delay Skew)* réservent la transmission parallèle aux liaisons de processeur à processeur ou d'hôte à hôte (ordinateur central). Des techniques apparentées sont mises en œuvre dans les réseaux locaux.

© Dunod – La photocopie non autorisée est un délit

2. Voir chapitre 2, *Les supports de transmission.*

➤ Transmission série

En transmission série (figure 3.4), tous les bits d'un mot ou d'un message sont transmis successivement sur une même ligne.

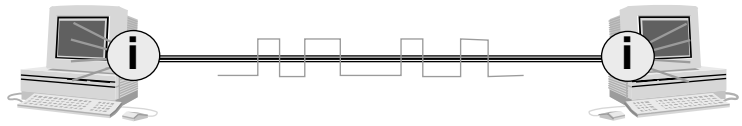


Figure 3.4 La transmission série.

Dans les calculateurs, les données (bits) sont traitées en parallèle (bus). La transmission série nécessite une interface de conversion pour sérialiser les bits en émission (conversion parallèle/série) et les désérialiser en réception (conversion série/parallèle). La transmission série n'utilise, pour la transmission des données, que deux conducteurs. D'un coût moins élevé, elle est adaptée aux transmissions sur des distances importantes.

➤ Comparaison

Si on désigne par **temps bit** le temps d'émission d'un bit sur le support, et en considérant que ce temps est identique pour la transmission parallèle et série de la figure 3.5, on constate qu'il faut seulement trois temps bit pour transmettre le mot « ISO » en transmission parallèle, alors que la transmission série nécessite huit temps bit pour transmettre la seule lettre « O ».

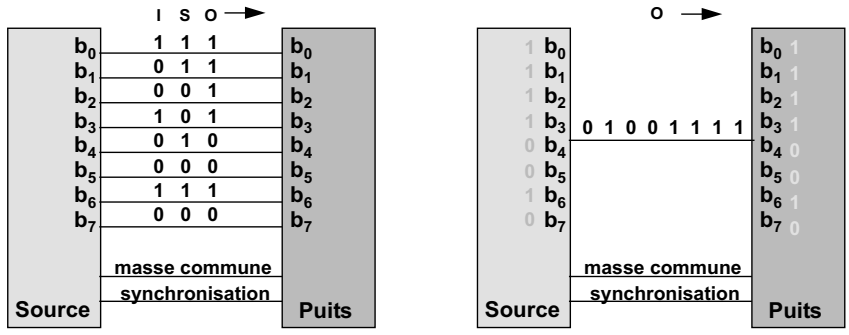


Figure 3.5 **5** – Transmission parallèle, transmission série.

Transmission asynchrone, transmission synchrone

Les bits sont émis sur la ligne à une certaine cadence. Cette cadence est définie par une horloge dite horloge émission. Pour décoder correctement la suite de bits reçus, le récepteur doit examiner ce qui lui arrive à la même cadence que celle de l'émission des bits sur le support. Les horloges récepteur et émetteur doivent « battre » en harmonie.

Il ne suffit pas que les horloges battent au même rythme, encore faut-il que les instants d'analyse des niveaux électriques sur la ligne soient les mêmes pour les deux éléments ; ils doivent être en phase. L'opération qui consiste à asservir l'horloge de réception sur celle d'émission s'appelle la **synchronisation** (figure 3.6). Selon le mode de synchronisation de l'horloge du récepteur sur celle de l'émetteur, on distingue deux types de transmission : les transmissions asynchrones et les transmissions synchrones.

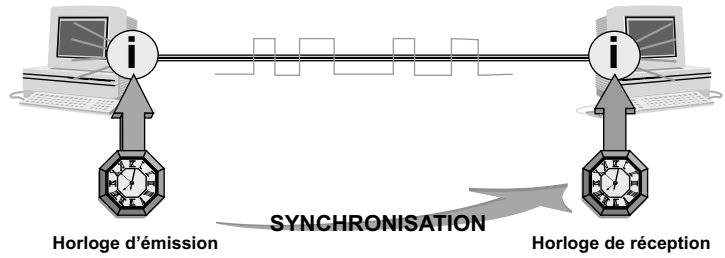


Figure 3.6 Principe de la synchronisation.

Dans les transmissions asynchrones les horloges sont indépendantes, tandis que dans les transmissions synchrones on maintient en permanence une relation de phase stricte entre les horloges émission et réception.

➤ Notion d'horloge

La synchronisation des différentes horloges mises en œuvre dans les systèmes de transmission est l'une des préoccupations principales des concepteurs de systèmes de transmission. Les dérives d'horloge et, par conséquent, les pertes de synchronisation sont, aujourd'hui, les principales causes des pertes de données et des erreurs de transmission dans les réseaux.

Les bits sont émis au rythme de l'horloge locale de l'émetteur que nous supposons stable. L'horloge du récepteur est supposée fonctionner à la même cadence ou fréquence (nombre d'instants significatifs par seconde identique). Cependant, rien ne permet de garantir sa stabilité. La fréquence varie, on dit que l'horloge dérive. En admettant que lors de la réception du premier bit, l'horloge du récepteur soit parfaitement calée sur l'horloge d'émission (synchronisée), la dérive de l'oscillateur local du récepteur fait que quelques bits plus tard, l'instant significatif de lecture est sur le bit suivant ou précédent selon le sens de la dérive. En admettant (hypothèse simplificatrice) que l'instant d'interprétation du signal reçu corresponde au front descendant de l'horloge de réception, la dérive illustrée figure 3.7 (dérive positive) montre que, du fait de cette dernière, le cinquième bit est omis. Une erreur de transmission est apparue.

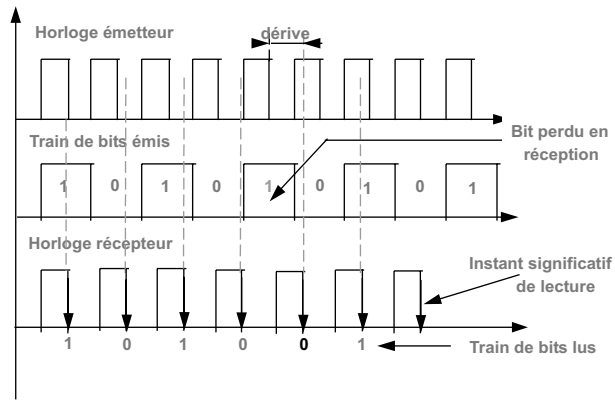


Figure 3.7 La dérive de l'horloge réception occasionne la perte d'un bit.

© Dunod – La photocopie non autorisée est un délit

Le signal de synchronisation peut être transmis sur un lien spécifique (figure 3.8) ou déduit du train binaire. La première méthode, plus complexe et plus onéreuse, est utilisée par les opérateurs de télécommunication pour transmettre la synchronisation aux différents éléments du réseau (réseau de synchronisation).

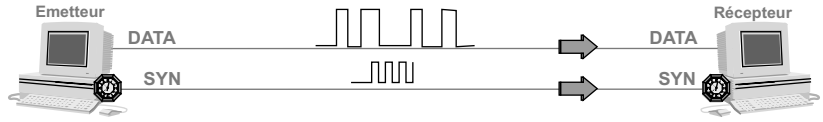


Figure 3.8 La transmission du signal de synchronisation.

En général, une liaison utilise les deux modes. Localement, entre l'ETTD source et ETCD source, la synchronisation est transmise sur un lien spécifique. Sur la liaison distante, entre les deux ETCD (DCE), le signal d'horloge n'est pas directement transmis. C'est l'ETCD destination qui, à partir du train binaire reçu, déduira l'information de synchronisation et la transmettra à l'ETTD destination (figure 3.9).

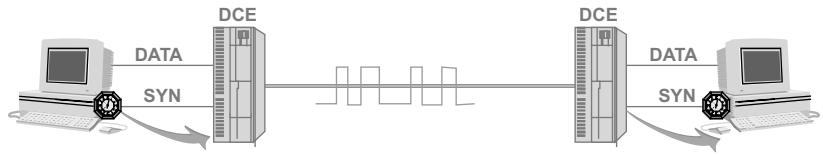


Figure 3.9 La transmission de la synchronisation sur une liaison informatique.

La figure 3.10 montre le principe de l'asservissement de l'oscillateur local à partir des signaux binaires reçus.

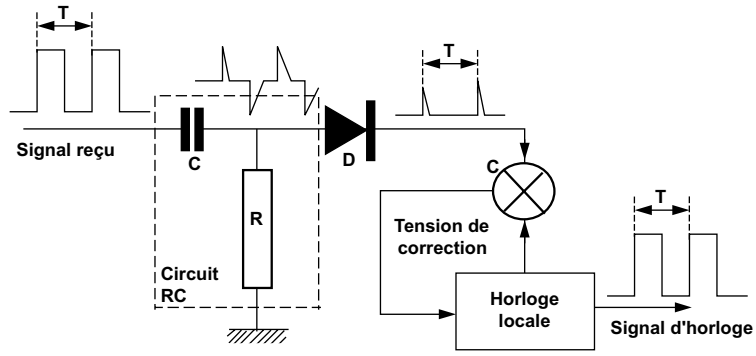


Figure 3.10 Principe d'asservissement de l'horloge du récepteur.

Lorsque les systèmes terminaux sont reliés *via* un réseau de transport, c'est ce dernier qui fournit aux systèmes d'extrémité l'horloge de référence (figure 3.11).

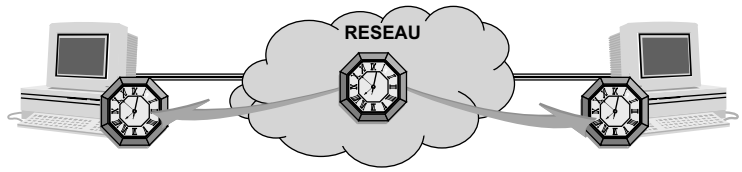


Figure 3.11 La synchronisation des horloges locales sur l'horloge réseau.

➤ Transmission asynchrone

Dans les transmissions asynchrones, les horloges émetteur et récepteur sont indépendantes. Cependant pour assurer une lecture correcte des bits reçus, l'émetteur envoie, avant toute suite binaire significative, un signal spécifique d'asservissement (synchronisation initiale de l'horloge). Après cette opération, l'horloge de réception est libre, elle dérive. L'intervalle de temps pendant lequel la dérive est tolérable et autorise un décodage correct de la séquence binaire est faible, il n'autorise que la transmission d'une courte séquence binaire : le caractère.

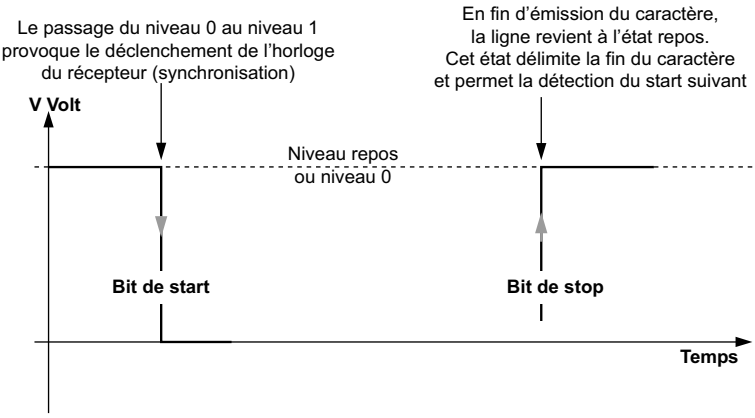


Figure 3.12 Principe de la synchronisation en transmission asynchrone.

En transmission asynchrone, les caractères émis sont donc précédés d'un signal de synchronisation : le **bit de start**. Entre chaque caractère, pour garantir la détection du bit de start suivant, la ligne est remise à l'état zéro. Ce temps de repos minimal varie de un à deux temps bit, il constitue le ou les **bits de stop** (figure 3.12). Le niveau de repos de la ligne ou niveau zéro est fixé à un certain potentiel (V) et non pas au zéro électrique pour ne pas confondre un zéro binaire avec une rupture de la ligne. Cette tension de repos signale aux systèmes que les terminaux sont actifs.

Le bit de start et celui ou ceux de stop servent de délimiteur de caractères (figure 3.13). Les transmissions asynchrones s'effectuent selon un ensemble de règles régissant les échanges (protocole). On distingue deux types de protocoles asynchrones (figure 3.14) :

– Les protocoles en mode caractère : la transmission a lieu caractère par caractère. L'intervalle de temps qui sépare chaque caractère peut être quelconque (multiple de la fréquence d'horloge).

© Dunod – La photocopie non autorisée est un délit

– Les protocoles en mode bloc : les caractères sont rassemblés en blocs. L'intervalle de temps entre l'émission de deux blocs successifs peut être quelconque (multiple de la fréquence d'horloge).

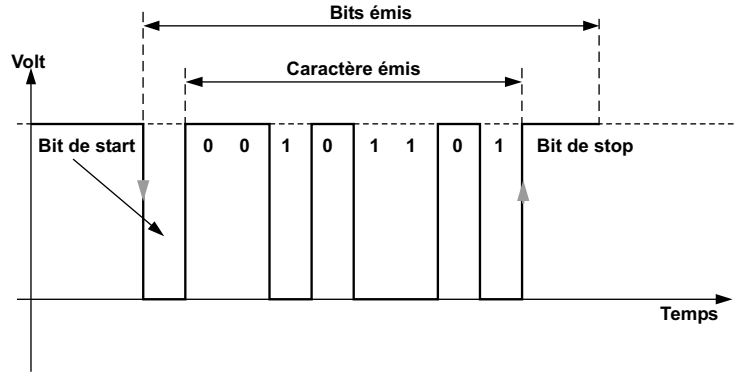


Figure 3.13 Le caractère asynchrone.

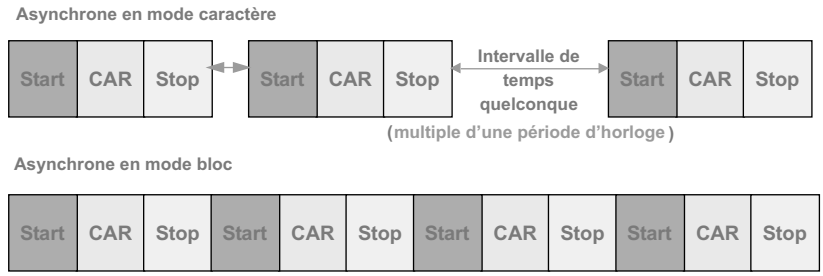


Figure 3.14 Mode caractère et mode bloc.

Le principe des protocoles de transmission sera étudié au chapitre suivant. Les principaux protocoles asynchrones sont :

– **XON-XOFF**, protocole orienté caractère, le terminal réactive la ligne quand il est prêt à émettre (XON), il la désactive quand il n'a plus de données disponibles (XOFF) ;
– **X-Modem**, protocole orienté bloc, les caractères sont regroupés en blocs. Ce protocole du domaine public met en œuvre des techniques de détection et reprise sur erreur ;
– **Y-Modem**, protocole orienté bloc, les blocs de données sont suivis de code de détection d'erreur. Aucune reprise sur erreur n'est assurée ;
– **Z-Modem**, protocole orienté bloc, il met en œuvre des mécanismes de détection et de reprise automatique sur erreur ;
– **SLIP** (*Serial Line Internet Protocol*), protocole orienté bloc. Très simple, SLIP n'effectue que la délimitation des blocs ;
– **PPP** (*Point to Point Protocol*) protocole orienté bloc, PPP effectue la délimitation des blocs et la détection d'erreur.

➤ Transmission synchrone

En transmission synchrone, la synchronisation des horloges émission et réception est maintenue en permanence entre l'émetteur et le récepteur. Il est alors possible de transmettre des blocs de taille importante. Pour maintenir la synchronisation, des signaux spécifiques sont émis durant les silences de l'émetteur (bourrage de ligne).

Si la synchronisation de lecture des bits est maintenue par ce procédé (synchronisation bit), il n'en est pas de même de la frontière entre chaque caractère. Celle-ci est délimitée en transmission asynchrone par les caractères de start et de stop, mais ces caractères sont évidemment absents de la transmission synchrone. Afin de cadrer la lecture des bits sur une frontière d'octet, chaque bloc transmis est précédé d'une séquence de synchronisation spécifique dite synchronisation caractère. La synchronisation caractère est réalisée par reconnaissance dans le train binaire d'une séquence binaire prédéfinie. Lorsque cette séquence est reconnue par le récepteur, celui-ci se cale alors sur une lecture de 8 bits en 8 bits du flot de bits pour lire un flux d'octets (figure 3.15). Cette séquence binaire ou **fanion** sert aussi de délimiteur de début et de fin de bloc, c'est elle qui est utilisée, en l'absence d'émission, pour maintenir la synchronisation bit et par conséquent la synchronisation caractère.

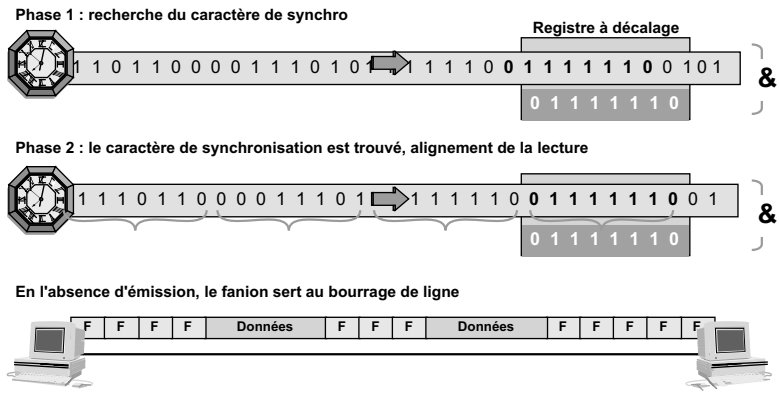


Figure 3.15 Principe de la synchronisation caractère.

Les principaux protocoles synchrones sont :

– **BSC**, *Binary Synchronous Communication* (BULL) ;
– **SDLC**, *Synchronous Data Link Control* (IBM) ;
– **HDLC**, *High Level Data Link Control* (ISO) ;
– **PPP**, *Protocol Point to Point*, ce dernier est aussi un protocole asynchrone (IETF).

Mode de transmission électrique

Les zéros ou les uns sont différenciés par un niveau électrique différent. Selon la manière dont l'information binaire est traduite en impulsions électriques, on distingue deux modes de fonctionnement.

© Dunod – La photocopie non autorisée est un délit

➤ Le mode dissymétrique

Dans le mode dissymétrique ou encore asymétrique, l'information d'état est fournie par la différence de potentiel entre le conducteur concerné et un conducteur de retour. Le fil de retour peut être commun à plusieurs fonctions. Ce conducteur commun est souvent désigné sous le terme de **terre de signalisation**. La figure 3.16 représente les variations de potentiel (+*V*, –*V*) autour d'une valeur de référence dite « zéro électrique ».

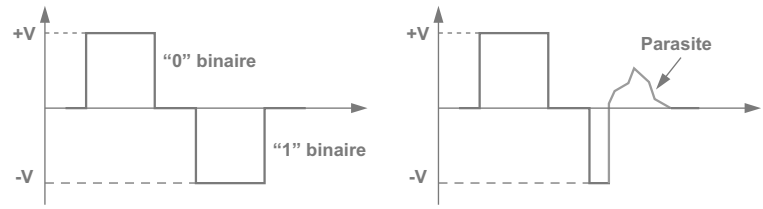


Figure 3.16 La transmission asymétrique.

Ce mode de transmission est simple à réaliser au niveau de l'électronique, il ne nécessite que deux conducteurs mais est très sensible aux parasites.

➤ Le mode symétrique

Dans le mode symétrique appelé aussi **transmission différentielle**, l'information d'état est déduite de la différence de potentiel entre deux conducteurs. La figure 3.17 illustre ce mode de transmission. À l'état repos, chaque conducteur est, par exemple, au potentiel +V volts par rapport à une référence commune, la différence de potentiel entre ces conducteurs est nulle (repère 1). Pour transmettre une information binaire, chacun des conducteurs voit son potentiel évoluer en sens inverse (repère 2 et 3) de la figure 3.17.

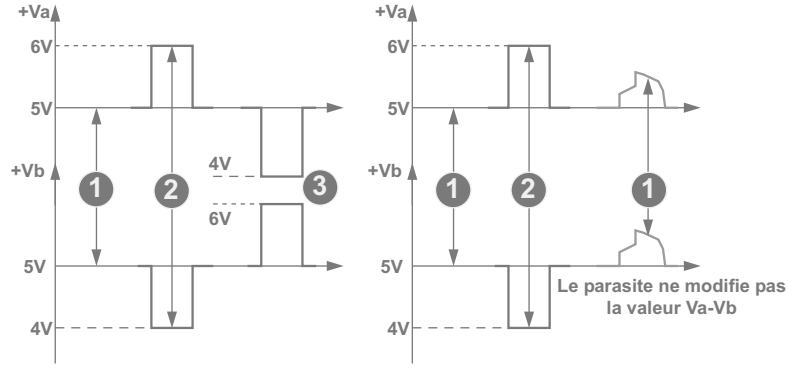


Figure 3.17 La transmission symétrique ou différentielle.

En 1, position de repos, la tension lue (*V*a-*V*b) est nulle. En 2, l'expression *V*a–*V*b = 6 – 4 = 2 V c'est par exemple le niveau 0 ; alors qu'en 3, *V*a–*V*b = 4 – 6 = – 2V pourrait représenter le un binaire. Ce mode de représentation, plus complexe, nécessite certes plus de conducteurs mais un parasite électrique ne modifie pas le niveau relatif. La transmission présente une certaine insensibilité aux parasites.

3.3 LE MODE D'ADAPTATION AU SUPPORT

3.3.1 Généralités

Chaque machine participant à une transmission de données est reliée à la terre locale. Si la terre constitue une référence locale, son potentiel est différent en divers points. De ce fait, réaliser une liaison cuivre directe entre les deux calculateurs provoquerait un courant d'équilibrage qui peut ne pas être supporté par la ligne et qui risque de perturber la transmission. Ce problème conduit à distinguer deux références électriques :

– une référence pour la transmission : la terre de signalisation ;
– une référence pour les équipements : la terre de protection.

Cependant, rien ne garantit que dans un équipement les deux terres ne soient pas confondues[3]. Pour pallier ce défaut, on réalise l'isolement galvanique des deux machines par des transformateurs dits *transformateurs d'isolement* (figure 3.18). Ces transformateurs réduisent la bande passante et sont perturbés par la composante continue du signal.

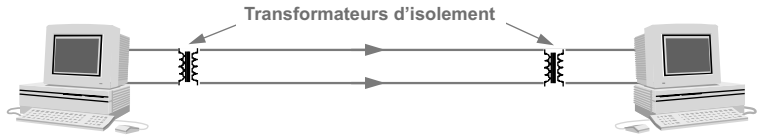


Figure 3.18 L'insertion de transformateurs d'isolement sur le lien de transmission.

La ligne de transmission se comporte comme un filtre passe-bas et les transformateurs insérés comme des filtres passe-haut, la ligne de transmission devient alors un filtre passe-bande (figure 3.19).



Figure 3.19 Le filtre et la liaison de données.

La limitation en fréquence du système conduit à modifier le signal électrique pour l'adapter aux contraintes physiques du système de transmission. Deux types d'adaptation ou techniques de transmission sont envisageables (figure 3.20) :

– La première consiste à modifier légèrement le signal, elle est essentiellement destinée à réduire la composante continue. Cependant, les composantes hautes fréquences étant fortement atténuées, la transmission sera limitée en distance : c'est la transmission en bande de base.
– La seconde translate le spectre du signal à émettre dans une bande de fréquence mieux admise par le système, c'est la transmission large bande.

3. Certaines réglementations nationales imposent la confusion des deux terres.

© Dunod – La photocopie non autorisée est un délit

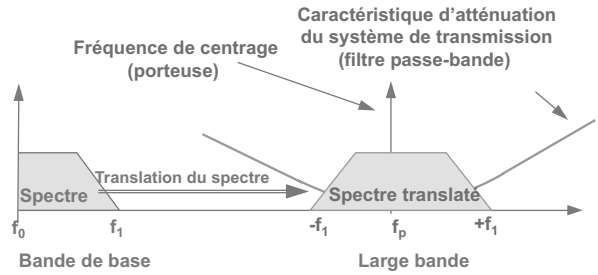


Figure 3.20 Les spectres et les modes de transmission.

3.3.2 La transmission en bande de base

Définitions

On qualifie de systèmes de transmission en bande de base les systèmes qui n'introduisent pas d'écart de fréquence entre les signaux émis et ceux reçus. Cette définition n'exclut nullement des modifications du signal pour mieux l'adapter aux caractéristiques du support de transmission.

On appelle **codage**, l'opération qui fait correspondre à un symbole appartenant à un alphabet, une représentation binaire (codage à la source). On désigne par **transcodage**, ou **codage en ligne**, l'opération qui consiste à substituer au signal numérique (représentation binaire) un signal électrique mieux adapté à la transmission (figure 3.21). Cette transformation est réalisée par un codeur/décodeur appelé Émetteur/récepteur en bande de base (**ERBdB**).

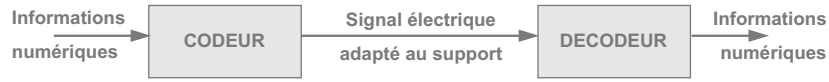


Figure 3.21 Principe du codage en ligne.

Les fonctions d'un codeur/décodeur en bande de base

Le signal numérique, issu du calculateur, présente une composante continue[4] non nulle. Cette composante continue est inutile, elle ne transporte aucune information et provoque un échauffement (effet Joule) des organes d'extrémité (transformateurs d'isolement). Le comportement de filtre passe-bas du système introduit une distorsion de phase qui provoque l'étalement du signal. L'absence de transition, lors de la transmission d'une longue suite de 0 ou de 1, introduit un risque de perte de synchronisation des horloges. Ces différentes considérations conduisent à :

- transformer le signal numérique en un autre, tel que la composante continue soit réduite à son minimum voire supprimée ;
- choisir une méthode de codage pour que le spectre du nouveau signal soit mieux adapté aux caractéristiques du support de transmission ;
- et enfin, pour maintenir la synchronisation, assurer un minimum de transitions, même lors de la transmission de longues séquences de 1 ou de 0.

4. La composante continue représente la valeur moyenne du signal pour un intervalle de temps donné.

En résumé, le transcodage, ou codage en ligne, a essentiellement pour objet de supprimer la composante continue, d'adapter le spectre au canal de transmission et de maintenir la synchronisation de l'horloge de réception.

On utilise essentiellement trois types de codes :

– ceux qui effectuent un codage des 1 et 0 (Manchester...) ;

– ceux qui ne codent que les 1 ou les 0 (bipolaire...) ;

– ceux qui substituent à un ensemble de *n* bits un autre ensemble de *m* bits (nBmB).

Les principaux codes utilisés

En symétrisant le signal par rapport au potentiel de référence (0 volt), on diminue la composante continue. Pour cela, on représente les 1 (ou les 0) par une valeur +*V* et les 0 (ou les 1) par -V. Ce codage élémentaire connu sous le nom de code **NRZ** (*No Return to Zero*, non-retour à zéro) est à la base de tous les codes (figure 3.22). Cependant, le spectre de ce signal est relativement large. Il présente un maximum de puissance à la fréquence zéro, ce qui correspond à une composante continue encore importante.

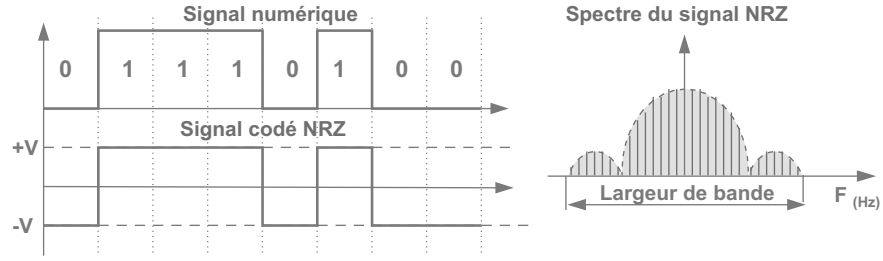


Figure 3.22 Le signal NRZ.

Le codage NRZ symétrise la valeur 1 et la valeur 0 par rapport à un niveau potentiel nul. Cependant, ce codage a une composante continue non nulle et ne présente aucune transition lors de longues séquences de 0 ou de 1.

Avec une transition au milieu de chaque temps bit, le codage Manchester (figure 3.23) remédie à l'absence d'information de synchronisation. La transition est croissante pour les 0, décroissante pour les 1. Le sens des transitions est significatif, ce qui pose des problèmes en cas d'inversion des fils de liaison. Multipliant les transitions, le codage Manchester a un spectre très large, il est utilisé dans les réseaux locaux de type Ethernet sur câble coaxial. La bande passante du support y est importante et l'inversion de fils impossible.

Le codage Manchester différentiel (figure 3.24) résout le problème d'inversion des conducteurs. Chaque transition, au milieu du temps bit, est codée par rapport à la précédente. Si le bit à coder vaut 0, la transition est de même sens que la précédente ($\Delta\varphi = 0$) ; si le bit est à 1, on inverse le sens de la transition par rapport à celui de la précédente ($\Delta\varphi = \pi$). Ce codage résout la plupart des problèmes posés, mais son spectre est relativement large. Il est utilisé dans les réseaux locaux de type Token Ring.

© Dunod – La photocopie non autorisée est un délit

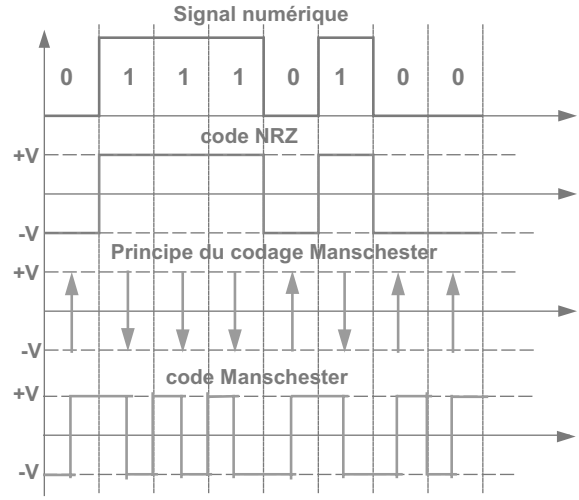


Figure 3.23 La construction du code Manchester.

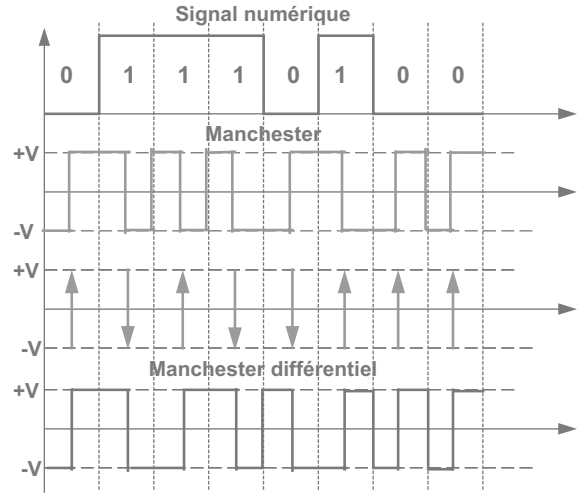


Figure 3.24 Le code Manchester différentiel.

Pour réduire le spectre on peut, à partir du Manchester simple, supprimer une transition sur deux, que celle-ci soit ou non significative, on obtient alors le code dit *Delay Mode* ou Miller (figure 3.25). En appliquant cette règle, on constate que les 1 ont une transition au milieu du temps bit et les 0 pas de transition. Mais un 0 suivi d'un 0 a une transition en fin du temps bit.

Une réduction encore plus significative du spectre peut être obtenue en ne codant qu'un type de bit (par exemple les 1) et en alternant leur polarité pour éliminer la composante continue (figure 3.26). Cependant, lors de longues séquences de 0, ou de 1, il n'y a pas de transition (risque de perte de l'horloge) ; ce code est appelé **code bipolaire**.

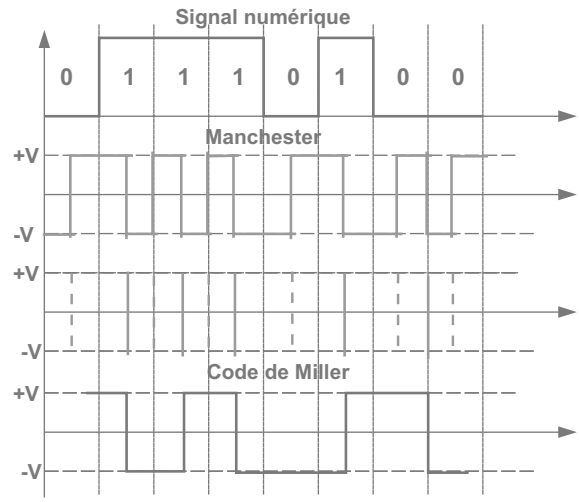


Figure 3.25 Le code Miller.

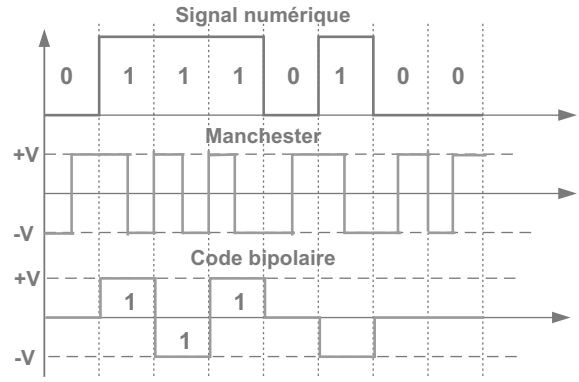


Figure 3.26 Principe des codes bipolaires.

Pour éviter de longues séquences sans transition (suite de 0), les codes **HDBn** (Haute densité binaire d'ordre *n*) sont des codes bipolaires dans lesquels, si le bit de rang $n + 1$ est à zéro, on le remplace par un bit particulier. Ce bit, sans signification numérique (bit électrique), viole la loi d'alternance des bits (**bit de viol**). Ce viol de polarité permet de le distinguer des bits significatifs. Pour respecter la loi d'alternance du codage (composante continue à zéro), les bits de viol doivent alternativement être inversés (comme les bits à 1). De ce fait, les bits de viol peuvent ne plus être en viol par rapport au dernier bit à 1. Dans ce cas, pour éviter la confusion, on introduit un bit supplémentaire, dit **bit de bourrage**, qui rétablit le viol. Ainsi, en HDB3, les séquences de 4 bits à zéro successifs peuvent être codées : B00V ou 000V (V signifiant viol et B bourrage). HDB3 est utilisé dans les liaisons spécialisées louées[5], son principe de construction est illustré en figure 3.27.

5. Les liaisons louées sont des liaisons mises à disposition d'une personne privée par un opérateur public moyennant une redevance d'usage.

© Dunod – La photocopie non autorisée est un délit

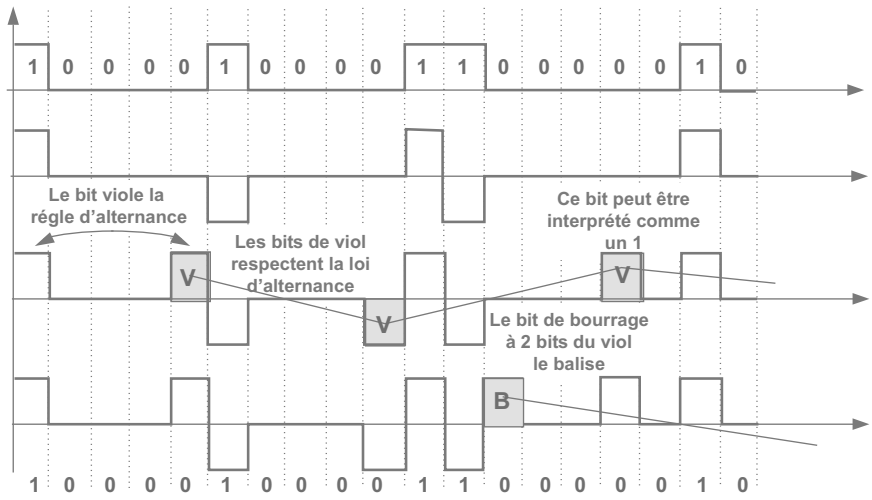


Figure 3.27 Le code HDB3.

La troisième catégorie de code, dit nBmB avec $m > n$ ou encore codage de blocs, est utilisée dans les réseaux dits à haut débit. Dans ces codes, on substitue à une combinaison binaire de n bits une autre combinaison de m bits. Le principe de tels codes est représenté figure 3.28.

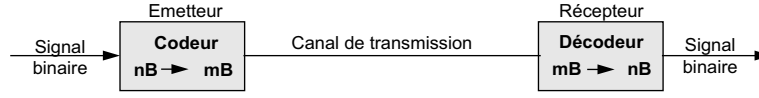


Figure 3.28 Principe du codage nBmB.

Le choix de 2^n valeurs parmi 2^m permet de résoudre facilement les problèmes de composante continue, de largeur de spectre et parfois autorise une autocorrection. Les combinaisons binaires sont choisies de telle manière qu'au moins une transition soit assurée pendant un intervalle de temps t dépendant essentiellement de la stabilité de l'horloge de réception.

Dans le code 4B5B, une séquence de 4 bits binaires est remplacée par une combinaison de 5 bits. Les séquences de 5 bits, ou **symboles**, sont choisies de telle manière qu'aucune ne commence par plus d'un bit à 0 et qu'aucune ne se termine par plus de deux bits à 0. Ainsi, ce code garantit qu'aucune séquence de plus de trois bits consécutifs à 0 ne sera transmise. La figure 3.29 indique les codes valides. Les réseaux de type Ethernet à 100 Mbits/s et **FDDI**[6] utilisent le codage 4B5B. Certaines combinaisons, non représentées, sont utilisées pour représenter les commandes de contrôle du réseau FDDI.

La montée en débit des réseaux locaux sur paires torsadées conduit à rechercher des schémas de codage de plus en plus efficaces, mais aussi plus complexes.

6. FDDI, *Fiber Distributed Data Interface*, réseau local à haut débit voir chapitre 16.

Symbole	Valeur binaire	code 4B/5B	Symbole	Valeur binaire	code 4B/5B
0	0000	11110	8	1000	10010
1	0001	01001	9	1001	10011
2	0010	10100	A	1010	10110
3	0011	10101	B	1011	10111
4	0100	01010	C	1100	11010
5	0101	01011	B	1101	11011
6	0110	01110	E	1110	11100
7	0111	01111	F	1111	11101

Figure 3.29 Le codage 4B5B de FDDI.

Le codeur ou émetteur récepteur en bande de base (ERBdB)

Le signal modifié par l'ERBdB n'a aucune signification binaire directe, ce n'est que la représentation électrique du signal numérique. C'est par abus de langage qu'on appelle cette transmission « transmission numérique », on devrait plutôt parler de transmission en régime impulsionnel. L'opération d'adaptation au support (transcodage ou codage en ligne) est effectuée par des **ERBdB** (figure 3.30) souvent improprement appelés modems bande de base.

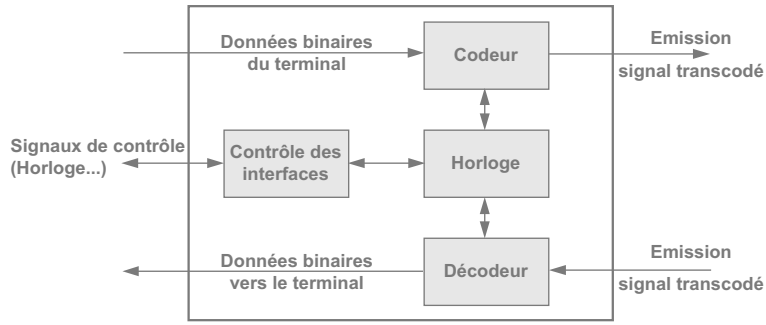


Figure 3.30 Schéma synoptique simplifié d'un ERBdB.

Limitations de la transmission en bande de base

La transmission en bande de base est une technique simple à mettre en œuvre, mais elle est limitée par la bande passante du canal de communication et par le rapport signal sur bruit de celui-ci.

➤ Critère de Nyquist

Notion de rapidité de modulation

Une ligne ou canal de transmission se comporte comme un filtre passe-bas, les différentes composantes sont atténuées (distorsion d'amplitude) et retardées (distorsion de phase). L'une des conséquences les plus visibles est l'étalement du signal. Dans des conditions limites, la fin d'une impulsion transmise peut se confondre avec le début de la suivante. Les circuits électroniques ne peuvent, alors, distinguer deux impulsions successives, il y a interférence de symboles (figure 3.31).

Il existe une relation étroite entre le nombre maximal de symboles (impulsions électriques) que le système peut admettre et la bande passante de celui-ci. Supposons un signal de fréquence F, deux instants significatifs peuvent être distingués. Le premier correspond à la première alternance

© Dunod – La photocopie non autorisée est un délit

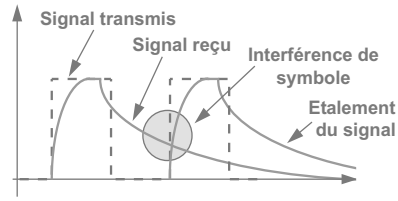


Figure 3.31 L'étalement du signal ne permet plus la récupération d'horloge.

du signal, le second à la seconde. En assimilant chaque alternance à une impulsion électrique, le nombre maximal d'impulsions que peut transmettre un système, par unité de temps, est au plus égal au nombre d'alternances du signal. D'où R_{max}, le nombre maximal d'impulsions, et F_{max}, la fréquence de coupure du système sont approximativement liés par la relation :

$$R_{max} = 2 \cdot F_{max}$$

En toute rigueur il faut tenir compte de toutes les composantes du signal, c'est-à-dire de la bande passante (BP). Aussi le nombre maximal d'impulsions électriques et la bande passante sont liés par la relation[7] appelée **critère de Nyquist** :

$$R_{max} \leqslant 2 \cdot BP$$

où R_{max} désigne le nombre maximal de transitions qu'un système peut supporter, et est appelé **rapidité de modulation**. La rapidité de modulation, grandeur analogue à une fréquence, s'exprime en baud et représente le nombre d'instants élémentaires du signal par unité de temps. La rapidité de modulation est aussi appelée vitesse de signalisation sur le support.

Application au canal téléphonique

Quelle est la rapidité de modulation maximale admissible sur une voie téléphonique caractérisée par une bande passante (*BP*) allant de 300 à 3 400 hertz ?

La bande passante a pour valeur :

$$BP = 3\,400 - 300 = 3\,100 \text{ Hz}$$

La rapidité de modulation maximale est :

$$R_{max} = 2 \cdot \text{BP} = 2 \cdot 3\,100 = 6\,200 \text{ bauds.}$$

Si durant un intervalle de temps significatif, le symbole ne peut prendre que les valeurs 0 ou 1, le débit binaire du canal est égal à la rapidité de modulation. Pour la ligne téléphonique de l'exemple ci-dessus, le débit binaire ne peut excéder 6 200 bit/s.

7. Cette relation est très théorique. En effet, Nyquist a considéré le système comme étant un filtre passe-bande idéal (fréquences de coupure nettes).

➤ Rapidité de modulation et débit binaire

Imaginons que, durant un temps élémentaire, le symbole prenne plusieurs états (figure 3.32), la quantité d'information transportée alors par un symbole est supérieure à 1 bit. Débit binaire et rapidité de modulation sont liés par la relation :

$$D = R \cdot Q = R \cdot \log_2 (1/p)$$

avec D, débit binaire exprimé en bit/s
R, rapidité de modulation en bauds
Q, quantité d'information en bits
p, probabilité d'apparition d'un état.

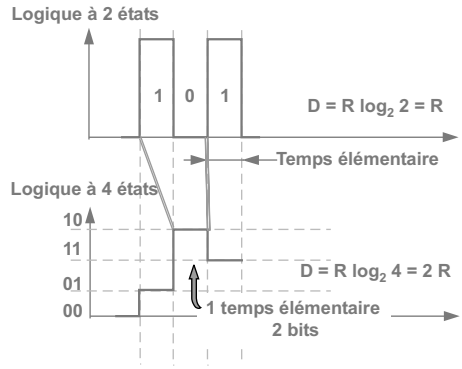


Figure 3.32 Notion de valence du signal.

Si on appelle valence du signal (v) le nombre d'états que peut prendre le signal durant un temps élémentaire ($v = 1/p$). Le débit s'exprime, alors, par la relation :

$$D = R \cdot \log_2 v = 2 \cdot BP \cdot \log_2 v$$

avec D, débit binaire en bit/s
v, valence du signal, valant $1/p$
R, rapidité de modulation

Dans le cas de l'exemple précédent, la rapidité de modulation est égale au débit binaire. Si durant le temps élémentaire, le signal peut prendre plusieurs valeurs, par exemple 4 (figure 3.32), la probabilité d'apparition d'une valeur est de 0,25. Dans ces conditions, le débit du canal est :

$$D = R \cdot \log_2 (1/0{,}25) = R \cdot \log_2 4 = 2 \cdot R \text{ bit/s}$$

Le débit binaire est le double de la rapidité de modulation. C'est ainsi qu'il est possible d'augmenter, sur un canal de transmission de bande passante limitée, le débit binaire. L'opération qui consiste à faire correspondre à un ensemble de symboles binaires (00, 01...000, 001...) un signal électrique spécifique représentatif de cette combinaison est réalisée par un codeur.

© Dunod – La photocopie non autorisée est un délit

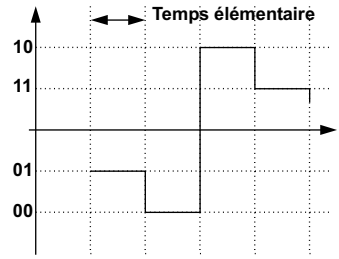


Figure 3.33 Le codage 2B1Q.

La figure 3.33 illustre le codage de la suite binaire 01001011 soit 8 bits en quatre temps d'horloge. Ce type de codage, utilisé sur les liaisons RNIS, est dénommé 2B1Q (2 bits, un symbole quaternaire soit un temps d'horloge, quatre valeurs). En conclusion, rappelons que l'on peut augmenter les possibilités de débit binaire, sur un canal de transmission donné, en agissant sur :

– la bande passante du canal ;
– et/ou la valence du signal transporté.

La bande passante est limitée par le système de transmission (support...). Cependant, on ne peut augmenter indéfiniment le nombre d'états du signal (valence), car les niveaux d'amplitude à discriminer deviennent si faibles qu'ils ne peuvent être distingués du bruit (figure 3.34).

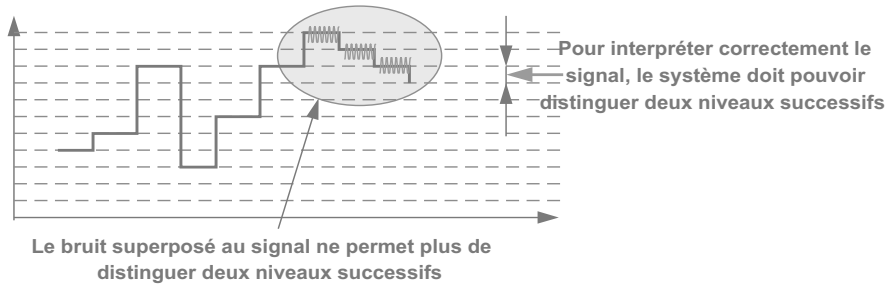


Figure 3.34 La limitation du nombre d'états par le bruit.

➤ Transmission en milieu bruyant

Notion de bruit

Les signaux transmis sur un canal peuvent être perturbés par des phénomènes électriques ou électromagnétiques désignés sous le terme générique de **bruit**. On distingue essentiellement deux types de bruit : le **bruit blanc** et le **bruit impulsionnel**.

Le bruit blanc provient de l'agitation thermique des électrons. Ses composantes (raies de fréquence) sont également réparties dans le spectre des fréquences, d'où son nom. D'amplitude généralement faible, il est peu gênant pour les transmissions.

Le bruit impulsionnel est une perturbation brève qui a pour origine l'environnement physique du canal de transmission (parasite d'origine électromagnétique). D'intensité élevée et d'apparition erratique, il provoque des erreurs portant sur un ensemble de bits.

Rappelons que le rapport entre la puissance du signal transmis et celle du signal de bruit, ou rapport signal sur bruit (*S*/*N* avec *N* pour *Noise* ou SNR, *Signal Noise Ratio*), s'exprime en dB et vaut :

$$S/N_{\text{dB}} = 10 \log_{10} S / N_{\text{(en valeur)}}$$

Capacité d'un canal perturbé, relation de Shannon

Reprenant les travaux de Nyquist, Claude Shannon a montré qu'en milieu perturbé le nombre maximal d'états discernables ou **valence** est donné par la relation :

$$n = \sqrt{1 + \frac{S}{N}}$$

La capacité maximale de transmission d'un canal est alors de :

$$C = 2 \cdot BP \cdot \log_2 n = BP \cdot \log_2 [1 + (S/N)]$$

Application au réseau téléphonique commuté (RTC)

Quelle est la capacité maximale de transmission sur une voie RTC caractérisée par une bande passante de 300 / 3 400 Hz et un rapport signal sur bruit de 1 000 ?

La rapidité de modulation maximale de ce canal est :

$$R_{\text{max}} = 2 \cdot BP = 2 (3\,400 - 300) = 6\,200 \text{ bauds}$$

La capacité de transmission est donnée par la relation de Shannon :

$$C = BP \cdot \log_2 [1 + (S/N)]$$

$$C = (3\,400 - 300) \log_2 (1 + 1\,000) \approx 3\,100 \cdot 3{,}32 \log_{10}(1\,000)$$

$$C = 3\,100 \cdot 3{,}32 \cdot 3$$

$$C = 30\,876 \text{ bit/s}$$

Ce débit maximal théorique correspond aux performances maximales que l'on peut obtenir sur une ligne téléphonique[8].

Conclusion

La bande passante ou encore la rapidité de modulation et le rapport signal sur bruit limitent les possibilités de transmission en bande de base. La transmission bande de base occupe la totalité de la bande passante du canal interdisant l'utilisation des techniques de multiplexage (voir chapitre 5, *Mutualisation des ressources*).

Les techniques dites « bande de base » restent utilisées sur des liaisons spécialisées privées, les liaisons louées par les opérateurs aux entreprises pour se constituer des réseaux privés, les liaisons d'accès aux réseaux des opérateurs et les réseaux locaux d'entreprise. En l'absence de normalisation concernant les ERBdB, il est impératif d'associer ces équipements par paire de même référence et du même constructeur. Les ERBdB couvrent une gamme de débits allant de 2 400 bits/s à 2 Mbit/s. La distance maximale d'utilisation dépend essentiellement de la qualité du support utilisé et du débit en ligne, elle varie de quelques kilomètres à quelques dizaines de kilomètres.

8. Le débit maximal sur ligne téléphonique ordinaire (*BP* = 300 – 3 400 Hz) est aujourd'hui atteint par les modems V.34 bis (33 600 bits/s).

© Dunod – La photocopie non autorisée est un délit

3.3.3 La transmission en large bande

Généralités

En transmission large bande, le spectre du signal numérique est translaté autour d'une fréquence centrale appelée **porteuse**. La translation de spectre résout les deux problèmes posés par la transmission en bande de base : dispersion du spectre (étalement du signal) et la monopolisation du support qui interdit le multiplexage. Elle est réalisée par un organe appelé modulateur. En réception le signal doit subir une transformation inverse, il est démodulé. Le modem, contraction de **mod**ulation/**dém**odulation, est un équipement qui réalise la modulation des signaux en émission et leur démodulation en réception (figure 3.35).

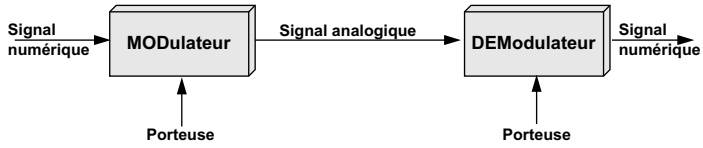


Figure 3.35 La transmission analogique.

Principe de la modulation

La dégradation du signal impulsionnel de la bande de base est rapide, la distance franchissable est limitée à quelques kilomètres. Le signal sinusoïdal est plus résistant, d'où l'idée de substituer au signal impulsionnel, un signal sinusoïdal et de modifier l'un de ses paramètres en fonction du signal numérique d'origine : c'est la **modulation**. Un signal sinusoïdal est de la forme :

$$u = A_0 \sin(\omega_0 t + \varphi_0) \text{ avec } \omega_0 = 2\pi f_0$$

Sur ce signal, on peut faire varier (figure 3.36) :

– l'amplitude A_0, c'est la modulation d'amplitude (**ASK**, *Amplitude Shift Keying*) ;
– la fréquence f_0, c'est la modulation de fréquence (**FSK,** *Frequency Shift Keying*) ;
– la phase φ_0, c'est la modulation de phase (**PSK,** *Phase Shift Keying*).

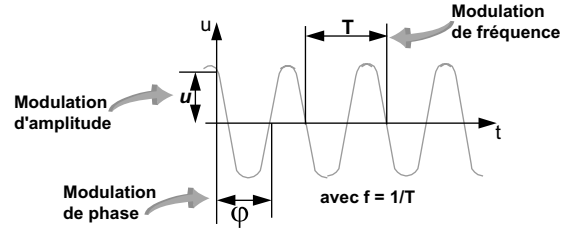


Figure 3.36 Le signal sinusoïdal et la modulation.

➤ La modulation d'amplitude

La modulation d'amplitude établit une correspondance entre l'amplitude d'un signal sinusoïdal et la valeur d'un signal numérique. Les variations d'amplitude du signal modulé sont alors l'image

du signal modulant. Pour retrouver le signal d'origine (signal numérique), il suffit d'interpréter l'enveloppe du signal modulé (amplitude). C'est la démodulation (figure 3.37).

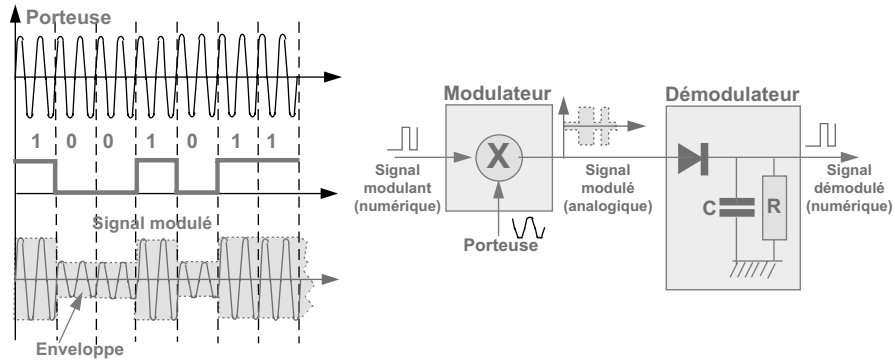


Figure 3.37 Principe de la modulation d'amplitude.

Soit S_0, le signal source ou signal à transmettre, supposé sinusoïdal de fréquence f_0, son spectre est représenté par une seule raie, et P_p le signal modulé ou **porteuse** supposé lui aussi sinusoïdal.

Soit S_m le signal en sortie du modulateur, il comprend une partie de la porteuse (modulation d'amplitude avec porteuse) et un signal égal au produit du signal modulant et de la porteuse, ce signal est de la forme :

$$S_m(t) = kp_p(t) + S_0(t) \cdot P_p(t)$$

où $S_0 = \mathrm{S}_0 \cos \omega_0 t$ est le signal modulant
$P_p = P_p \cos \omega_p t$ est le signal porteur
k est un coefficient dépendant du système

$$S_m(t) = k\, P_p \cos \omega_p t + P_p S_0 \,(\cos \omega_p\, t \cdot \cos \omega_0\, t)$$

En posant $k\, P_p = A_p$, et $P_p S_0 = 2\, M_0$ on écrit :

$$S_m = \mathrm{A}_p \cos \omega_p\, t + 2\, M_0 \,(\cos \omega_p\, t \cdot \cos \omega_0\, t)$$

Ce qui peut s'écrire en développant :

$$S_m = A_p \cos \omega_p\, t + M_0 \cos\,(\omega_p - \omega_0)\, t + M_0 \cos\,(\omega_p + \omega_0)\, t$$

Le signal résultant comporte trois raies de fréquence, le signal porteur ou porteuse (A_p) à la fréquence f_p et le signal modulé (M_0) avec ses deux raies l'une à $f_p - f_0$ et l'autre à $f_p + f_0$. Remarquons qu'après modulation, l'espace de fréquences utilisé est le double de celui du signal modulant mais centré autour du signal porteur, c'est la transposition de fréquence (figure 3.38).

D'une manière générale, le spectre transposé d'un signal de largeur de bande $[f_1, f_2]$ avec $f_2 > f_1$, s'étend de $f_p - f_2$ à $f_p + f_2$, il est centré autour de f_p, fréquence du signal translateur ou porteuse. Chaque demi-spectre ou bande latérale contient l'intégralité de l'information à transmettre. Aussi, pour réduire la largeur de bande et la dispersion du spectre, certains équipements n'utilisent qu'une

© Dunod – La photocopie non autorisée est un délit

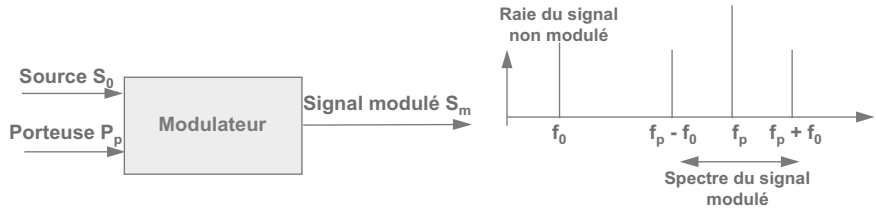


Figure 3.38 Le spectre du signal modulé en amplitude.

seule des deux bandes latérales (**BLU**, Bande latérale unique). La porteuse, nécessaire à la démodulation, est régénérée par le récepteur.

L'amplitude étant représentative de l'information, la modulation d'amplitude est très sensible aux bruits parasites, elle n'est utilisée qu'en combinaison avec la modulation de phase.

➤ La modulation de fréquence

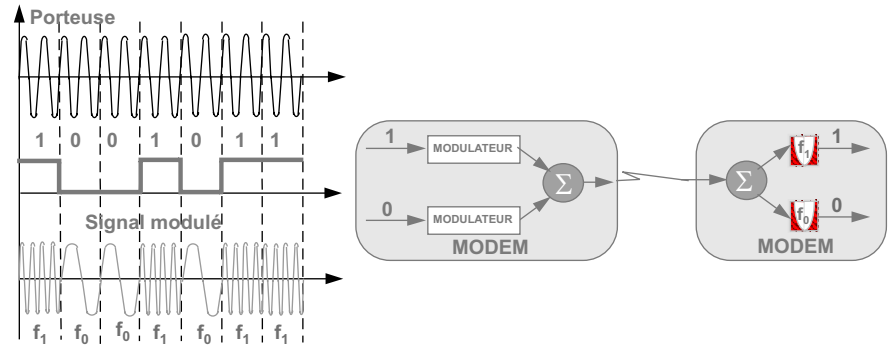


Figure 3.39 Principe de la modulation de fréquence.

Dans ce type de modulation, on associe à une valeur binaire (0,1, ou 01,10...) une fréquence particulière (figure 3.39). En réception, un filtre permet la restitution de la valeur binaire d'origine. La technique de la modulation de fréquence est particulièrement simple à mettre en œuvre. Elle est très résistante aux bruits, mais la grande largeur du spectre du signal résultant la limite aux faibles débits.

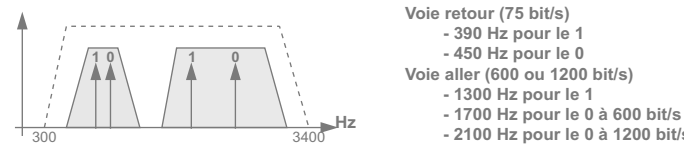


Figure 3.40 Le spectre du modem V.23.

Le modem V.23 utilisé notamment par le Minitel est conçu pour fonctionner sur ligne téléphonique ordinaire (bande passante 300-3 400 Hz). Il permet de réaliser des liaisons *full duplex* asymétriques (la voie aller et la voie retour ont des débits différents). La figure 3.40 indique les fréquences affectées à chaque valeur binaire.

➤ La modulation de phase

En modulation de phase, on associe une valeur binaire à un signal dont la phase est fixée par rapport à un signal de référence. Dans la figure 3.41, la valeur binaire 1 est associée à un signal en phase avec le signal de référence, et la valeur binaire 0 à un signal déphasé de 180°. La représentation est bivalente : modulation de phase à deux états ou **BPSK**, *Binary Phase Shift Keying*.

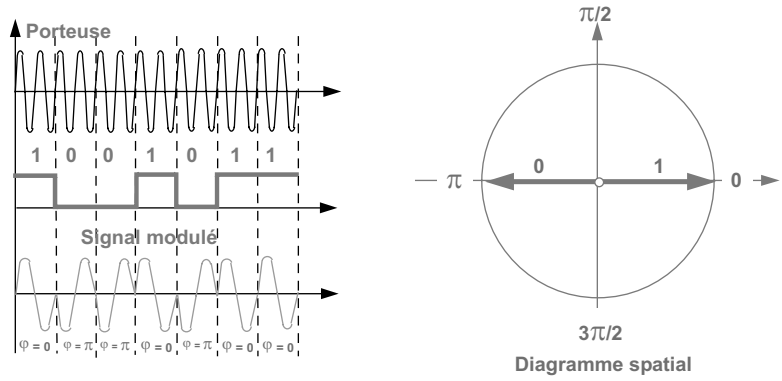


Figure 3.41 Principe de la modulation de phase.

Si le procédé est simple en émission, il est plus complexe en réception. En effet, il faut reconstituer une porteuse de référence avec une probabilité non nulle d'inversion de phase, donc d'inversion du décodage. Pour cela, dans ces systèmes, une séquence d'initialisation précède l'envoi de données.

On peut facilement augmenter le nombre d'états représentés. Par exemple, pour une représentation quadrivalente, il est possible d'associer les déphasages φ_n à des valeurs binaires telles que :

$$00 \Rightarrow \varphi_1 = 0° \qquad 10 \Rightarrow \varphi_3 = \pi$$
$$01 \Rightarrow \varphi_2 = \pi/2 \qquad 11 \Rightarrow \varphi_4 = 3\pi/2$$

Cette technique est limitée par l'erreur de phase introduite par le bruit (figure 3.42).

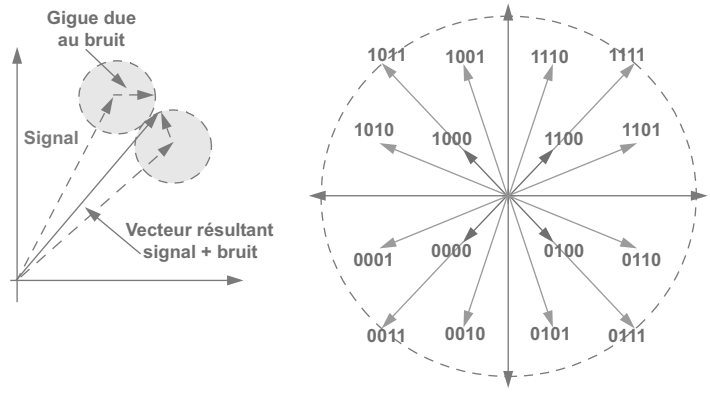


Figure 3.42 Principe de la modulation MAQ (MAQ16) et ses limitations.

© Dunod – La photocopie non autorisée est un délit

On peut aussi combiner la modulation de phase et la modulation d'amplitude, on obtient des schémas de modulation complexes mais très efficaces. Ce type de modulation appelé modulation en amplitude à porteuse en quadrature (**MAQ**, ou **QAM** *Quadrature Amplitude Modulation*) résiste bien au bruit et autorise des débits élevés avec une rapidité de modulation relativement faible.

La figure 3.42 représente le diagramme spatial d'un schéma de modulation à 16 états (MAQ16). Remarquons que les niveaux d'amplitude significatifs de deux vecteurs voisins sont différents. Ce type de codage rend possible, en réception, l'estimation du symbole le plus vraisemblable et améliore la résistance aux erreurs.

Les modems de la dernière génération peuvent mettre en œuvre des codages jusqu'à 64 états, autorisant ainsi des débits élevés avec une rapidité de modulation faible. Par exemple, la modulation MAQ32 définit une modulation à 32 états. Pour un débit effectif de 9 600 bits/s la rapidité de modulation n'est que de :

$$D = R \log_2 (1/p)$$

où p, probabilité de réalisation de l'information, vaut $p = 1/32$. Soit, compte tenu que $\log_2 32 = 5$ ($2^5 = 32$) :

$$R = D/\log_2 32 = 9\,600/5 = 1\,920 \text{ bauds.}$$

3.3.4 Les liaisons *full duplex*

Les liaisons *full duplex* (figure 3.43) peuvent être réalisées simplement par l'utilisation de deux voies de communications distinctes (liaisons 4 fils) ou par mise en œuvre de techniques spécifiques (liaison 2 fils).



Figure 3.43 Les liaisons *full duplex* à 4 et 2 fils.

En transmission large bande, il est facile de réaliser une liaison *full duplex* sur deux fils par simple décalage des porteuses comme, par exemple dans le modem V.23 (figure 3.40). En transmission bande de base, cette technique est inapplicable. L'émetteur et le récepteur sont raccordés à la liaison 2 fils par un système hybride permettant le passage de 4 en 2 fils, ce système n'isole pas parfaitement les deux voies. Une partie du signal d'émission se retrouve sur la voie de réception (écho local et écho distant). Le système annuleur d'écho évalue la valeur de ces signaux parasites et les ajoute en opposition de phase au signal reçu. La figure 3.44 illustre ce système.

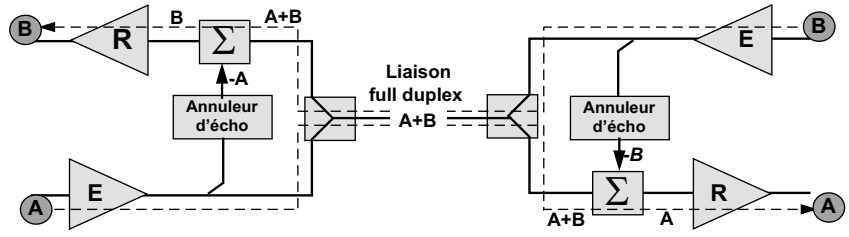


Figure 3.44 Les système hybride de passage de 4 à 2 fils.

Les systèmes à annulation d'écho sont aussi utilisés dans les modems large bande.

3.3.5 Les dispositifs complémentaires

Les dispositifs d'embrouillage

Les dispositifs d'embrouillage ont pour rôle de modifier les données pour équirépartir la distribution des 0 et des 1. Cette méthode de modification des données à transmettre facilite la récupération du rythme d'horloge. Dans les ETCD *full duplex* à annulation d'écho, les techniques d'embrouillage facilitent le discernement des deux voies.

L'embrouillage consiste à assimiler les données à transmettre aux coefficients d'un polynôme (D_x), à diviser celui-ci par une séquence pseudo-aléatoire (d_x), enfin à transmettre le quotient (Q_x) et le reste (R_x) de cette division[9]. Le récepteur ayant connaissance du diviseur retrouve les données (le dividende D_x) en effectuant l'opération (débrouillage) :

$$D_x = (Q_x \cdot d_x) + R_x$$

Le brouillage en émission et le débrouillage en réception sont réalisés par des registres à décalage de *n* étages comportant une ou plusieurs portes OU exclusifs (figure 3.45).

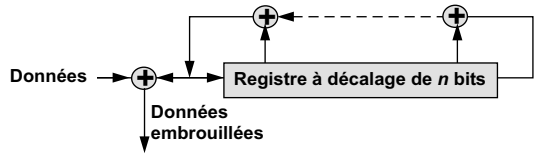


Figure 3.45 Principe d'un embrouilleur.

L'avis V.22 (modem V.22) met en œuvre un circuit embrouilleur/débrouilleur utilisant le polynôme :

$$d_x = 1 + x^{14} + x^{17}$$

L'avis V.32 et V.32 bis utilisent deux polynômes :

– dans le sens appel (celui qui initialise la liaison) $x^{23} + x^{18} + 1$
– dans le sens réponse $x^{23} + x^5 + 1$.

La compression de données et le mode correction d'erreur

Le constructeur américain Microcom, en dotant ses modems de fonctions évoluées (détection et correction d'erreur, compression...), a créé un standard. Les fonctions offertes par les modems Microcom (figure 3.46) sont connues sous le nom de *Microcom Networking Protocol* (**MNP**). Certaines de ces fonctions ont fait l'objet de normalisation. L'avis V.42 pour le contrôle d'erreur entre modems a pour origine MNP 4, alors que l'avis V.42bis pour la compression de données est issu des protocoles MNP2, 3 et 4.

Les fonctionnalités MNP sont de moins en moins supportées par les modems des dernières générations. Cependant pour assurer la compatibilité, certains constructeurs intègrent les fonctions équivalentes normalisées et les fonctions MNP d'origine.

9. La technique de la division polynomiale, utilisée aussi pour la détection des erreurs de transmission, est étudiée au chapitre suivant.

© Dunod – La photocopie non autorisée est un délit

MNP 1	Protocole de correction d'erreur au niveau de l'octet, il n'est plus utilisé aujourd'hui.
MNP 2	Protocole de correction d'erreur au niveau de l'octet en *full duplex*, pour liaison asynchrone en *full duplex* à 2 400 bits/s.
MNP 3	Protocole de correction d'erreur au niveau bit, il utilise le protocole SDLC en *full duplex*. Mis en œuvre dans les liaisons asynchrones (vu des ETTD, le protocole de transmission est asynchrone alors que les modems, ou ETCD, conversent en mode synchrone).
MNP 4	Protocole de correction d'erreur au niveau du paquet. La taille des paquets est variable (*Adaptative Packet Assembly*) en fonction de la qualité de la ligne ; utilisé pour des liaisons asynchrones sur le RTC.
MNP 5	Protocole de correction d'erreur et de compression de données (combinaison du code d'Huffman et du *Run Length Encoding*). Le taux de compression peut atteindre deux.
MNP 6	Semblable à MNP 5, MNP 6 simule une liaison *full duplex* sur une liaison *half duplex*, en mettant en œuvre un procédé de retournement de modem très rapide.
MNP 7	Amélioration du protocole MNP 5 en associant la compression d'Huffman à un algorithme de prédiction, le taux de compression peut atteindre trois.
MNP 8	N'est plus commercialisé.
MNP 9	Protocole de correction d'erreur et de compression de données pour modems asynchrones ou synchrones sur liaison RTC.
MNP 10	Amélioration de MNP 4, MNP 10 autorise l'adaptation dynamique de la taille des paquets et un repli de la vitesse de transmission.

Figure 3.46 Synthèse des protocoles MNP.

Le langage de commande

Hayes, autre constructeur américain de modems (Hayes Microcomputer Products), est connu par l'implémentation dans ses modems d'un langage de commande qui est devenu un véritable standard. Le langage Hayes ne nécessite pas l'utilisation d'un logiciel spécifique pour piloter le modem, c'est l'une des raisons de son succès.

Tant que le modem n'est pas connecté à un équipement distant, il considère que ce qu'il reçoit est une commande et il l'exécute. Lorsqu'il est connecté, il est transparent aux caractères reçus : ce qu'il reçoit, il le transmet. Le langage Hayes, implémenté par de nombreux constructeurs, dans leurs équipements, n'est pas normalisé. Le respect plus ou moins rigide du standard Hayes crée des incompatibilités entre modems, et entre modems et logiciels. Le CCITT (UIT-T) a spécifié un langage de commande pour modem dérivé du langage Hayes.

Les commandes Hayes (figure 3.47) commencent toutes par les 2 lettres AT (attention) suivies d'une lettre qui indique la commande et, éventuellement, de paramètres. La commande ATD 01 46 35 53 99 signifie « composer le numéro 01 46 35 53 99 ».

Les tests de fonctionnement

Lors d'incidents de fonctionnement, il peut être intéressant de localiser l'élément défectueux par simple bouclage des composants sans avoir à se déplacer. La recommandation V.54 du CCITT (UIT-T) définit quatre bouclages (figure 3.48) qui sont :

– le bouclage 1, pontage entre le terminal et le modem (les ETTD et ETCD), permet de tester le fonctionnement de l'ETTD ;

Commandes	Signification	Commentaires
+++	Séquence d'échappement	Permet de revenir en mode commande en cours de communication.
ATA	Answer	Prise de ligne immédiate en réponse.
ATD	Dial	Numérotation automatique, la commande est suivie du numéro et éventuellement de caractères : – T, numérotation en fréquence. – P, numérotation par impulsion. – R, appel en mode retourné. – , (virgule) pause de deux secondes. – ; (point virgule) retour en mode commande après numérotation.
ATE	Echo	Paramétrage de l'écho des commandes : – ATE 0, pas d'écho. – ATE 1, écho des commandes.
ATF	Full	Choix entre half ou *full duplex* : – ATF 0, *half duplex*. – ATF 1, *full duplex*.
ATH	Hang	Raccrocher.
ATM	Monitor	Paramétrage du haut parleur : – ATM 0, pas de haut-parleur. – ATM 1, haut-parleur jusqu'à la connexion. – ATM 2, haut-parleur permanent.
ATO	On Line	Prise de ligne immédiate (correction manuelle).
ATQ	Quiet	Paramétrage des messages : – ATQ 0, émission de messages de compte rendu (OK, ERROR...). – ATQ 1, la carte n'émet aucun message.
ATS		Lecture et écriture des registres : – ATS x?, lecture/affichage du contenu du registre x. – ATS x = nn, écriture de nn dans le registre x.
ATV	Verbal	Sélection du type de messages émis par la carte. – ATV 0, message numérique. – ATV 1, message en clair.
ATX		Extension de message : – ATX 0, message normal. – ATX 1, message étendu
ATZ		Réinitialisation de la carte.

Figure 3.47 Les commandes Hayes.

– le bouclage 2, effectué entre l'ETCD et l'ETTD récepteurs, vérifie l'intégrité de la liaison, modems y compris ;
– le modem local peut être vérifié par le bouclage 3 ;
– le bouclage 4 autorise l'évaluation de la qualité de la liaison (réservé aux lignes à 4 fils).

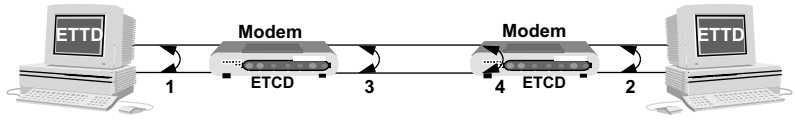


Figure 3.48 Le bouclage des modems.

© Dunod – La photocopie non autorisée est un délit

Les indicateurs de fonctionnement

Les modems sont généralement dotés d'indicateurs d'état qui permettent d'en contrôler le fonctionnement. Ces indicateurs numérotés selon une convention que nous étudierons un peu plus tard (voir figures 3.59 à 3.62) sont les suivants :

– Ali est le témoin d'alimentation du modem.
– 103 visualise l'émission de données.
– 104 indique une réception de données.
– 106 le modem est prêt à émettre.
– 109 le modem reçoit une porteuse (liaison avec un modem distant établie).
– 142 le modem est en cours de bouclage.

3.3.6 Exemples de modem

Synoptique d'un modem

Un modem comprend deux parties, l'émetteur de données ou modulateur et le récepteur de données ou démodulateur. Les fonctions remplies par chaque partie sont symétriques.

Le synoptique du modem représenté figure 3.49 correspond à celui d'un modem synchrone. En fonctionnement asynchrone, les circuits débrouillage et horloge interne ne sont pas en fonction.

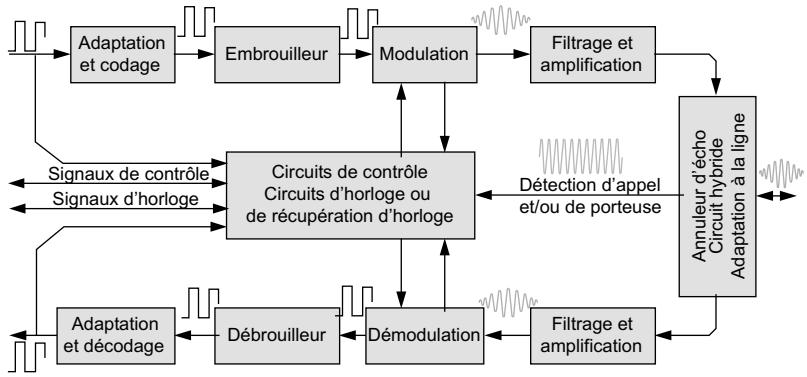


Figure 3.49 Synoptique simplifié d'un modem.

En émission, un codeur fournit les valeurs multiniveaux au modulateur. En réception, la fonction inverse est réalisée. Le dialogue avec le terminal (ETTD) est contrôlé par un circuit spécialisé. Les principales caractéristiques d'un modem sont :

– le mode de travail, bande de base ou large bande (attention, rappelons que c'est par abus de langage qu'on appelle « modem bande de base » un ERBdB) ;
– le type de transmission, asynchrone ou synchrone, certains modems sont susceptibles de travailler dans les deux modes ;
– le débit binaire, les modems modernes testent la ligne et adaptent leur débit aux caractéristiques de celle-ci (bande passante, rapport signal sur bruit) ;

– la rapidité de modulation qui permet de choisir, pour un débit donné, le modem le mieux adapté au support sur lequel il sera utilisé ;
– le support pour lequel il est prévu (RTC, liaison louée analogique à 2 ou 4 fils...) ;
– le mode de fonctionnement (*simplex*, *half duplex*, *full duplex*) ;
– le type de codage utilisé (ERBdB) ;
– le type de jonction (interface ETTD/ETCD).

Aucune normalisation n'a été édictée pour les ERBdB, ceux-ci doivent donc s'utiliser par paire de même référence et du même constructeur.

Le modem V.34

Le modem V.34 a introduit la notion d'adaptation du débit aux conditions de la ligne en cours de transmission. Le V.34 teste la qualité de la ligne en permanence et réalise l'adaptation des débits par pas de 2 400 bits/s. Le modem choisit en conséquence la meilleure porteuse parmi les neuf proposées par la norme. La figure 3.50 illustre les bandes de fréquences pouvant être utilisées (229–3 673 Hz), on remarquera que celles-ci peuvent excéder la bande traditionnelle de 300–3 400 Hz.

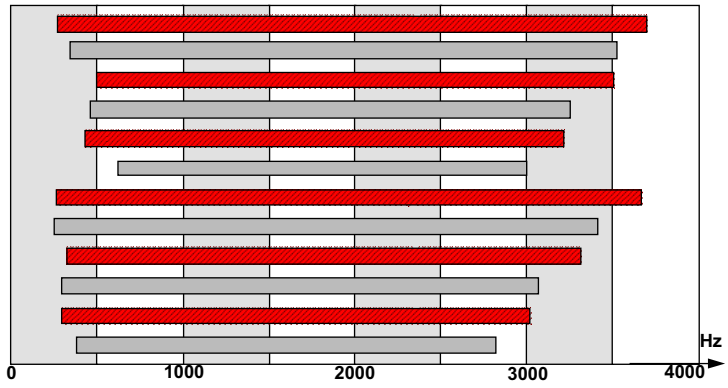


Figure 3.50 Les bandes de fréquences définies par la norme V.34.

Le modem V.34 a introduit la transmission asymétrique avec basculement. En mode *full duplex*, le canal de transmission est divisé en deux sous-canaux, l'un lent et l'autre rapide. Le basculement des canaux est automatique, le modem offrant le plus de bande passante à la source lui soumettant le plus de données. Un canal spécifique est dédié aux données de service (test de lignes...). À l'origine définie pour un débit de 28 800 bits/s, la norme V.34 a évolué pour offrir des débits pouvant aller jusqu'à 33 600 bits/s (V.34+).

Le modem V.90

Le débit d'un modem est limité par le rapport signal sur bruit de la liaison. La numérisation des réseaux a réduit considérablement le bruit de transmission. La liaison d'abonné en cuivre (boucle locale en téléphonie) et surtout l'opération de numérisation du signal (bruit de quantification) sont les principales sources de bruit. Si l'une des extrémités est directement reliée en numérique au réseau, le bruit global de la liaison est réduit et le débit peut être supérieur. C'est le principe du

© Dunod – La photocopie non autorisée est un délit

modem V.90, un modem dissymétrique. En effet, la liaison abonné vers **ISP** (*Internet Service Provider*) subit l'opération de quantification principale source de bruit, alors que le sens ISP vers abonné n'en subit pas. Le débit ISP vers abonné pourra, de ce fait, être supérieur au débit abonné/ISP (figure 3.51).

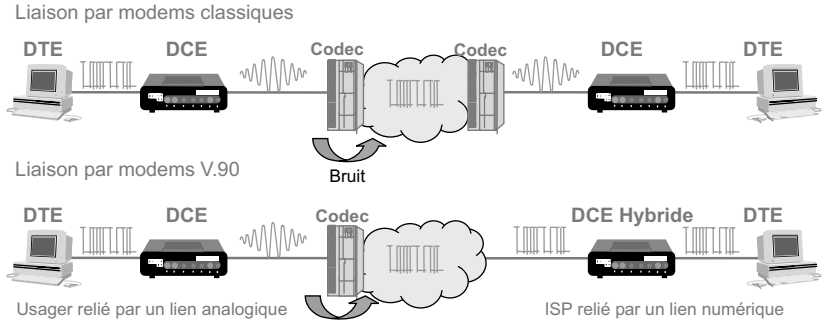


Figure 3.51 Le modem classique et le modem V.90.

L'avis V.90 autorise un débit brut de 56 kbits/s dans le sens ISP/usager et seulement de 33,6 kbits/s dans l'autre sens.

3.3.7 Principaux avis du CCITT

La figure 3.52 résume les principaux avis du CCITT (IUT-T).

Les modems les plus utilisés sont :

- V.34, V.32, V.32bis, V.22 et V.22 bis en transmission de données ;
- V.27ter, V.29 pour la télécopie (Fax) ;
- V.23 (Minitel) ;
- V.90, couramment utilisé pour les accès à Internet (modem dissymétrique 33/56 kbits/s) ;
- V.92 qui a remplacé le modem V.90 pour les accès Internet. Il offre en théorie un débit symétrique (56/56) et mémorise l'état de la ligne ce qui autorise des connexions plus rapides.

3.3.8 Comparaison transmission bande de base et large bande

La figure 3.53 compare les signaux et les spectres respectifs des deux modes de transmission. Il convient ici de préciser des termes dont l'emploi est généralement ambigu. Seul, le signal entre le calculateur (ETTD ou DTE) et l'ETCD ou DCE (codeur ou modem) est un signal numérique. Le signal en ligne est une représentation de celui-ci soit par simple codage (bande de base) soit après modulation (large bande). La transmission en large bande est dite analogique et, par abus de langage, la transmission en bande de base est dite numérique.

AVIS	Type modulation	Débit	Mode de transmission	Exploitation	Voie de retour	Support
V.21	Fréquence, 2 états	$\leqslant$ 300 bits/s	Asynchrone	*Full duplex*		RTC LS
V.22	Phase différentielle 4 états	2 400 bits/s 1 200 bits/s	Synchrone Asynchrone	*Full duplex*		RTC LS
V.22 bis	MAQ 16 états	2 400 bits/s 1 200 bits/s	Synchrone Asynchrone	*Full duplex*		RTC LS
V.23	Fréquence 2 états	$\leqslant$ 1 200 bits/s $\leqslant$ 600 bits/s	Asynchrone Synchrone	*Half duplex et full duplex*	optionnel 75 bauds	RTC LS
V.26	Phase différentielle 4 états	2 400 bits/s	Synchrone	*Half duplex et full duplex*	optionnel 75 bauds	LS 4 fils
V.26 bis	Phase différentielle 4 états	2 400 bits/s 1 200 bits/s	Synchrone	*Half duplex* *Full duplex*	optionnel 75 bauds	RTC LS
V.26 ter	Phase différentielle 8 états	2 400 bits/s 1 200 bits/s	Synchrone Asynchrone	*Full duplex*		RTC LS
V.27	Phase différentielle 8 états	4 800 bits/s	Synchrone	*Full duplex*	optionnel 75 bauds	LS 4 fils
V.27 bis	Phase différentielle 8 états	4 800 bits/s 2 400 bits/s	Synchrone	*Half duplex* *Full duplex*	optionnel 75 bauds	RTC LS
V.27 ter	Phase différentielle 8 états	4 800 bits/s 2 400 bits/s	Synchrone	*Half duplex* *Full duplex*	optionnel 75 bauds	RTC LS
V.29	MAQ 16 états	9 600 bits/s 7 200 bits/s 4 800 bits/s	Synchrone	*Full duplex*		LS 4 fils
V.32	MAQ 4 ou 32 états	9 600 bits/s 4 800 bits/s 2 400 bits/s	Synchrone Asynchrone	*Full duplex*		RTC LS
V.32 bis		14 400 bits/s 12 000 bits/s 9 600 bits/s 7 200 bits/s 4 800 bits/s	Asynchrone Synchrone	*Full duplex*		
V.33	MAQ	14 400 bits/s 12 000 bits/s	Synchrone	*Full duplex*		LS 4 fils
V.34	MAQ 16, 32 ou 64 états	de 28 800 à 2 400 bits/s par bond de 2 400 bits/s	Synchrone Asynchrone	*Half duplex et full duplex*		LS

Figure 3.52 La synthèse des principaux avis de IUT-T.

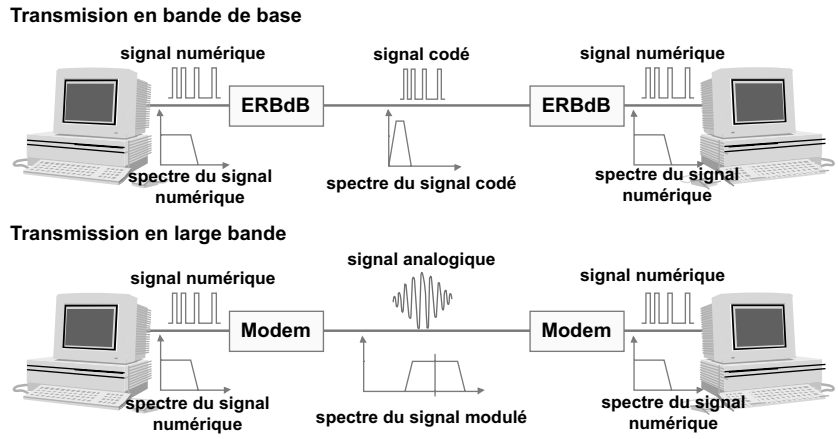


Figure 3.53 La comparaison des modes de transmission.

3.4 LA JONCTION DTE/DCE OU INTERFACE

3.4.1 Nécessité de définir une interface standard

La jonction ETTD-DTE/ETCD-DCE définit un ensemble de règles destinées à assurer la connectivité, le dialogue entre l'ETTD et l'ETCD (activation de la ligne...), la transmission des horloges, le transfert de données et le contrôle de celui-ci (figure 3.54).

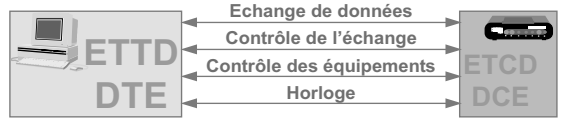


Figure 3.54 L'interface ou jonction ETTD/ETCD.

Une interface ETTD/ETCD spécifie :

– une interface mécanique qui décrit le connecteur physique ;
– une interface électrique qui détermine les niveaux électriques des signaux qui transitent par la jonction ;
– une interface fonctionnelle qui précise les fonctions remplies par telle ou telle broche : le transfert de données, les signaux de commande, les signaux de synchronisation et les masses ;
– enfin, une interface procédurale qui définit les procédures de commande et d'échange.

La normalisation des interfaces émane essentiellement de deux organismes : l'EIA (RS 232, RS 449, RS 422, RS 423A...) et l'UIT (V.24, X.21, X.21bis...). La figure 3.55 présente les principales interfaces normalisées et leurs caractéristiques essentielles.

	Interfaces				
Appellation	**Mécanique**	**Electrique**	**Fonctionnelle**	**Portée**	**Débit nominal**
V.24/RS 232	ISO 2110 DB25	V.28	V.24	12 m	2,4 à 19,2 kbit/s
V.35	ISO 2593 DB34	V.11/V.10	V.24	15 m 10 m	48 à 64 kbit/s 128 à 256 kbit/s
V.36	ISO 4902 37 points	V.11/V.10	V.24	15 m 10 m	48 à 64 kbit/s 128 à 256 kbit/s
X.24/V.11	ISO 4903 DB15	V.11	X.24	100 m 50 m	64 à 1 024 kbit/s 1 920 kbit/s
G.703	ETSI 300.166	G.703	G.703	300 m	2 048 kbit/s
G.703/704	DB9	G.703	G.704	300 m	256 à 1 984 kbit/s

Figure 3.55 Les principales interfaces normalisées.

3.4.2 Les principales interfaces

Les interfaces mécaniques

De nombreux connecteurs ont été définis et associés à des interfaces spécifiques. La figure 5.37 représente les principaux connecteurs utilisés. D'origine Cannon, ils sont plus connus sous les appellations de DB25 pour le connecteur 25 broches, DB15 pour le connecteur 15 broches... que sous leurs appellations officielles attribuées par l'ISO (voir figure 3.55).

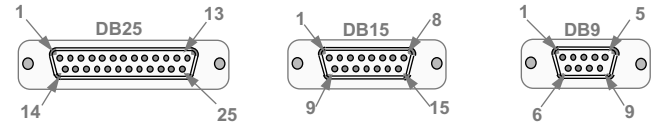


Figure 3.56 Les principaux connecteurs physiques.

La figure 3.56 présente les connecteurs de face, ils sont de type mâle (ceux qui ont des picots). Les micro-ordinateurs sont généralement équipés d'un connecteur DB25 femelle pour la liaison parallèle avec l'imprimante et d'un connecteur DB25 mâle pour la transmission de données. Ce dernier est de plus en plus aujourd'hui remplacé par un connecteur DB9.

Les interfaces électriques

Les interfaces électriques fixent les niveaux électriques des signaux et leur mode de transmission entre l'ETTD et l'ETCD. Les principaux avis sont :

– l'avis V.28 pour une interface en mode asymétrique (retour commun),
– l'avis V.10 (X.26) qui met en œuvre des niveaux de tension plus en adéquation avec l'intégration des circuits, utilise un mode asymétrique mais différencie la masse ETTD et ETCD,
– enfin, l'avis V.11 (X.27) qui reprend les niveaux électriques de l'avis V.10 mais en mode symétrique.

➤ L'avis V.28

En mode asymétrique (figure 3.57), chaque fonction est matérialisée par un fil. L'information d'état est déduite de la différence de potentiel entre ce fil et la masse commune (terre de signalisation).

© Dunod – La photocopie non autorisée est un délit

Selon les différents niveaux, un courant résiduel peut circuler sur le fil de masse perturbant la transmission.

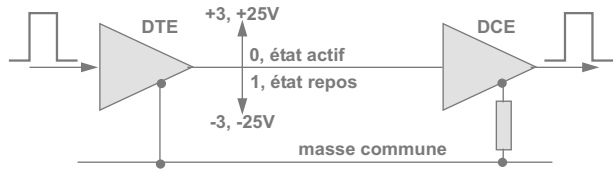


Figure 3.57 L'interface dissymétrique de l'avis V.28.

Les niveaux compris entre +3 V et –3 V ne doivent donner lieu à aucune interprétation, ce qui n'est pas toujours respecté.

L'avis V.10 est mieux adapté aux technologies modernes. Les tensions maximales sont de ±5 V. Les seuils de détection sont réduits à $V \leqslant$ –0,3 V pour le 1 binaire et à $V \geqslant$ +0,3 V pour le 0 binaire.

➤ L'avis V.11

L'avis V.11 (figure 3.58) devrait permettre d'atteindre des débits de l'ordre de la dizaine de Mbit/s sur une distance de quelques mètres (15 m).

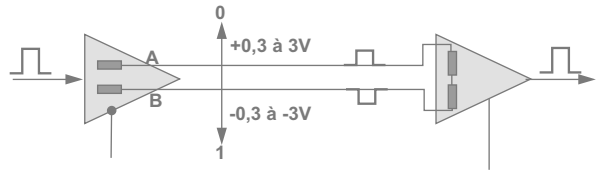


Figure 3.58 L'interface symétrique de l'avis V.11.

Chaque signal est défini par deux fils notés A et B, l'écart de tension maximal est de ±5 V. Les seuils de détection sont définis pour le 1 binaire $V_A - V_B \leqslant$ –0,3 V et $V_A - V_B \geqslant$ +0,3 V pour le 0 binaire.

Les interfaces fonctionnelles

Les interfaces fonctionnelles définissent un ensemble de circuits destinés à établir la liaison physique, la maintenir durant l'échange, assurer le transfert des données, fournir les signaux d'horloge et enfin rompre la liaison en fin d'échange.

➤ L'avis V.24

Description

L'avis V.24 (CCITT 1960, proche de la RS 232C), utilise un connecteur Canon DB25 (25 broches), il spécifie quatre types de signaux :

– des signaux de masse ;
– des signaux de transfert de données ;
– des signaux de commande ;

– des signaux de synchronisation.

Ceux-ci sont répartis en deux familles de circuits, chaque circuit ou signal est identifié par un numéro :

– les circuits de la série 100, la série 100 spécifie 39 circuits qui s'appliquent aux transmissions de données synchrones et asynchrones, aux services de transmission de données sur lignes louées à 2 ou à 4 fils en exploitation point à point ou multipoint ;
– les circuits de la série 200 pour les appels automatiques (devenu obsolète).

Les figures 3.59 à 3.62 fournissent la signification des principaux circuits et leur correspondance pour les interfaces V.24 du CCITT et RS 232C de l'EIA.

CCITT V..24				EIA RS-232 C		
Les circuits de masse						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
101	1	TP	Terre de protection	PG	Protective groung	
102	7	TS	Terre de signalisation	SG	Signal ground	Est utilisé comme retour commun en cas de jonction dissymétrique (V.24) ou comme potentiel de référence dans les jonctions symétriques (V.10, V.11, V.35).

Légende : ***Code*** N° attribué au circuit.
Br. N° de la broche utilisé sur un connecteur DB25.
Abr. Abréviation couramment utilisée pour désigner le circuit.

Figure 3.59 Les signaux (circuits de masse) de la série 100.

CCITT V..24				EIA RS-232 C		
Les circuits de transfert						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
103	2	ED	Émission de données	TD	Transmitted data	Circuit par lequel l'ETTD transmet à l'ETCD les données.
104	3	RD	Réception de données	RD	Receive data	Circuit par lequel l'ETCD transmet à l'ETTD les données reçues

Figure 3.60 Les signaux (circuits de transfert) de la série 100.

Les signaux sont définis de manière identique du côté ETTD et ETCD, la liaison est dite **droite en point à point**. Ceci implique un comportement différent des équipements. En effet, le circuit 103, émission de données, vu de l'ETTD, correspond à une réception de données vue de l'ETCD. La figure 3.63 illustre une liaison complète, seuls les circuits les plus utilisés ont été représentés.

Les circuits d'horloge ont été volontairement omis. Les transmissions de données en mode asynchrone ne nécessitent aucune horloge. Les transmissions en mode synchrone exigent une référence d'horloge. L'horloge est transmise par un circuit spécifique. Elle peut être fournie par l'ETTD (DTE) ou l'ETCD (DCE). En réception, c'est toujours le DCE qui fournit l'horloge (circuit 115). En émission, l'horloge peut être fournie par le ETTD (circuit 113) ou l'ETCD (circuit 114), l'ETTD doit être paramétré en fonction du choix réalisé. En général, on préfère l'horloge de l'ETCD (DCE), le rythme de l'émission est ainsi adapté aux capacités du support (réseau).

© Dunod – La photocopie non autorisée est un délit

	CCITT V..24			EIA RS-232 C		
Les circuits de commande						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
105	4	DPE	Demande pour émettre	RTS	Request to send	Circuit par lequel l'ETTD demande à l'ETCD de s'apprêter à recevoir des données, par le 103, pour les émettre sur la ligne.
106	5	PAE	Prêt à émettre	CTS	Clear to send	Circuit par lequel l'ETCD signale qu'il est prêt à émettre sur la ligne les données qui lui parviendront de l'ETTD.
107	6	PDP	Poste de données prêt	DSR	Data set ready	L'ETCD indique qu'il est en fonction et prêt à recevoir les commandes en provenance de l'ETTD.
108	20	TDP	Terminal de données prêt	DTR	Data terminal ready	108-1 Connecter le poste de données à la ligne, circuit par lequel l'ETTD demande à l'ETCD de se connecter à la ligne. 108-2 Équipement terminal de données prêt, circuit par lequel l'ETTD signale qu'il est en fonction, l'ETCD se met à son tour en fonction et se connecte à la ligne.
109	8	DS	Détection signal de ligne	CD	Data carrier detect	Signale que le signal reçu par l'ETCD est conforme à ce qu'il attendait
110	21	QS	Qualité du signal de données	SQD		Signale que des erreurs ont été reçues sur la voie de données.
111	23		Sélection débit ETTD		DTE rate	Est utilisé pour piloter l'ETCD lorsque celui-ci possède plusieurs débits.
112	18		Sélection débit ETCD		DCE rate	Indique à l'ETTD le débit binaire choisi quand l'ETCD possède plusieurs débits.
120	19		Demande à émettre		Request to send	Idem au 105, utilisé quand la voie de retour est utilisée.
125	22	IA	Indicateur d'appel	RI	Ring Indicator	Utilisé pour les appels automatiques, indique à l'ETTD que l'ETCD vient de détecter une demande de connexion.

Figure 3.61 Les signaux (circuits de commande) de la série 100.

	CCITT V..24			EIA RS-232 C		
Les circuits de synchronisation						
Code	**Br**	**Abr.**	**Signification**	**Abr.**	**Signification**	**Fonction**
113	24		Horloge émission de l'ETTD		DTE timing	La base de temps pour le codage des signaux est fournie par l'ETTD
114	15		Horloge émission de l'ETCD		DCE timing	La base de temps est fournie par l'ETCD
115	17		Horloge réception de l'ETCD		Receive timing	La base de temps est fournie par l'ETCD
Les circuits de test						
140	21		Commande de test			Mise en œuvre de la boucle de test 2
141	18		Commande de test			Mise en œuvre de la boucle de test 3
142	25		Indication de test			Indique le bouclage et signale l'interdiction d'émettre des signaux.

Figure 3.62 Les signaux (circuits de synchronisation et de tests) de la série 100.

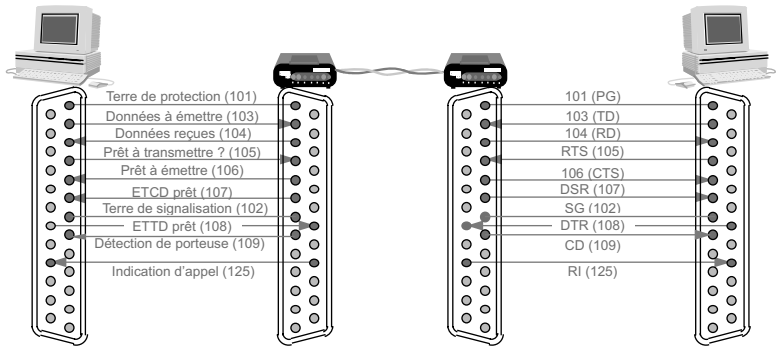


Figure 3.63 Les principaux circuits utilisés dans une liaison V.24.

Exemple de fonctionnement

L'interface ETTD/ETCD véhicule les signaux de contrôle et les données transmises. La procédure d'établissement de la liaison dépend du type de relation : liaison spécialisée, réseau téléphonique commuté avec ou non appel automatique et réponse automatique, liaison synchrone ou asynchrone... La figure 3.64 représente une connexion entre deux correspondants. La liaison est supposée *full duplex* et en mode asynchrone (pas de circuit d'horloge).

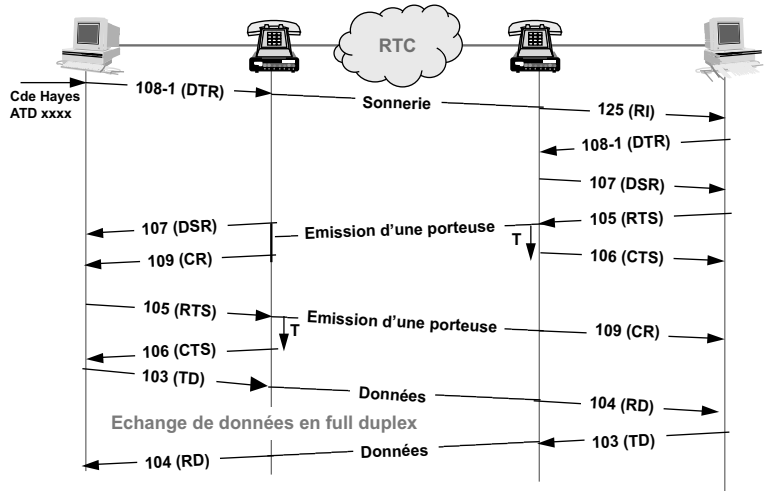


Figure 3.64 Exemple de dialogue ETTD/ETCD.

Les modems appelant et appelé sont sous tension et non connectés à la ligne. L'appelant reçoit la commande Hayes de demande d'appel. Non connecté à la ligne, il exécute la commande, prend la ligne (108-1, DTR ou *Data Terminal Ready*), émet le numéro d'appel du modem distant. Le modem distant, en attente de demande de connexion reçoit l'appel, il l'indique à son ETTD en levant le signal 125 (Indication d'appel ou **RI**, *Ring Indicator*). L'appelé accepte l'appel et demande à l'ETCD de se connecter à la ligne (108-1). La connexion réalisée l'ETCD signale qu'il est connecté à la ligne et prêt à recevoir des commandes (107, DSR ou *Data Set Ready*).

© Dunod – La photocopie non autorisée est un délit

L'ETTD appelé indique alors par le signal 105 (**RTS**, *Request To Send*) à son ETCD de se mettre en état de recevoir des données sur son circuit 103 (**TD**, *Transmitted Data*) afin de les émettre sur la ligne. L'ETCD se met, alors, en position d'émission et signale au distant qu'il va émettre des données par l'émission d'une porteuse (109, **CD** *Data Carrier Detect*). À réception de ce signal, l'appelé sait son appel accepté, il signale à l'ETTD qu'il est connecté à la ligne et prêt à son tour à recevoir des commandes (107, DSR ou *Data Set Ready*). Puis il indique à l'ETTD qu'il reçoit une porteuse du distant et que par conséquent celui-ci est prêt à transmettre. L'appelant procède comme l'appelé, demande à son ETCD de se mettre en position d'émission (105, RTS ou *Request To Send*), l'ETCD envoie une porteuse au distant et, après un délai (T), signale à son ETTD qu'en principe le distant est prêt à recevoir et que lui est prêt à émettre (106, CTS ou *Clear To Send*). L'échange de données peut alors avoir lieu.

Deux situations sont envisageables pour le modem appelé. Celle décrite précédemment correspond à l'utilisation dite 108-1. Le modem doit lever le signal 125 (Indication d'appel ou **RI**), pour que l'appelé décide ou non de monter le signal 108 (prendre la ligne ou **DTR**, *Data Terminal Ready*).

Une autre utilisation correspond à la levée anticipée du signal 108 (108-2), le modem est alors en attente d'appel. Lors de la réception d'un appel, celui-ci décroche automatiquement et signale la connexion par la levée du signal 107. Le signal 125 est alors inutile. En principe, une option de configuration du modem permet de choisir l'un ou l'autre fonctionnement.

Notons que, dans le cas d'une liaison *half duplex*, avant de « lever » le signal 105, l'ETTD vérifie que le signal 109 est « bas », c'est-à-dire, qu'il ne reçoit rien du distant. Supposons le 109 bas, en levant le signal 105, l'ETTD demande à son distant de se mettre en position de réception (109). La liaison étant *half duplex*, le distant est en position de réception. Il ne peut acquitter la demande, c'est pour cette raison que la réponse de l'ETCD à la levée du signal 105 se fait sur temporisation. Ce temps (T) est appelé **temps de retournement** du modem, c'est le temps nécessaire pour passer d'une position d'émission en position de réception et inversement.

Éliminateur de modem

Lorsque l'on désire réaliser une connexion locale entre deux ordinateurs, il serait dommage de mobiliser deux modems pour réaliser la liaison. Un simple câble (figure 3.65) peut être utilisé pour mettre en relation les deux correspondants. Il suffit pour cela de croiser les fils émission et réception, d'où son appellation de câble croisé par opposition au câble droit utilisé pour connecter un ETTD à un ETCD (figure 3.65).

Le schéma de la figure 3.65 représente ce que l'on nomme un éliminateur de modem. Trois fils suffisent (masse, émission et réception). Cependant, si les ETTD gèrent les signaux de commande, il sera nécessaire de compléter le câblage par des bouclages locaux pour simuler le dialogue ETTD/ETCD, on réalise alors un câble appelé **null modem**.

Un équipement est dit avoir un comportement DTE quand il émet les données sur le 103 et les reçoit sur le 104, il est dit DCE dans une configuration inverse (émission sur le 104, réception sur le 103).

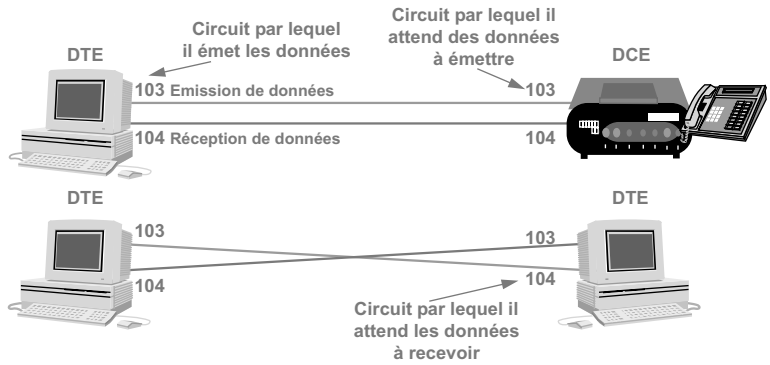


Figure 3.65 Notion de câble droit et de câble croisé.

L'interface d'accès aux réseaux publics

➤ L'interface X.21

Afin d'optimiser l'accès aux réseaux publics de données une nouvelle interface a été définie : l'avis X.21. Cette interface autorise des débits synchrones pouvant atteindre 10 Mbit/s sur quelques mètres et un temps d'établissement de la connexion d'environ 200 à 300 ms contre 3 à 15 secondes pour l'interface V.24.

L'avis X.21 définit l'interface d'accès entre un ETTD et un réseau public de transmission de données (figure 3.66), il fixe les règles d'échange pour :

– l'établissement de la connexion avec un ETTD distant à travers un ou plusieurs réseaux,
– l'échange des données en mode duplex synchrone,
– la libération de la connexion.

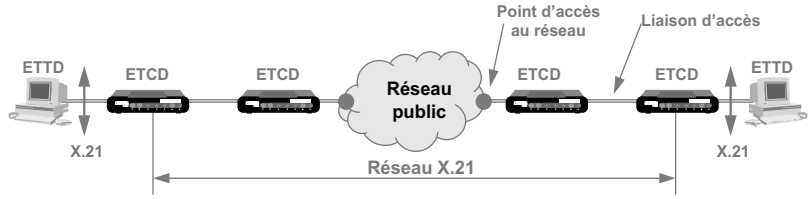


Figure 3.66 Le réseau X.21.

L'avis X.21 prévoit deux modes électriques de fonctionnement. Côté ETCD (modem réseau) seul le mode équilibré peut être utilisé (2 fils par circuits), côté ETTD (modem ETTD) les deux modes sont possibles : le mode équilibré ou le mode non équilibré (retour commun). L'avis X.21 n'utilise que huit circuits, les commandes ne sont pas matérialisées par des tensions sur un circuit spécifié mais par une combinaison de signaux. L'état de l'interface est indiqué par la combinaison des quatre circuits Transmission (T), Contrôle (C), Réception (R) et Indication (I). Le circuit C est activé par le terminal pour émettre l'appel et le circuit I par le réseau pour indiquer la connexion.

Malgré ses avantages, cette interface n'a pas connu un développement important. En effet, l'interface X.21 utilise un connecteur DB15 (ISO 4903) et la plupart des équipements sont équipés

© Dunod – La photocopie non autorisée est un délit

d'un connecteur DB25. Une adaptation a donc été réalisée : l'avis X.21 bis. Il consiste en une simplification de l'interface V.24. L'avis X.21 bis (figure 3.67) décrit l'accès à un réseau public au travers un connecteur DB25 (ISO 2110) ou DB34 (ISO 2593), il organise l'interfonctionnement de l'interface ETTD-ETCD.

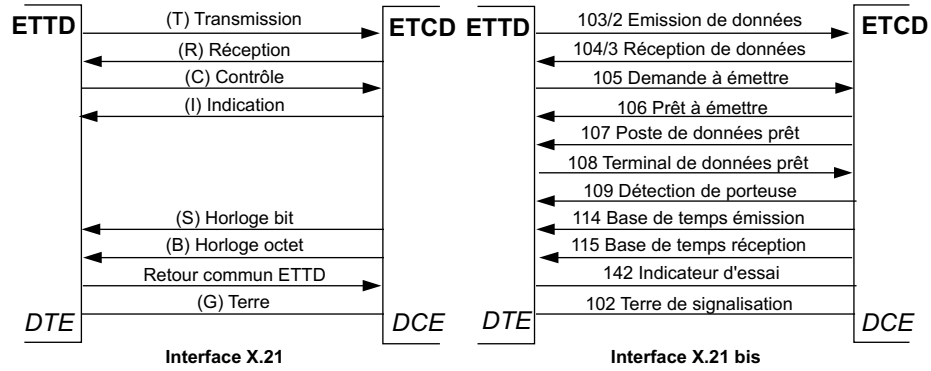


Figure 3.67 L'interface X.21 et X.21bis.

X.21 est une interface de commandes logiques, alors que X.21 bis utilise les signaux fonctionnels de la V.24 dont les niveaux électriques ont été réduits pour tenir compte des tensions supportées par les composants électroniques de type circuit intégré.

➤ L'accès au réseau téléphonique numérique

Les terminaux (téléphone, télécopieur...) des réseaux téléphoniques numériques (**RNIS**, Réseau numérique à intégration de service ou **ISDN** *Integrated Services Digital Network*) sont raccordés à l'interface d'accès au réseau par un connecteur à contacts glissants : le connecteur RJ45 (figure 3.68). Le connecteur RJ45 (*Registered Jack*) est aussi utilisé dans les réseaux locaux.

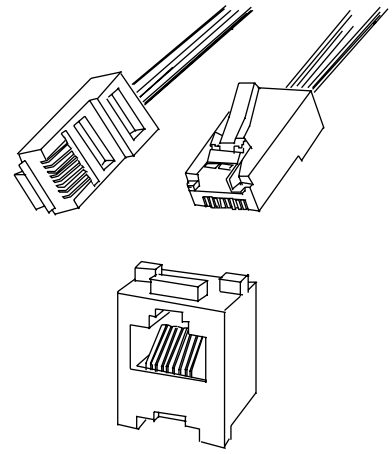


Figure 3.68 Le connecteur RJ45.

3.5 CONCLUSION

La limitation des débits est essentiellement due aux caractéristiques physiques des supports, mais les limites sont loin d'être atteintes. Les progrès des techniques de traitements du signal et de celles de codage des informations permettent d'améliorer la résistance au bruit et laissent espérer des débits se rapprochant de plus en plus des limites physiques.

EXERCICES

Exercice 3.1 Organisation des échanges

Donnez un exemple de la vie courante pour chacun des modes de contrôle des échanges (*simplex, half duplex, full duplex*).

Exercice 3.2 Transmission parallèle

Combien de conducteurs sont nécessaires pour réaliser une transmission en parallèle de mots machines de 32 bits si on utilise ou non un retour commun ?

Exercice 3.3 Transmission synchrone et asynchrone

Rappelez brièvement ce qui distingue ces deux modes de transmission.

Exercice 3.4 Efficacité

Une liaison de données est caractérisée par son débit (D) qui représente le nombre de bits transmis par unité de temps (bit/s). Cependant, il convient de distinguer le débit nominal (Dn) qui correspond au nombre de symboles binaires que le système est susceptible de transmettre, du débit réel (Dr) ou effectif qui mesure le nombre de bits utiles émis sur le support durant le temps réel de la session de transfert ramené à l'unité de temps. Le rapport de ces deux grandeurs mesure l'efficacité du système (Eff).

$$Eff = \frac{Dr}{Dn}$$

Le protocole PPP (*Point to Point Protocol*), utilisé pour l'accès à Internet, fonctionne en mode asynchrone et en mode synchrone. Lors de la connexion, pour un obtenir un fonctionnement optimal, une phase de négociation permet de configurer les différents paramètres du protocole PPP. En admettant que, dans les deux cas, cette phase ait défini l'utilisation de la trame standard, notamment une charge utile de 1 500 octets, quelle est l'efficacité de ce protocole dans les deux modes de fonctionnement ?

La figure 3.69 représente la trame PPP ; la signification et le rôle des différents champs seront précisés lors de l'étude de ce protocole.

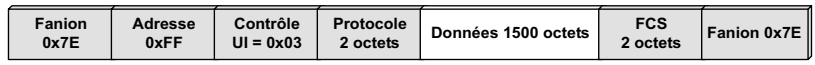


Figure 3.69 La trame PPP.

Exercice 3.5 Élément d'accès aux réseaux

Un DTE peut-il être raccordé directement au réseau d'un opérateur ?

Exercice 3.6 Transmission asynchrone

En transmission asynchrone, l'horloge du récepteur n'est synchronisée qu'en début de transmission. Une source a une horloge de 1 000 Hz (1 000 bits/s) avec une stabilité de 10^{-2}. Sachant que pour lire correctement un bit on ne peut admettre qu'une dérive maximale de 10 % par rapport à un temps bit et que le débit binaire est égal à la rapidité de modulation, quel est le nombre de bits que l'on peut émettre entre le bit de start et celui de stop ?

Exercice 3.7 Durée d'un transfert d'information

Une entreprise désire réaliser la sauvegarde de ses données sur un site distant. Le volume de données à sauvegarder est estimé à 10 Go/jour. La sauvegarde doit s'effectuer la nuit de 22 h 00 à 6 h 00. Les deux sites sont reliés par une ligne à 2 Mbits/s.

1. Vérifiez si cette solution est réalisable.
2. Le cas échéant, proposez une solution qui permette cette sauvegarde.

Pour ce problème on admettra que 1 ko = 1 000 octets et 1 Go = 1 000 ko.

Exercice 3.8 Caractéristiques d'un modem

Un modem V.29 fonctionne à 9 600 bits/s sur un canal de bande passante (BP) de 500 à 2 900 Hz. On utilise une modulation de phase à huit états avec une amplitude bivalente pour chaque état. Calculez :

1. la valence du signal modulé ;
2. la rapidité de modulation possible et celle utilisée ;
3. le rapport signal sur bruit pour garantir le fonctionnement correct de ce modem.

Exercice 3.9 Débit possible sur un canal TV

Si un canal de télévision a une bande passante de 6 MHz, quel est le débit binaire possible en bit/s si on utilise un encodage de valence 4 ?

Exercice 3.10 Rapport signal sur bruit

Appliquez la relation de Shannon à un circuit téléphonique et déterminez la capacité maximale théorique du canal, sachant que la bande passante est de 300-3 400 Hz et le rapport signal sur bruit (S/B) de 30 dB.

Exercice 3.11 Null modem

Vous désirez relier deux ordinateurs par un câble. Le protocole d'échange de données gère les signaux de commandes : 105, 106, 107, 108, 109. Rappelez la fonction de chacun des circuits nécessaires et réalisez le schéma de câblage (le câble réalisé s'appelle un null modem).

Exercice 3.12 Contrôle de flux matériel

Par quels signaux l'ETTD ou l'ETCD peut signaler qu'il n'est plus en état de recevoir des données ?

Exercice 3.13 Modem dissymétrique

Les utilisateurs nomades d'une entreprise accèdent au réseau de celle-ci *via* le réseau téléphonique (RTPC, Réseau téléphonique public commuté ou plus simplement RTC). L'établissement est relié au réseau téléphonique par une liaison numérique. Ce mode de liaison, lors de la transmission de données, permet l'économie d'une numérisation du signal, principale source de bruit (bruit de quantification). La liaison réalisée est dissymétrique, le bruit de quantification n'intervient que dans le sens Usager/Entreprise, ce procédé est mis en œuvre dans les modems V.90.

Dans toute liaison, chacun des composants participe au rapport signal sur bruit de l'ensemble. Pour cet exercice, on supposera que le rapport signal sur bruit de chacun des éléments constituant la liaison est indiqué par la figure 3.70.

Élément	Rapport S/B
Boucle locale analogique (DCE-Codec)	$2 \cdot 10^5$
Bruit de quantification du Codec (transformation analogique/numérique)	$1 \cdot 10^3$
Réseau de transport (RTPC)	$1 \cdot 10^8$
Boucle locale numérique (Réseau-DCE hybride ou MIC/PCM)	$2 \cdot 10^5$

Figure 3.70 Le rapport S/B de chaque élément participant à la liaison.

La figure 3.71 représente la liaison utilisateur nomade/entreprise.

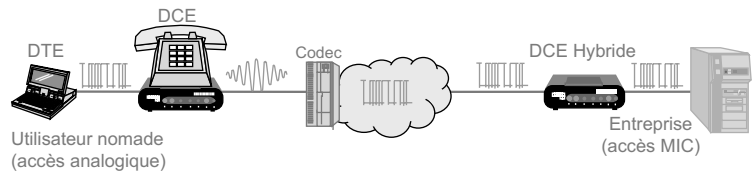


Figure 3.71 La liaison dissymétrique de type V.90.

© Dunod – La photocopie non autorisée est un délit

Dans cette liaison le modem utilisateur nomade (modem analogique) génère un signal analogique et reçoit un signal modulé G.711. Le modem hybride, ou numérique, génère un signal G.711 et reçoit un signal analogique numérisé par le codec source du bruit de quantification.

1. Sachant que le rapport signal sur bruit d'une liaison composée de n éléments est donné par la relation :

$$\left[\frac{S}{B}\right]^{-1} = \left[\frac{S1}{B1}\right]^{-1} + \left[\frac{S2}{B2}\right]^{-1} + \ldots + \left[\frac{Sn}{Bn}\right]^{-1}$$

   Calculez :

   a) le rapport S/B (signal/bruit) dans le sens Nomade/Entreprise ;
   b) le rapport S/B dans le sens Entreprise/Nomade, on arrondira les valeurs à la puissance de 10 entière la plus faible.

2. Sachant qu'un filtre passe-haut, en amont du codec (codeur/décodeur), limite la bande passante de la liaison à 3 400 Hz :

   a) déterminez la rapidité de modulation envisageable sur cette liaison dans les deux sens ;
   b) calculez le débit maximal admissible dans chacun des deux sens ;
   c) dans le sens Utilisateur/Entreprise le modem est classique et utilise une modulation de type MAQ, quel est le nombre d'états de celle-ci pour le débit normalisé maximal envisageable (on arrondira le $\log_2$ à la valeur entière la plus proche) ?
   d) en admettant qu'il en soit de même dans le sens Entreprise/Utilisateur, quel serait alors le nombre d'états ?

Exercice 3.14 Rapidité de modulation

Quelle est la rapidité de modulation en bauds du signal sur un réseau local 802.3 10 base 5 (Ethernet, codage Manchester) lorsqu'il émet une suite continue de 1 ou de 0 ?

Chapitre **4**

Notions de protocoles

4.1 GÉNÉRALITÉS

Dans les chapitres précédents nous avons étudié tous les mécanismes à mettre en œuvre pour transmettre un flot de bits entre deux systèmes distants. Cependant, il ne suffit pas de lire correctement les bits reçus, encore faut-il les traduire en données utilisables par les applications, c'est le rôle des protocoles que d'assurer le transfert et la délivrance des données aux applications. On appelle protocole un ensemble de conventions préétablies pour réaliser un échange fiable de données entre deux entités (figure 4.1).



Figure 4.1 Un protocole organise l'échange de données.

Lors de l'échange de données, le protocole de transfert doit assurer :

- la délimitation des blocs de données échangés ;
- le contrôle de l'intégrité des données reçues[1] ;
- l'organisation et le contrôle de l'échange.

Indépendant des fonctions en relation directe avec le transfert de données, un protocole doit assurer le contrôle de liaison. En particulier, le contrôle de l'échange implique la prise en compte du type de liaison et de la relation éventuellement hiérarchique entre les machines en communication.

1. Dans ce chapitre, le terme *intégrité* sera utilisé dans son sens le plus restrictif, il ne concernera que le contrôle d'erreur.

4.2 LES TYPE DE LIAISONS ET LEUR CONTRÔLE

4.2.1 La liaison point à point

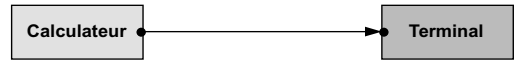


Figure 4.2 La relation point à point.

Dans ce mode de liaison, chaque correspondant est relié par un lien dédié à un seul autre correspondant. C'est, par exemple, le cas d'une liaison entre nœuds[2] d'un même réseau ou entre un ordinateur et un terminal (figure 4.2). L'une des entités est dite primaire, c'est celle qui initialise le dialogue et émet les commandes, l'autre est dite secondaire. Selon la répartition des fonctions de primaire et de secondaire, on distingue deux modes de contrôle :

– La symétrie synchrone, elle permet, à chaque extrémité, d'être primaire en émission et secondaire en réception (figure 4.3), il n'y a pas de hiérarchie entre les communicants. Connue sous le nom de mode équilibré ou *Asynchronous Balanced Mode* (**ABM**), elle est employée dans les liaisons *full duplex* (*Link Access Protocol Balanced* ou **LAP-B**) et *half duplex* (**LAP-X,** *LAP semi dupleX*).
– La dissymétrie asynchrone dans ce mode, le secondaire peut émettre sans y avoir été autorisé, ce qui implique qu'un seul secondaire puisse être actif à la fois ou qu'un algorithme de résolution des collisions soit mis en œuvre. Ce mode est appelé *Asynchronous Response Mode* (**ARM**).

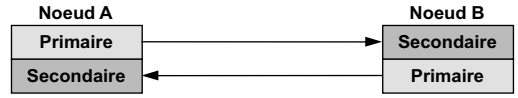


Figure 4.3 La symétrie synchrone.

4.2.2 Les liaisons multipoints

Une liaison est dite **multipoint** lorsqu'un même support est partagé par plusieurs nœuds. Dans ce cas, des conflits d'accès étant inévitables, il est nécessaire d'instaurer une politique d'accès au support. L'ensemble des mécanismes particuliers mis en œuvre, pour assurer le partage de l'accès au support, porte le nom de politique d'accès au canal. On distingue deux modes de contrôle de l'accès selon la manière dont est gérée la politique d'accès : le mode centralisé ou maître/esclave et le mode décentralisé ou d'égal à égal.

Le mode maître/esclave

Dans le mode de relation dit maître/esclave (figure 4.4) le primaire, généralement un ordinateur multiposte (*Mainframe* ou mini-ordinateur) est responsable de l'initialisation du dialogue, de la récupération des erreurs et de l'organisation des échanges. Le transfert des données s'effectue selon

2. Le terme nœud (*node*) désigne d'une manière générale tout calculateur qui reçoit, émet et/ou traite des données.

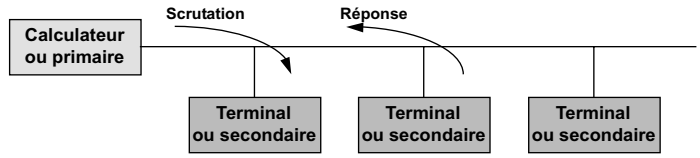


Figure 4.4 La relation maître/esclave.

la technique dite du « *polling/selecting* » (figure 4.5). Le maître invite le terminal (secondaire) à émettre (*polling*) ou lui demande de passer en mode réception (*selecting*).

Dans de grandes configurations, le *polling* de toutes les stations peut demander beaucoup de temps. Pour améliorer les temps de réponse, on utilise la technique dite du *polling* lent et *polling* rapide. À l'initialisation, toutes les stations sont interrogées, ensuite uniquement celles qui ont répondu (*polling* rapide) ; périodiquement, toutes les stations sont de nouveau interrogées (*polling* lent).

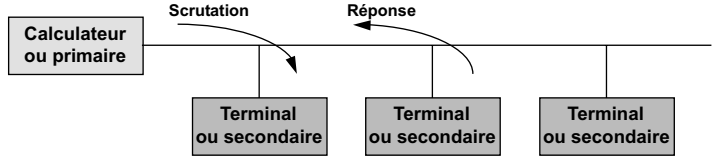


Figure 4.5 Polling/Selecting.

Le mode de relation ou dissymétrie synchrone est appelé *Normal Response Mode* (**NRM**) ou *Link Access Protocol* (**LAP**).

Le mode d'égal à égal

Dans ce type de configuration, tous les calculateurs sont autorisés à émettre vers n'importe quel autre calculateur et ce, à tout moment. Cet accès partagé peut donner lieu à des collisions ou contentions de messages (deux stations transmettent en même temps). Mais contrairement à la relation maître/esclave, ici, chaque calculateur dispose d'un algorithme d'accès ou méthode d'accès pour assurer le partage du support. La politique d'accès est dite décentralisée. Les réseaux locaux[3] constituent un exemple de ce mode de contrôle de l'accès au support.

4.3 LES FONCTIONS ÉLÉMENTAIRES

4.3.1 La délimitation des données

Notion de fanion

À l'instar des transmissions asynchrones où les bits de start et de stop encadrent les bits d'information, en transmission synchrone un caractère spécial ou une combinaison de bits particulière, le **fanion**, permet de repérer le début et la fin des données transmises (figure 4.6).

3. Voir chapitre 16 , *Les réseaux locaux*.

© Dunod – La photocopie non autorisée est un délit



Figure 4.6 La délimitation des données par fanions.

Le fanion assure trois fonctions essentielles :

– il délimite les données ;
– en l'absence de données à émettre, il permet de maintenir la synchronisation de l'horloge réception ;
– en identifiant le fanion, le récepteur peut se caler correctement sur une frontière d'octets (**synchronisation caractère**) et, par conséquent, traduire le flux de bits reçus en un flux d'octets.

Notion de transparence

L'utilisation d'un caractère spécifique pour indiquer le début ou la fin d'un bloc de données interdit l'usage de ce caractère dans le champ données. En conséquence, si on veut transmettre, en tant que données, le caractère ou la combinaison binaire représentative du fanion, il faut prévoir un mécanisme particulier. Ce mécanisme se nomme **mécanisme de transparence** au caractère, si le fanion est un caractère, ou mécanisme de transparence binaire, si le fanion est une combinaison de bits.

Le mécanisme de transparence consiste à « baliser » le caractère à protéger par un autre caractère dit **caractère d'échappement**. Ce caractère inséré à l'émission devant le caractère à protéger (le faux fanion) doit lui-même être protégé s'il apparaît dans le champ données (figure 4.7).

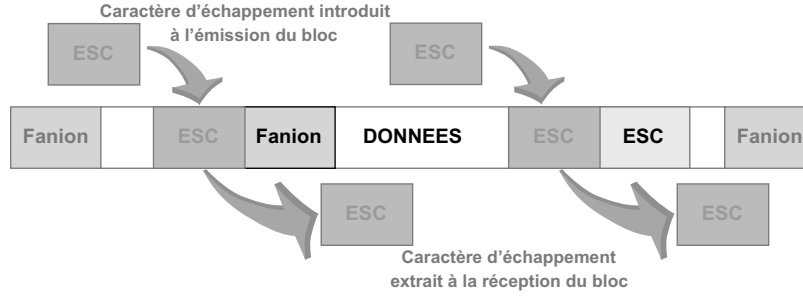


Figure 4.7 Principe de la transparence au caractère.

L'émetteur insère le caractère d'échappement devant le caractère à protéger. En réception, l'automate examine chaque caractère pour découvrir le fanion de fin. S'il rencontre le caractère d'échappement, il l'élimine et n'interprète pas le caractère qui le suit, il le délivre au système comme un caractère ordinaire.

Certains protocoles utilisent les 32 premiers caractères du code ASCII pour assurer le contrôle de l'échange. Ces caractères dits caractères de commande nécessitent aussi la mise en place d'un mécanisme de transparence. Les protocoles qui utilisent des caractères pour le contrôle de l'échange sont dits **orientés caractères**. En principe, ils utilisent le caractère ASCII 16 (**DLE**, *Data Link Escape*) comme caractère d'échappement.

Dans d'autres protocoles, un champ particulier est réservé aux informations de contrôle. Ce champ peut contenir une combinaison binaire quelconque. Ces protocoles sont dits orientés bits. Dans ces protocoles le fanion est constitué de la combinaison binaire « 01111110 » soit 0x7E. La transparence binaire est assurée par l'insertion d'un « 0 » tous les 5 bits à « 1 » consécutifs. Seul, le fanion contiendra une combinaison binaire de plus de 5 bits à 1 consécutifs (01111110). Cette technique dite du **bit de bourrage** (*Bit stuffing*), outre la transparence au fanion, permet, en interdisant les longues séquences de bits à 1 consécutifs, de maintenir la synchronisation des horloges. Les bits de bourrage insérés à l'émission sont éliminés par l'automate de réception. La figure 4.8 illustre le principe de la transparence binaire.

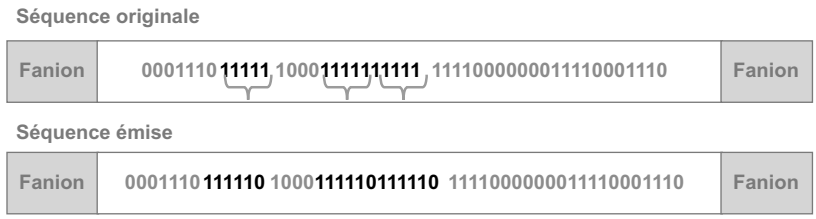


Figure 4.8 La technique du bit de bourrage.

Outre les délais introduits par l'insertion et l'élimination des bits ou caractères de transparence, cette technique modifie la taille des unités de données transmises. La longueur du bloc émis est variable, ce qui ralentit son traitement. Les protocoles dits à haut débit mettent en œuvre d'autres techniques, comme l'utilisation d'un codage de type 4B/5B, qui garantissent que le symbole choisi comme délimiteur ne pourra être présent dans le champ de données.

4.3.2 Le contrôle d'intégrité

D'une manière générale on doit, lors d'une transmission de données, s'assurer que les données reçues n'ont pas été altérées durant la transmission. Plusieurs facteurs peuvent modifier le contenu des données. Les uns sont d'origine humaine, le contrôle d'intégrité concerne alors la sécurité des données. Les autres sont d'origine physique, le contrôle d'intégrité porte alors le nom de contrôle d'erreur.

Notion d'erreur

➤ Taux d'erreur binaire

Les rayonnements électromagnétiques, les perturbations propres au système (distorsions, bruit...) peuvent modifier les informations transmises (bits erronés). Compte tenu de l'extension des réseaux et de l'utilisation massive de la fibre optique, la perte de la synchronisation des horloges est, aujourd'hui, la principale source d'erreurs.

On appelle **taux d'erreur binaire** ou **BER** (*Bit Error Rate*) le rapport entre le nombre d'informations (bits) erronées reçues et le nombre d'informations (bits) transmises.

Teb = Nb d'info. (ou bits) erronées / Nb d'info. (ou bits) transmises

Soit, par exemple, la transmission de la suite "011001001100100101001010"
qui est reçue "011001***1***0110010***1***10100***0***010".

© Dunod – La photocopie non autorisée est un délit

Le message reçu diffère de 3 bits du message émis. Le nombre de bits émis est de 24 bits. Le taux d'erreur binaire (Teb) est de :

$$\text{Teb} = 3/24 = 0{,}125$$

Le taux d'erreur binaire varie en pratique de 10^{-4} (liaisons RTC[4]) à 10^{-9} (réseaux locaux). Dans les réseaux, les erreurs se produisent généralement par rafale. Le Teb exprime une grandeur statistique, l'erreur affecte aléatoirement *n* bits consécutifs et non un bit tous les *x* bits.

Si t_e est la probabilité pour qu'un bit soit erroné, la probabilité de recevoir un bit correct est de $(1 - t_e)$. Soit, pour un bloc de *N* bits, une probabilité de réception correcte (p) de :

$$p = (1 - t_e)\,(1 - t_e)\,...\,(1 - t_e) = (1 - t_e)^N$$

La probabilité de recevoir un bloc sans erreur est d'autant plus faible que la longueur du bloc est grande.

Par exemple, supposons une transaction de 100 caractères émis sur une liaison en mode synchrone à 4 800 bits/s avec un Teb de 10^{-4}. Les erreurs sont supposées être distribuées aléatoirement. Quelle est la probabilité de recevoir un message erroné ?

Le message de 100 caractères correspond à un bloc de :

$$100 \cdot 8 = 800 \text{ bits}$$

La probabilité de réception d'un bloc correct (P_c) est de :

$$P_c = (1 - 0{,}0001)^{800} = (0{,}9999)^{800} = 0{,}923$$

Soit la probabilité de recevoir un message erroné (P_e) :

$$P_e = 1 - 0{,}923 = 0{,}077$$

➤ La détection d'erreur

On appelle détection d'erreur le mécanisme mis en œuvre par le système destinataire pour vérifier la validité des données reçues. La détection d'erreur repose sur l'introduction d'une certaine redondance dans l'information transmise. Quatre techniques peuvent être mises en œuvre pour détecter et éventuellement corriger les erreurs :

- La **détection par écho**, le récepteur renvoie en écho, à l'émetteur, le message reçu. Si le message est différent de celui qu'il a émis, l'émetteur retransmet le message. Cette technique est utilisée dans les terminaux asynchrones (Telnet, Minitel...).
- La **détection par répétition**, chaque message émis est suivi de sa réplique. Si les deux messages sont différents, le récepteur demande une retransmission. Cette technique est utilisée dans les milieux sécurisés très perturbés et dans certaines applications dites temps réel.
- La **détection d'erreur** par clé calculée, une information supplémentaire (clé) déduite des informations transmises est ajoutée à celles-ci (figure 4.9). En réception, le récepteur recalcule la clé, si le résultat obtenu correspond à la clé reçue, les données sont réputées exactes, sinon le récepteur ignore les données reçues et éventuellement en demande la retransmission (reprise sur erreur).

4. RTC, Réseau téléphonique commuté.

– La **détection et correction d'erreur par code**, cette technique consiste à substituer aux caractères à transmettre, une combinaison binaire différente du codage de base (code autocorrecteur) tel que, en cas d'erreur sur un nombre limité de bits, on puisse toujours déduire du code reçu la valeur binaire envoyée.

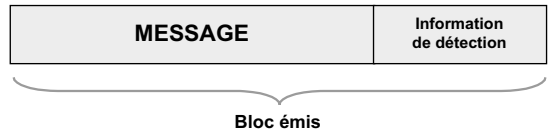


Figure 4.9 Principe de la correction d'erreur par redondance d'information.

➤ Détection d'erreur par clé calculée

Principe

Dans les systèmes à clé calculée, une séquence de contrôle (CTL1) déduite d'une opération mathématique appliquée au message à émettre est envoyée avec le message. Le récepteur effectue la même opération. Si le résultat trouvé (CTL2) est identique à la clé calculée par la source (CTL1), le bloc est réputé exact, dans le cas contraire le bloc est rejeté (figure 4.10).

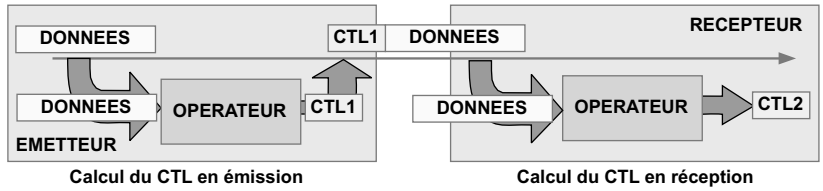


Figure 4.10 Principe de la détection d'erreur par clé calculée.

Technique dite du bit de parité

La technique du **bit de parité** consiste à ajouter, à la séquence binaire à protéger, un bit, telle que la somme des bits à 1 transmise soit paire (bit de parité) ou impaire (bit d'imparité). Cette arithmétique modulo 2 est simple, mais elle n'introduit qu'une faible redondance. La protection apportée est limitée à quelques bits : le caractère. La figure 4.11 illustre le mécanisme de calcul du bit de parité.

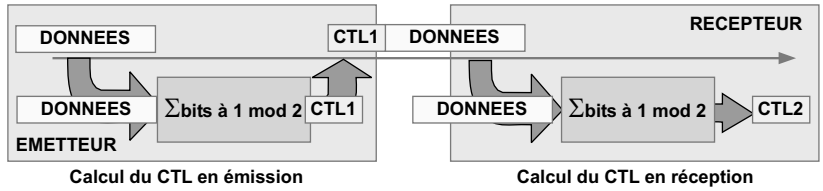


Figure 4.11 Le mécanisme du bit de parité.

La figure 4.12 fournit quelques exemples de calcul du bit de parité. Les caractères ASCII (7 bits) sont protégés par l'introduction d'un 8^{e} bit : le bit de parité.

© Dunod – La photocopie non autorisée est un délit

Caractère	O	S	I
Bit 6	1	1	1
Bit 5	0	0	0
Bit 4	0	1	0
Bit 3	1	0	1
Bit 2	1	0	0
Bit 1	1	1	0
Bit 0	1	1	1
Bit de parité	1	0	1
Bit d'imparité	0	1	0

Figure 4.12 Exemple de calcul du bit de parité et d'imparité.

Cette technique, connue sous le nom de **VRC** (*Vertical Redundancy Check*), vérification par redondance verticale, ne permet de détecter que les erreurs portant sur un nombre impair de bits. Elle n'est guère plus utilisée que dans les transmissions asynchrones (figure 4.13).

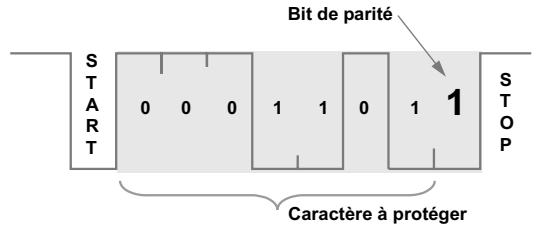


Figure 4.13 Le contrôle de parité dans les transmissions asynchrones.

Dans les transmissions synchrones, les caractères sont envoyés en blocs (figure 4.14). La technique du bit de parité est insuffisante, elle est complétée d'une autre information : le **LRC** (*Longitudinal Redundancy Check*).

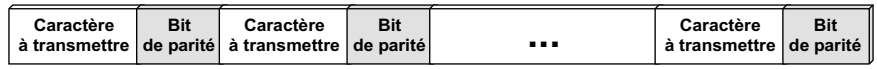


Figure 4.14 La structure d'un bloc de caractères protégé par LRC.

Dans ce mode de contrôle dit de parité à deux dimensions, un caractère : le LRC est ajouté au bloc transmis (figure 4.14). Chaque bit du caractère LRC correspond à la « parité » des bits de même rang que lui des caractères composant le message : le premier bit du LRC est la parité de tous les premiers bits de chaque caractère, le second de tous les deuxièmes bits... Le caractère ainsi constitué est ajouté au message (figure 4.15). Le LRC est lui-même protégé par un bit de parité (VRC).

Dans l'ensemble (pile) de protocoles TCP/IP[5] utilisé par Internet, le mode de calcul du mot de contrôle se rapproche des techniques de parité. Le mot de contrôle sur 16 bits ou total de contrôle est le complément à 1 de la somme en complément à 1 des mots de 16 bits composant le message.

5. TCP/IP (*Transmission Control Protocol/Internet Protocol*), cet ensemble de protocoles sera étudié en détail aux chapitres suivants.

	H	E	L	L	O	*LRC* →
bit 0	0	1	0	0	1	0
bit 1	0	0	0	0	1	1
bit 2	0	1	1	1	1	0
bit 3	1	0	1	1	1	0
bit 4	0	0	0	0	0	0
bit 5	0	0	0	0	0	0
bit 6	1	1	1	1	1	1
VRC ↓	0	1	1	1	1	0

1001000	0	1000101	1	1001100	1	1001100	1	1001111	1	1000010	0
H		E		L		L		O		LRC	

Figure 4.15 La transmission du mot « HELLO ».

Les codes cycliques ou détection par clé calculée

Dans la détection par clé calculée, l'information redondante, la clé (**CRC**, *Cyclic Redundancy Check*), est déterminée par une opération mathématique complexe appliquée au bloc de données à transmettre et transmise avec celui-ci (figure 4.16).

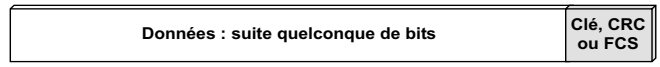


Figure 4.16 La structure d'un bloc de bits protégé par clé calculée.

La méthode de contrôle par clé calculée considère le bloc de N bits à transmettre comme un polynôme de degré $N - 1$: $P_{(x)}$. Ce polynôme est divisé par un autre, dit polynôme générateur $G_{(x)}$ selon les règles de l'arithmétique booléenne ou arithmétique modulo 2. Le reste de cette division $R_{(x)}$ constitue le CRC parfois appelé aussi **FCS** (*Frame Check Sequence*). Le CRC calculé est transmis à la suite du bloc de données. En réception, le destinataire effectue la même opération sur le bloc reçu (figure 4.17). Le CRC transmis et celui calculé par le récepteur sont comparés, si les valeurs diffèrent une erreur est signalée.

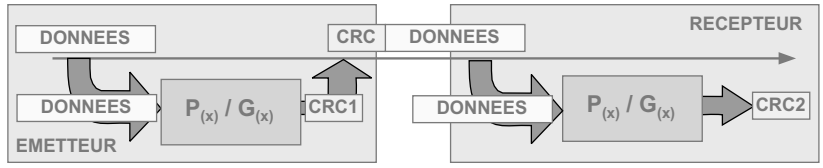


Figure 4.17 Principe de la détection d'erreur par clé calculée.

En réalité la méthode utilisée est quelque peu différente. En effet, si D est le dividende, d le diviseur et R le reste, la division $(D - R)/d$ donne un reste nul. En arithmétique booléenne, l'addition et la soustraction sont la même opération (figure 4.18), l'opération $(D - R)$ est équivalente à l'opération $(D + R)$.

Addition

+	0	1
0	0	1
1	1	0

Soustraction

–	0	1
0	0	1
1	1	0

Multiplication

x	0	1
0	0	0
1	0	1

Figure 4.18 Les opérations booléennes.

© Dunod – La photocopie non autorisée est un délit

Dans ces conditions (figure 4.19), la division par le polynôme générateur ($G_{(x)}$) de l'ensemble bloc de données et du CRC soit $P_{(x)} + R_{(x)}$ donne un reste égal à zéro. En réception, l'automate effectue la division sur l'ensemble du bloc de données y compris la clé calculée lorsque le calcul du reste donne zéro et que le caractère suivant est le fanion, le bloc est réputé exact.

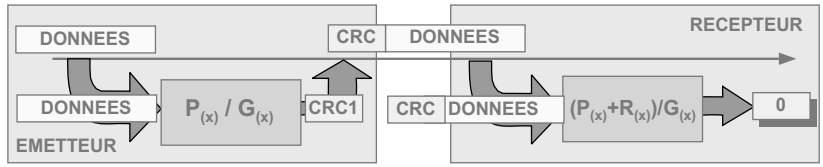


Figure 4.19 La détection d'erreur par CRC.

L'arithmétique modulo 2 est une arithmétique sans retenue, l'affirmation précédente n'est donc exacte que si le reste est ajouté à une séquence binaire nulle. Pour réaliser cette condition, avant d'effectuer la division, on multiplie le polynôme $P_{(x)}$ par x^m où m est le degré du polynôme générateur, ce qui correspond à une translation de *m* positions. Rappelons que le reste de la division par un diviseur de degré *m* est de degré *m – 1*, il comporte donc *m* termes. Cette opération a pour effet d'insérer *m* bits à zéro, pour y ajouter les termes du reste. L'exemple développé ci-dessous devrait éclairer le lecteur.

Exemple

On désire protéger le message « 110111 » par une clé calculée à l'aide du polynôme générateur $x^2 + x + 1$:

Au message 1 1 0 1 1 1

On fait correspondre le polynôme $x^5 + x^4 + 0x^3 + x^2 + x^1 + x^0$

Pour permettre l'addition de la clé au message sans altérer ce dernier, on multiplie le polynôme représentatif du message par x^m où *m* est le degré du polynôme générateur. Le dividende devient :

$$(x^5 + x^4 + 0x^3 + x^2 + x^1 + 1) \;.\; x^2 = x^7 + x^6 + 0x^5 + x^4 + x^3 + x^2 + \mathbf{0} + \mathbf{0}$$

$x^7 + x^6 + 0 + x^4 + x^3 + x^2 + \mathbf{0} + \mathbf{0}$	$x^2 + x + 1$
$x^7 \quad x^6 \quad x^5 \;\downarrow\; \downarrow \;\downarrow$	$x^5 \quad x^3 \quad 1$
$x^5 \quad x^4 \quad x^3 \;\downarrow$	
$x^5 \quad x^4 \quad x^3 \;\downarrow$	
$x^2 \quad 0 \quad 0$	
RESTE ⇒ $x^2 \quad x \quad 1$	
$\mathbf{x \quad 1}$	

Le reste de la division polynomiale est de degré inférieur à celui du diviseur, la division est terminée.

La division est réalisée par des systèmes « hardware » qui réalisent des « ou exclusif ». Aussi, appliquons la division par « ou exclusif » au polynôme 1010010111. Si le polynôme générateur est $x^4 + x^2 + x + 1$, il lui correspond la séquence binaire :

$$1\,(x^4) + 0\,(x^3) + 1(x^2) + 1(x^1) + 1(x^0) \text{ soit } 10111$$

Multiplier par x^N, le polynôme représentatif du message, revient à ajouter N bits à 0 au message (voir exemple précédent). Le degré du polynôme générateur étant de quatre, on ajoute quatre zéros à la trame de données (initialisation à zéro d'un registre à quatre positions). On obtient la division suivante :

```
1 0 1 0 0 1 0 1 1 1 0 0 0 0 | 1 0 1 1 1
1 0 1 1 1                   | 100 110 0100
0 0 0 1 1 1 0 1             | Le quotient est sans intérêt
      1 0 1 1 1
      0 1 0 1 0 1
        1 0 1 1 1
        0 0 0 1 0 1 0 0
              1 0 1 1 1
              0 0 0 1 1 0 0
```

Le reste (clé) comporte quatre termes, il est de degré –1 par rapport au polynôme générateur. Le reste ou CRC4 est donc 1100. Le message à transmettre est $P_{(x)} + R_{(x)}$:

$$10100101111\mathbf{1100}$$

En réception, l'ensemble du message, données et clé, subit la même opération ; si le reste de la division est égal à zéro, on estime que le message n'a pas été affecté par une erreur de transmission. Vérifions cette affirmation sur l'exemple précédent :

```
message      reste  | 1 0 1 1 1
1010010111   1100   |
10111               |
00011101            |
   10111            |
   010101           |
    10111           |
    000101   11     |
       101   11     |
       000   0000   |
```

Le reste de la division (message + reste) est nul, le message est réputé correctement transmis.

Exemples de polynômes générateurs

Déterminer un polynôme générateur consiste à rechercher une combinaison binaire telle que la probabilité de non-détection d'une erreur soit aussi faible que possible et que le calcul du CRC ne pénalise pas exagérément la transmission. Les polynômes générateurs utilisés font l'objet de normalisation. Le degré du polynôme est d'autant plus élevé que la probabilité d'apparition d'une erreur est grande, c'est-à-dire que la longueur du bloc à protéger est importante. Les principaux polynômes employés sont :

– Protection de l'en-tête des cellules ATM[6].

$$x^8 + x^2 + x + 1$$

6. ATM, *Asynchronous Transfert Mode*, protocole de transfert haut débit étudié au chapitre 14.

© Dunod – La photocopie non autorisée est un délit

– Détection d'erreur couche AAL[7] type 3 et 4 d'ATM,

$$x^{10} + x^9 + x^5 + x^4 + x + 1.$$

– Avis du CCITT N°41,

$x^{16} + x^{12} + x^5 + 1$ permet de détecter

  – toutes les séquences d'erreurs de longueur égale ou inférieure à 16 bits,
  – toutes les séquences erronées comportant un nombre impair de bits,
  – 99,99 % des erreurs de longueur supérieure à 16 bits,
  – utilisé dans HDLC[8].

– Comité IEEE 802[9]

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

  – utilisé dans les réseaux locaux.

➤ Les codes autocorrecteurs

Dans les systèmes autocorrecteurs, on substitue au mot à transmettre (mot naturel) un nouveau mot (mot code), tel que deux mots codes successifs diffèrent de α bits, où α est appelé **distance de Hamming**. On montre que si la distance de Hamming est de α on peut :

– détecter toute erreur portant sur $(\alpha - 1)$ bits ;
– corriger toute erreur portant sur $(\alpha - 1) / 2$ bits.

Dans la technique du bit de parité, la distance de Hamming est de deux. Cette technique ne permet pas la correction d'erreur, seule la détection d'erreur portant sur un bit est possible. En réalité, compte tenu de la spécificité du calcul du bit de parité, toute erreur portant sur un nombre impair de bits est détectable.

Supposons le code de Hamming suivant :

Mots naturels	Mots codes
00	10011
01	10100
10	01001
11	01110

Dans ce code, il y a toujours, au moins, trois bits qui diffèrent d'un mot code à un autre, la distance de Hamming est de trois. Ce code permet donc de détecter toutes les erreurs portant sur 2 bits et de corriger toutes les erreurs ne portant que sur un seul bit.

Soit le mot 00 (figure 4.20), on transmet le mot code « 10011 », une erreur sur un bit correspond à la réception de l'un des mots suivants :

10010 10001 10111 11011 00011

7. AAL, *ATM Adaptation Layer*, couche d'adaptation entre les protocoles de niveaux supérieurs et la couche ATM proprement dite.
8. HDLC, *High Data Link Control*, étudié dans la suite de ce chapitre
9. IEEE 802, comité de l'IEEE créé en 1980 (**80**) au mois de février (***2***) d'où 802 qui est spécialisé dans l'étude des réseaux locaux.

Le mot reçu ne correspond à aucun des mots du code. Le code pouvant corriger toute erreur portant sur un bit, on considère que le mot transmis est celui du code dont la distance de Hamming n'est que de un avec le mot reçu. La figure 4.20 illustre ce propos, le mot reçu « 11011 » est comparé à tous les autres mots du code. Seul le mot code 10011 est à une distance de Hamming de un. La valeur reçue sera supposée être 10011, soit le mot origine 00.

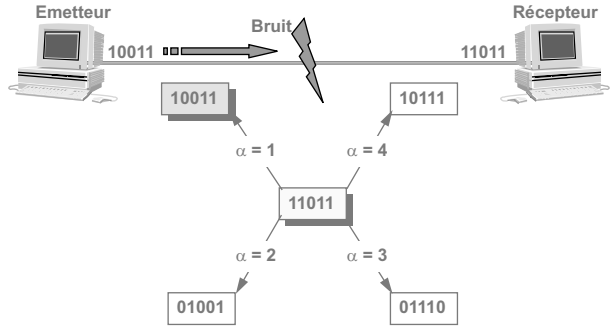


Figure 4.20 Estimation du mot reçu.

4.3.3 Le contrôle de l'échange

Du mode Send and Wait *aux protocoles à anticipation*

➤ Les mécanismes de base

Le principe de base de toute transmission repose sur l'envoi (*Send*) d'un bloc d'information. L'émetteur s'arrête alors (*Stop*) dans l'attente (*Wait*) d'un accusé de réception. À la réception de l'acquittement, noté **ACK** pour *Acknowledge*, l'émetteur envoie le bloc suivant (figure 4.21 gauche).

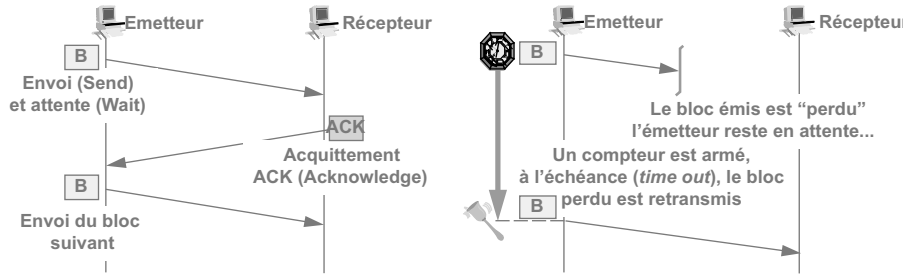


Figure 4.21 Le mode Send et Wait et la reprise sur temporisation.

En cas d'erreur de transmission, le bloc reçu est rejeté. Le bloc est dit perdu, il n'est pas acquitté. L'émetteur reste alors en attente. Pour éviter un blocage de la transmission, à l'émission de chaque bloc de données, l'émetteur arme un temporisateur (*Timer*). À l'échéance du temps imparti (*Time Out*), si aucun accusé de réception (ACK) n'a été reçu, l'émetteur retransmet le bloc non acquitté, cette technique porte le nom de reprise sur temporisation (**RTO**, *Retransmission Time Out*) ou correction d'erreur sur temporisation (figure 4.21 droite).

© Dunod – La photocopie non autorisée est un délit

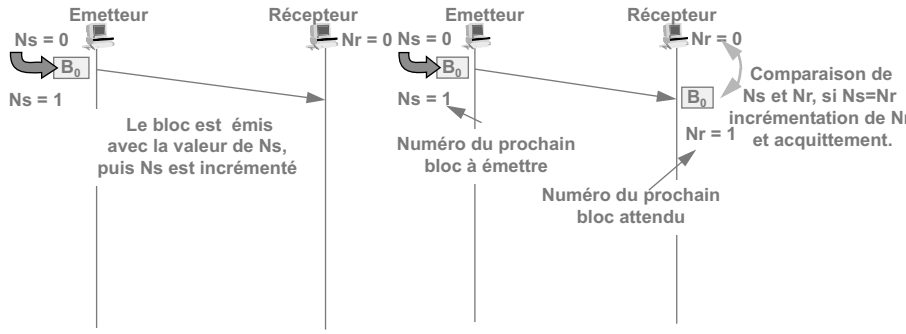


Figure 4.22 La numérotation des blocs de données.

Une difficulté survient si la perte concerne l'ACK. En effet, bien que les données aient été correctement reçues, l'émetteur les retransmet sur temporisation. Les informations sont ainsi reçues deux fois. Pour éviter la duplication des données, il est nécessaire d'identifier les blocs. À cet effet, l'émetteur et le récepteur entretiennent des compteurs (figure 4.22). Les compteurs Ns (Ns, Numéro émis, s pour *send*) et Nr (Numéro du bloc à recevoir, r pour *receive*) sont initialisés à zéro. Le contenu du compteur Ns est transmis avec le bloc, le récepteur compare ce numéro avec le contenu de son compteur Nr. Si les deux valeurs sont identiques, le bloc est réputé valide et accepté. Si les valeurs diffèrent, le bloc reçu n'est pas celui attendu. Il est rejeté et acquitté s'il correspond à un bloc déjà reçu. Dans le cas contraire (Ns > Nr), il s'agit d'une erreur de transmission, nous verrons dans ce qui suit le comportement du récepteur dans ce cas (figure 4.52). Cette numérotation évite la duplication et autorise le contrôle de séquencement des données reçues (figure 4.23).

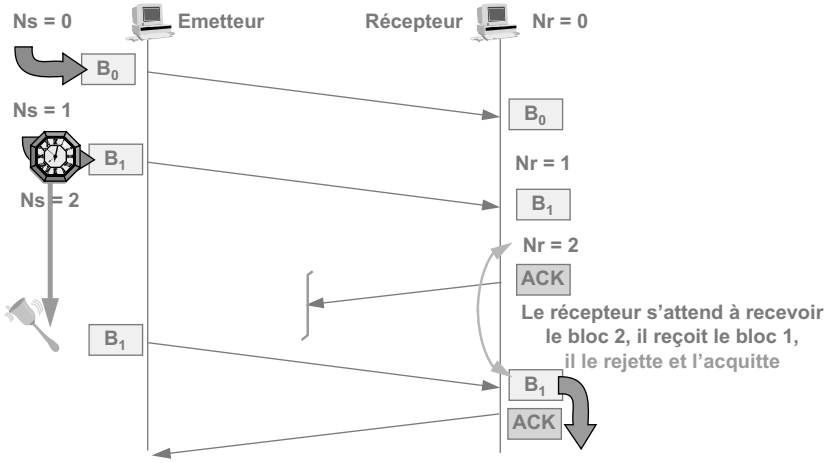


Figure 4.23 Le contrôle de séquencement après une reprise sur temporisation.

Cependant, dans certains cas, le temps de traitement des données reçues est plus important que prévu ou (et) les délais de transmission sont devenus excessivement longs (figure 4.24). Dans ces conditions, les données reçues peuvent ne pas être acquittées à temps. L'émetteur effectue alors une retransmission sur temporisation. Le récepteur ayant déjà reçu ces informations les élimine et

les acquitte. En effet, pour le récepteur, s'il y a eu une retransmission, c'est que l'émetteur n'a pas reçu le précédent ACK. Ainsi, figure 4.24, à la réception du premier ACK (acquittant le bloc 0) l'émetteur envoie le bloc suivant (B1).

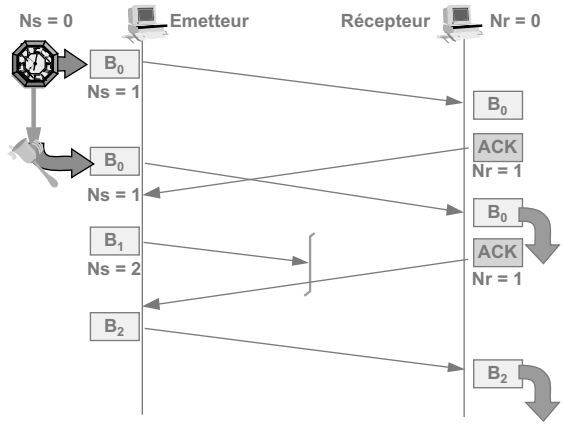


Figure 4.24 Délai d'acquittement trop important.

Supposons que ce bloc se « perde », à réception du second ACK (concernant le second envoi de B0) l'émetteur considère que cet ACK est relatif au bloc B1, il envoie le bloc suivant (B2). Ce bloc comporte un Ns différent du numéro attendu, il est rejeté. Pour éviter cette confusion d'interprétation, il est aussi nécessaire de numéroter les ACK.

➤ Efficacité du protocole de base

Pour déterminer l'efficacité d'un protocole, il faut non seulement tenir compte des informations de contrôle (figure 4.25), mais aussi du délai d'acquittement. D'une manière générale, l'efficacité d'un protocole mesure le rapport du temps effectivement consacré à l'émission d'informations utiles au temps pendant lequel le support a été occupé, ou encore le rapport du nombre de bits utiles transmis au nombre de bits qui auraient pu être émis.

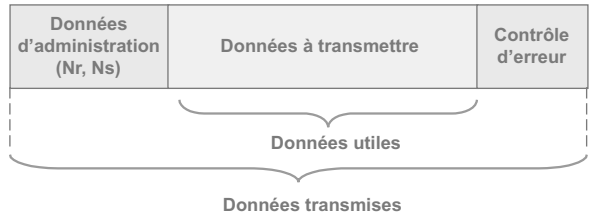


Figure 4.25 La structure de base d'un bloc d'information.

Transmission sans erreur

Considérons l'échange représenté par le diagramme temporel de la figure 4.26, on distingue les phases suivantes :

– l'émission du bloc de données, ou **U** représente les données utiles, **G** les données de gestion du protocole ;

© Dunod – La photocopie non autorisée est un délit

– un temps mort pendant lequel l'émetteur attend l'acquittement qui correspond au temps de transit aller et retour sur le support et au temps de traitement des données reçues par le récepteur. Ce temps, généralement désigné sous le terme de temps de traversée des équipements, noté **RTT** (*Round Trip Time*, temps aller et retour), équivaut à l'émission de (D · RTT) bits où **D** représente le débit nominal du système ;
– enfin, la réception de l'accusé de réception de **K** bits.

Le temps entre l'émission du premier bit du bloc *N* et le premier bit du bloc suivant (*N* + 1) est appelé temps d'attente et noté *Ta*.

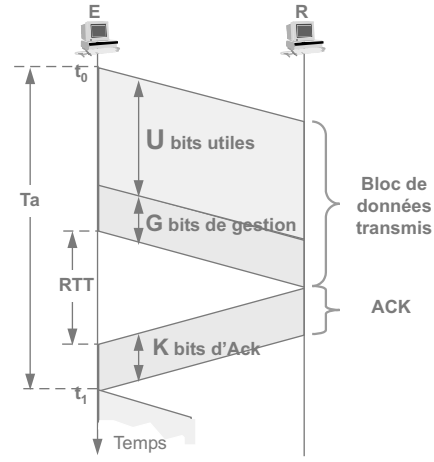


Figure 4.26 L'efficacité du mode de base.

Établissons l'efficacité du protocole dans une transmission sans erreur. Rappelons que l'efficacité d'un protocole (*E*) est le rapport entre le nombre de bits utiles transmis (*U*) au nombre de bits total transmis ou qui auraient pu être transmis (*N*).

$$E = U / N \qquad (1)$$

Le nombre de bits qui auraient pu être transmis entre t_0 et t_1 (Ta) s'exprime par la relation :

$$N = U + G + K + D \cdot \text{RTT}$$

Dès lors, on peut déterminer l'efficacité du protocole dans le cas où aucune erreur ne se produit, posons :

$$S = G + K + D \cdot \text{RTT}$$

avec :

– $D \cdot RTT$ = nombre de bits représentatifs du temps de traversée des équipements
– *G* les bits de gestion (contrôle, adresse...)
– *K* les bits d'accusé de réception,

Soit, en reprenant l'équation (1) :

$$E_0 = U/N = U / (U + S) \quad \text{avec } E_0\text{, efficacité du protocole sans erreur}$$

Transmission avec erreur

Si t_e (taux d'erreur) est la probabilité pour qu'un bit transmis soit erroné, $1 - t_e$ est la probabilité pour qu'un bit soit correctement transmis. Si la transmission porte sur N bits, la probabilité pour que N bits soient correctement transmis, est :

$$p = (1 - t_e)^N \quad \text{avec} \quad N = U + G$$

La probabilité pour que l'ACK soit correctement transmis est de :

$$p = (1 - t_e)^K$$

La probabilité pour qu'un bloc soit supposé correctement transmis est la probabilité composée :

$$p' = (1 - t_e)^N \cdot (1 - t_e)^K$$

L'efficacité du protocole avec erreur (E_{er}) est alors :

$$E_{er} = U \cdot (1 - t_e)^N \cdot (1 - t_e)^K / (U + S)$$

$$E_{er} = (U / U + S) \cdot (1 - t_e)^N \cdot (1 - t_e)^K$$

Soit :

$$E_{er} = E_0 \cdot (1 - t_e)^N \cdot (1 - t_e)^K = E_0 (1 - t_e)^{N+K}$$

Or $K \ll N$, on peut donc admettre que l'efficacité en présence d'erreur est, par rapport à celle sans erreur :

$$E_{er} = E_0 \cdot (1 - t_e)^N$$

Application numérique

Déterminons l'efficacité d'une transmission à 4 800 bits/s par blocs de 128 octets de données utiles, chaque bloc nécessite 6 octets de gestion ; l'accusé de réception comporte 6 octets. On considérera que le temps de traversée des équipements (RTT) est de 50 ms et que la liaison est affectée d'un taux d'erreur de 10^{-4}.

Calculons les bits représentatifs de la traversée des équipements :

$$N = D \cdot \text{RTT} = 4\,800 \times 50 \cdot 10^{-3} = 240 \text{ bits}$$

Soit $S = G + K + D \cdot \text{RTT} = 8\,(6 + 6) + 240$

$$S = 336 \text{ bits}$$

L'efficacité sans erreur (E_0) est :

$$E_0 = U / (U + S) = 128 \times 8 / (128 \times 8 + 336)$$

$$E_0 = 1\,024 / (1\,024 + 336)$$
$$E_0 = 1\,024/1\,360$$
$$\boldsymbol{E_0 = 0{,}75}$$

© Dunod – La photocopie non autorisée est un délit

Avec erreur (E_{er}) :

$$E_{er} = 0{,}75 \cdot (1 - t_e)^N \cdot (1 - t_e)^K$$

$N = U + G$
$N = (128 + 6) \times 8$
$N = 1\,072$
$E_{er} = 0{,}75 \times (1 - 0{,}0001)^{1\,072} \cdot (0{,}9999)^{48}$
$E_{er} = 0{,}75 \times 0{,}89 \times 0{,}995$
$E_{er} = 0{,}667$
$\boldsymbol{E_{er} \approx 0{,}67}$

Remarque

L'efficacité permet de déterminer le débit réel, c'est-à-dire le débit vu par l'application, celui-ci est donné par la relation :

Débit réel = Débit nominal · Efficacité réelle du protocole

➤ Les protocoles à anticipation

Les faibles performances du mode *Send and Wait* sont essentiellement dues au temps d'attente de l'ACK (T_t). Dans ces conditions, une amélioration substantielle peut être obtenue en émettant les blocs suivants sans attendre la réception des ACK, ce processus se nomme anticipation.

Principe

Le principe est illustré par la figure 4.27.

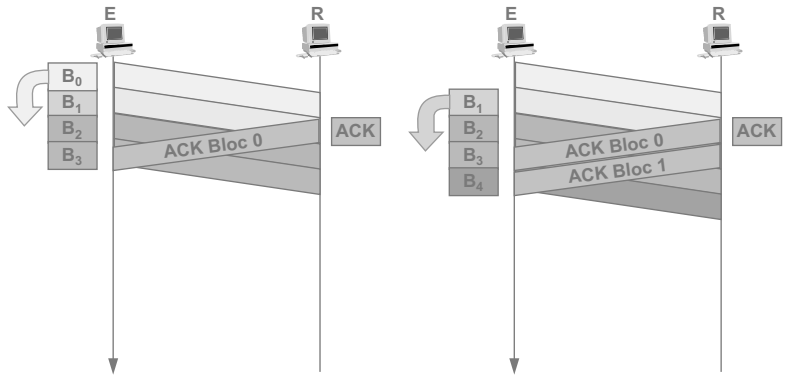


Figure 4.27 Principe des protocoles à anticipation.

L'émetteur émet en continu les blocs de données. Pour autoriser une éventuelle retransmission après erreur (reprise sur erreur), en l'attente de l'acquittement, il mémorise les différents blocs émis (mise en mémoire tampon ou *bufferisation*). À la réception de l'ACK d'un bloc émis, il libère le *buffer*[10] correspondant. La notion d'anticipation est limitée par le nombre de *buffers* que l'émetteur est susceptible de mettre à disposition du protocole.

10. Le terme *buffer*, en français mémoire tampon, est désormais passé dans le langage courant. Par la suite nous adopterons ce terme, car bufferisation est plus évocateur que tamponnage !

On appelle fenêtre d'anticipation ou crédit d'émission, notée **W** (*Window*), le nombre de blocs que l'émetteur peut mémoriser en attente d'acquittement. L'efficacité de la transmission est maximale lorsqu'il n'y a pas d'arrêt de l'émission pendant le temps d'attente de l'ACK (émission continue). La taille de la fenêtre optimale correspond donc au nombre de blocs à transmettre pour que l'émission soit continue (figure 4.28).

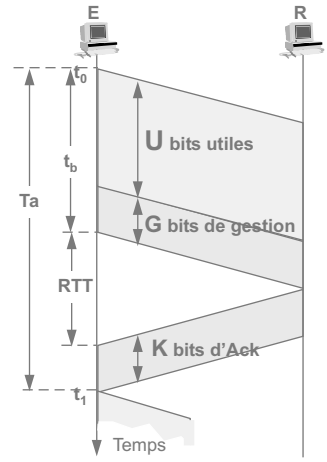


Figure 4.28 La détermination de la fenêtre.

Reprenons les paramètres définis au paragraphe précédent :

– T_a ou temps d'attente, temps entre l'émission du premier bit de la trame N et le premier bit de la trame $N + 1$ en mode *Send and Wait*

– RTT temps aller et retour,
et si t_b représente le temps d'émission d'un bloc (volume à émettre sur débit) :

$$t_b = (U + G) / D$$

en nommant W la taille de la fenêtre, il n'y aura pas d'arrêt des émissions si :

$$W \cdot t_b \geqslant T_a$$

La taille optimale de la fenêtre est :

$$W \geqslant T_a / t_b$$

Remarque : certains protocoles et notamment TCP/IP déterminent dynamiquement le délai d'acquittement (**RTO**, *Retransmission Time Out*) ; pour cela, le protocole évalue en permanence le délai d'acheminement aller et retour. La distinction entre le temps d'attente (T_a) et le délai aller retour (**RTT**, *Round Trip Time*) est difficilement réalisable. En conséquence, le RTT et le temps d'attente sont confondus. Dans la suite de cet ouvrage nous assimilerons RTT et temps d'attente et le désignerons sous la seule appellation de RTT.

© Dunod – La photocopie non autorisée est un délit

Modes de gestion de la fenêtre

Dans la figure 4.27, chaque bloc est acquitté. Lors de la réception d'un ACK, l'émetteur libère un *buffer* et émet le suivant. On dit que la fenêtre s'est ouverte de 1. Ainsi, dans la figure 4.29 en supposant une fenêtre de 3, à réception de l'ACK0, le *buffer* B0 est libéré, l'émetteur transmet B3. À la réception de l'ACK1, B1 est libéré, l'émetteur émet B4... La fenêtre est dite **glissante** ; dans l'hypothèse de la figure 4.29, la fenêtre est de 3, alors que la capacité de numérotation des blocs est de 8 (3 bits, numérotation modulo 8).

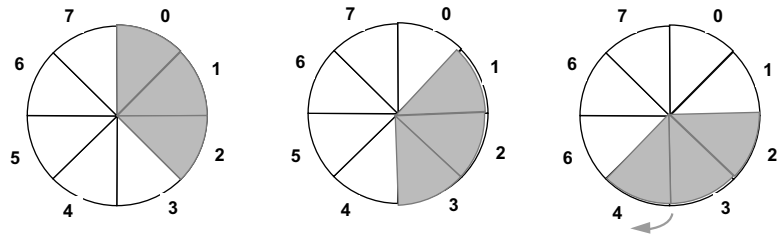


Figure 4.29 La gestion de la fenêtre dite « glissante ».

Cependant, chaque bloc n'a pas nécessairement besoin d'être acquitté individuellement. L'acquittement peut être différé et concerner plusieurs blocs. La figure 4.30 illustre ce propos. La fenêtre est de 3, l'acquittement du troisième bloc reçu (Nr = 3) acquitte les blocs 0, 1, 2 et demande l'émission du quatrième bloc qui portera le numéro 3. Nr représente le numéro du prochain bloc attendu. L'acquittement est dit global ou différé.

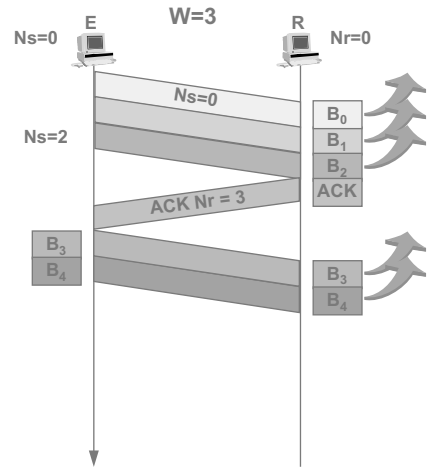


Figure 4.30 Principe de l'acquittement global ou différé.

Dans ce mode de fonctionnement, il y a arrêt des émissions quand le crédit d'émission est consommé. À la réception d'un ACK, la fenêtre se rouvre de tout le crédit, elle est dite **sautante** (figure 4.31).

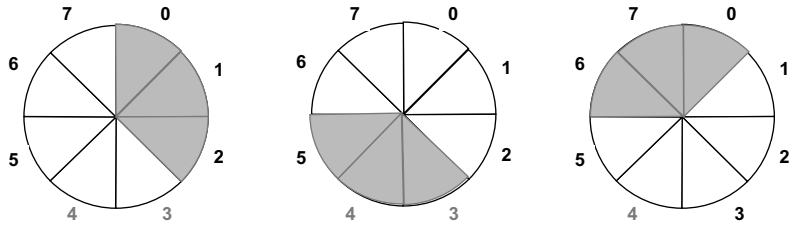


Figure 4.31 La gestion de la fenêtre dite « sautante ».

Les protocoles à fenêtre et la politique de reprise sur erreur

Le récepteur délivre les blocs reçus au fur et à mesure de leur réception. En cas d'erreur de transmission, deux politiques de reprise sur erreur sont envisageables :

– le récepteur mémorise les blocs reçus hors séquencement, l'émetteur sur temporisation ou sur demande explicite du récepteur ne retransmet que le bloc erroné (figure 4.32 gauche) ;
– le récepteur rejette tous les blocs reçus hors séquencement, l'émetteur reprend alors la transmission à partir du bloc perdu, (figure 4.32 droite).

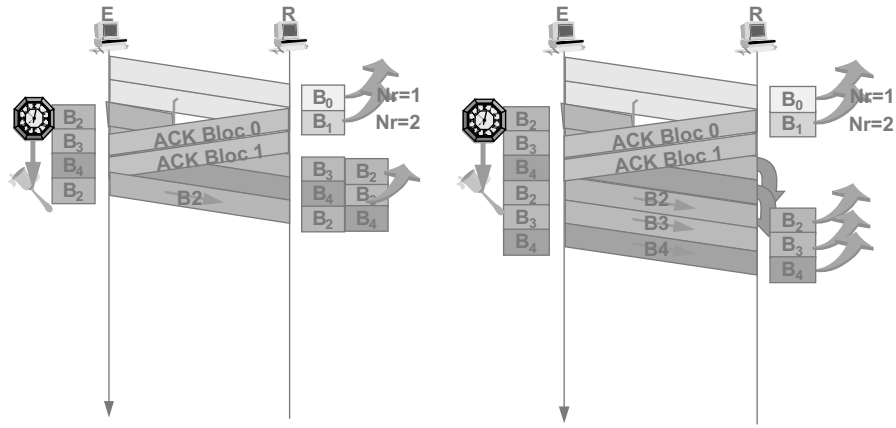


Figure 4.32 Les politiques de reprise sur erreur.

Dans la première hypothèse (figure de gauche), le rejet est qualifié de **rejet sélectif**, la transmission est optimisée mais nécessite des mémoires tampons importantes en réception (*buffers*) et le réordonnancement de tous les blocs. Le nombre de blocs déséquencés pouvant être reçus par le récepteur s'appelle **fenêtre de réception**.

Dans le second cas, la mémoire du récepteur est optimisée, la puissance de calcul du récepteur est minimisée, pas de reséquencement, mais la transmission est pénalisée par la retransmission de tous les blocs. Ce mode de reprise sur erreur est appelé **rejet simple**, la taille de la fenêtre de réception est alors de 1.

© Dunod – La photocopie non autorisée est un délit

Rejet simple ou rejet sélectif ?

À des fins de minimisation de mémoire, le rejet simple est généralement utilisé. Cependant, lorsque le temps de transit dans le système de transmission est important, le rejet sélectif s'impose.

Supposons deux systèmes de transmission illustrés par la figure 4.33. L'un utilise un réseau terrestre, l'autre une liaison satellitaire. Calculons, dans les deux hypothèses, les conséquences d'une reprise sur erreur dans le cas de l'utilisation du rejet simple.

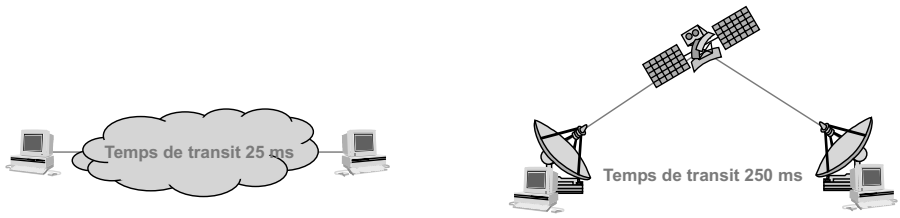


Figure 4.33 Le système de transmission et le traitement des erreurs.

Pour cela, formulons les hypothèses suivantes :

– taille moyenne des unités de données 128 octets ;
– débit des liaisons 64 kbits/s ;
– temps d'émission des ACK négligeable ;
– erreur affectant le premier bloc de la fenêtre (hypothèse pessimiste).

Pour déterminer l'influence de la reprise sur erreur, il nous faut connaître le nombre de blocs qui seront retransmis, ce qui correspond à la taille de la fenêtre ($W \geqslant T_a/T_b$) :

– Temps d'émission d'un bloc $T_b = (128 \times 8) / 64\,000 = 16$ ms
– Temps d'attente (supposé pour simplification égal au RTT) :

Liaison terrestre	50 ms
Liaison satellitaire	500 ms

– Fenêtre :

Liaison terrestre	$W \geqslant 50/16 = 4$
Liaison satellitaire	$W \geqslant 500/16 = 32$

En cas d'erreur, le récepteur reçoit le bloc retransmis après un temps minimal de T_a (reprise sur temporisation), auquel il faut ajouter le temps de retransmission du ou des blocs à retransmettre et le temps de transit dans le réseau.

	Transmission terrestre	Transmission satellitaire
T_a	50 ms	500 ms
Retransmission (Nb. blocs $\times$ T_b)	4 $\times$ 16 = 64 ms	32 $\times$ 16 = 512 ms
Temps de transit	25 ms	250 ms
Temps total	139 ms	1 262 ms

Figure 4.34 Temps de pénalisation de la transmission

Ce simple calcul montre l'inadéquation d'un système de reprise simple sur une liaison satellite. De plus, si l'on considère que le taux d'erreur sur des voies hertziennes est important, le rejet sélectif s'impose. En ce qui concerne les transmissions terrestres, le temps de reprise n'est pas négligeable ; cependant, pour minimiser l'espace mémoire dans les commutateurs des réseaux, on lui préfère le rejet simple.

4.3.4 Le contrôle de flux

Définition

Le mécanisme de la fenêtre d'anticipation optimise la transmission mais il ne prend pas en compte les capacités de réception du destinataire. L'émetteur ne doit envoyer des données que si le récepteur peut les recevoir. Lors d'une transmission, le destinataire met à disposition du transfert un certain nombre de mémoires tampons (*buffers*). Le récepteur peut, compte tenu d'autres tâches à réaliser, ne pas libérer ses *buffers* suffisamment rapidement, des blocs peuvent alors être perdus (figure 4.35).



Figure 4.35 Nécessité d'instaurer un contrôle de flux.

Le contrôle de flux consiste à asservir la cadence d'émission de l'émetteur sur les capacités de réception du récepteur. L'émetteur n'émet alors pas plus de données que le récepteur ne peut en accepter.

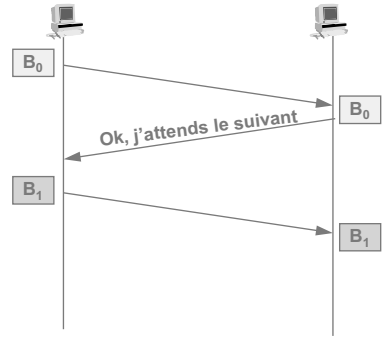


Figure 4.36 Principe du contrôle de flux.

La figure 4.36 illustre le principe du contrôle de flux. Dans ce modèle, le récepteur délivre une autorisation explicite à l'émetteur avant l'émission de chaque bloc, le protocole est dit « XON, XOFF ». Le crédit ou fenêtre d'émission est dit de un.

© Dunod – La photocopie non autorisée est un délit

Le contrôle de flux par crédit d'émission

On appelle **crédit d'émission**[11], noté Ct dans la figure 4.37, le nombre de blocs que l'émetteur est autorisé à transmettre. Deux politiques de gestion du contrôle de flux peuvent être envisagées (figure 4.37) :

- le contrôle de flux est dit **implicite** quand le crédit est prédéterminé (figure 4.37 gauche). Il reste constant durant toute la transmission (fenêtre statique). La transmission est optimisée par rapport au mode *Send and Wait*. Cependant, rien ne permet de garantir que le récepteur pourra toujours recevoir les *N* blocs du crédit. De plus, la transmission ne bénéficie pas d'éventuelles évolutions des capacités de réception du destinataire. Dans ce mode de fonctionnement, en cas de saturation, le récepteur envoie un message de demande d'arrêt des émissions.
- le contrôle de flux est dit **explicite** ou **dynamique** lorsque le récepteur informe en permanence l'émetteur sur ses capacités de réception (figure 4.37 droite).

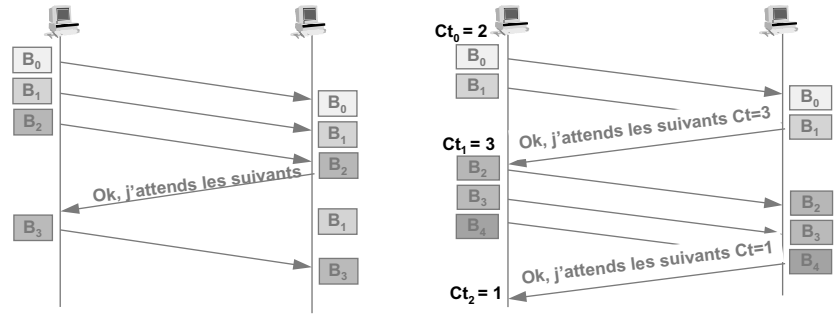


Figure 4.37 Le contrôle de flux par fenêtre.

Les limites du contrôle de flux

La saturation du système peut intervenir avant que le crédit ne soit épuisé. De ce fait, les protocoles implémentent un mécanisme spécifique pour indiquer au système émetteur l'état de saturation du récepteur et arrêter les émissions de données. Cependant, entre le moment où le système reçoit un message saturant et le moment où l'émetteur en est averti, l'émission des données se poursuit. Aussi, pour examiner les limites du contrôle de flux, il convient de déterminer l'inertie du système, c'est-à-dire le nombre de messages envoyés et donc perdus. Déterminons ce nombre dans le cas suivant (figure 4.38) :

- la distance internœud est de 100 km ;
- le débit des liens est de 155 Mbit/s ;
- la longueur moyenne des blocs de données est de 100 octets ;
- les temps d'acquisition des données reçues et d'émission de l'ACK seront considérés comme négligeables.

11. La notion de crédit d'émission est souvent confondue avec celle de fenêtre d'anticipation. Bien que les concepts soient proches, la distinction doit être faite. La fenêtre d'émission est un paramètre fixé par l'émetteur alors que le crédit d'émission correspond à une autorisation d'émettre émanant du récepteur.

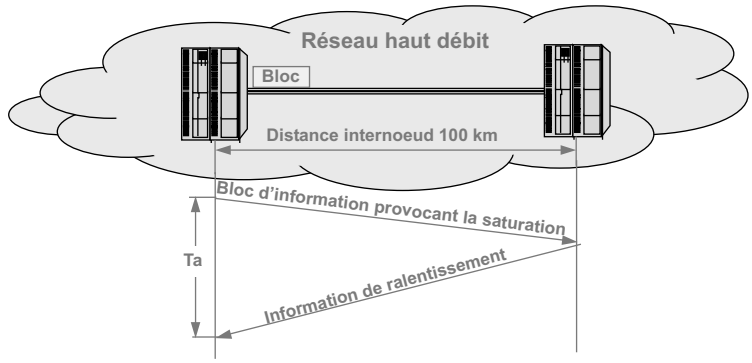


Figure 4.38 Le contrôle de flux et débit élevé.

Après saturation des buffers du récepteur, le délai qui sépare la réception de la demande de ralentissement ou d'arrêt des émissions est de T_a. Pendant ce temps, l'émetteur a poursuivi ses émissions, et a émis un nombre de blocs correspondant à la fenêtre. Calculons cette fenêtre :

– Temps d'émission d'un bloc :

$$T_b = \text{Volume / Débit} = (100 \times 8) / 155 \cdot 10^6 = 5 \cdot 10^{-6} \text{ s}$$

– Temps d'attente (si on admet une vitesse de propagation de $2 \cdot 10^8$ m/s) :

$$T_a = \text{Distance aller et retour / Vitesse} = 2 \cdot 10^5 / 2 \cdot 10^8 = 10^{-3} \text{ s}$$

– Fenêtre :

$$W = T_a/T_b = 10^{-3} / 5 \cdot 10^{-6} = 200 \text{ blocs}$$

Lors de la perte d'un bloc par saturation des buffers, l'émetteur continue d'envoyer 200 blocs avant de recevoir l'information de demande de ralentissement. Devant une telle fenêtre, le temps de réaction est trop important. De plus, le ralentissement du débit de l'émetteur est incompatible avec le transport d'information dite temps réel comme la voix (réseaux voix/données).

Le contrôle de flux par fenêtre n'est efficace que pour des débits relativement faibles, ce qui l'élimine dans la plupart des réseaux modernes. Dans ces réseaux aucun contrôle de flux, interne au réseau, n'est réalisé. Cependant, les débits d'accès aux réseaux sont généralement faibles devant les débits internes au réseau, il est donc envisageable d'instaurer un contrôle de flux à l'interface usager. Une autre solution, adoptée par TCP/IP, consiste à confier aux systèmes d'extrémité cette tâche (figure 4.39).

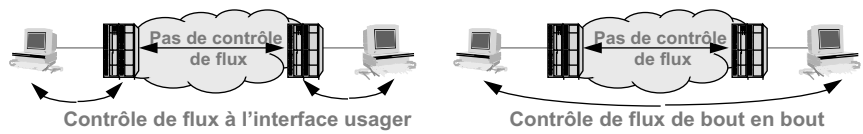


Figure 4.39 Le contrôle de flux et débit élevé.

© Dunod – La photocopie non autorisée est un délit

4.4 LA SIGNALISATION

4.4.1 Définition

Pour réaliser un transfert de données, il est nécessaire d'établir une liaison, de la superviser durant l'échange et enfin de libérer les ressources monopolisées en fin de communication. L'ensemble de ces informations nécessaires à la fourniture d'un service de télécommunication constitue la **signalisation**.

On distingue deux procédés pour l'acheminement des informations de signalisation :

– la signalisation dans la bande (*in band*) ;
– la signalisation par canal dédié ou hors bande (*out band*).

4.4.2 La signalisation dans la bande

Dans la signalisation dite dans la bande, les informations de signalisation empruntent le même canal de communication que les unités de données. Ces informations sont transportées dans une structure de bloc identique à celle utilisée pour le transfert de données. Un champ spécifique, dénommé type d'unité de données, doit alors identifier la nature des informations transportées : informations de signalisation ou données. La figure 4.40 illustre ce principe.

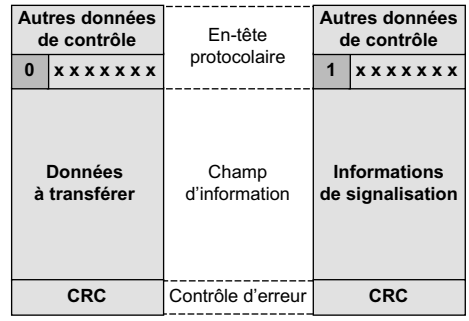


Figure 4.40 Unité de données et unité de signalisation.

Dans cet exemple (figure 4.40) le premier bit du champ type d'unité de données permet de distinguer une unité de données à transférer (bit à 0), d'une unité de transport d'informations de signalisation (bit à 1). Les autres bits de ce champ peuvent être utilisés pour distinguer différents types d'information de signalisation. Le champ données est alors généralement vide, il peut cependant contenir des informations complémentaires comme la cause de rupture de la liaison logique...

Une autre possibilité, utilisée par le système de téléphonie d'Amérique du Nord, consiste à substituer à des bits de données, des bits de signalisation (signalisation par vol de bits). Ainsi, par exemple, ce système substitue, tous les six échantillons de voix, un bit de signalisation au bit de poids faible de l'échantillon de parole. Ce système n'altère pas de façon audible la qualité de la voix, et offre un débit d'un peu plus de 1 kbit/s aux informations de signalisation.

La signalisation dans la bande est un procédé simple, mais la distinction des deux types d'unité de données pénalise le processus de commutation (interprétation des en-têtes). De ce fait, les informations transportées seront réduites à ce qui est strictement nécessaire, la signalisation est dite pauvre.

4.4.3 La signalisation hors bande

La signalisation par canal dédié ou hors bande distingue deux voies : une voie pour le transfert de données (canal de données) et une voie pour les informations de signalisation (canal de signalisation). Ces deux voies pouvant être physiquement distinctes ou utiliser le même support physique, on parle alors de **voies virtuelles**[12]. Dans un tel système, illustré figure 4.41, le canal de signalisation est établi en permanence, alors que le canal de données peut n'être établi qu'à la demande.

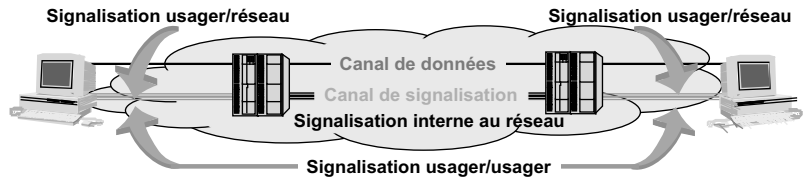


Figure 4.41 La signalisation par canal dédié à la signalisation.

La signalisation par canal dédié utilise un protocole différent du protocole de transfert de données : le protocole de signalisation. La mise en œuvre de deux protocoles, l'un de transfert de données l'autre de gestion de la communication autorise un traitement différencié, chaque protocole est traité par une instance de programme différente. De ce fait, indépendamment du gain en performance, le protocole de signalisation peut être parfaitement adapté aux exigences de la communication et être enrichi de nombreuses informations. Dans ce système, on distingue différents types de signalisation (figure 4.41) :

- la **signalisation usager/réseau**, chargée essentiellement de l'établissement de la liaison usager/réseau et de sa supervision ;
- la **signalisation interne au réseau** qui permet l'établissement d'une liaison à travers le réseau (routage ou acheminement) et de la contrôler durant l'échange ;
- la **signalisation usager/usager** dite aussi de **bout en bout**. Cette signalisation permet aux entités distantes de s'échanger des informations hors du protocole de transmission. C'est ainsi qu'il est possible de transmettre, via le protocole usager/usager de petites quantités d'information en l'absence de toute communication établie, comme, dans les réseaux téléphoniques, le numéro de téléphone de l'appelant.

Le Réseau téléphonique numérique à intégration de service (**RNIS**) met en œuvre ce type de signalisation. Cette approche est aussi utilisée dans tous les protocoles de transfert dits à haut débit comme le **Frame Relay**[13] ou l'**ATM** (protocoles issus des travaux sur le RNIS Large Bande).

12. Nous montrerons au chapitre 5, lors de l'étude du multiplexage, comment sur une même voie physique on peut réaliser plusieurs canaux de communication (voies logiques).
13. Voir chapitre 14, *Les protocoles de cœur de réseau*.

© Dunod – La photocopie non autorisée est un délit

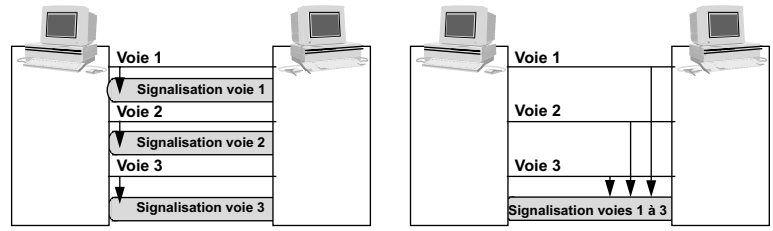


Figure 4.42 La signalisation par canal dédié.

Lorsque le support de communication est capable d'acheminer plusieurs communications, la signalisation des différentes communications peut être acheminée par un canal dédié à la signalisation de chacune des voies de communication. On parle alors de signalisation voie par voie ou **CAS**, *Channel Associated Signalling* (figure 4.42 gauche). Elle peut aussi être acheminée dans un canal commun à toutes les voies de communication, on parle alors de signalisation par **canal sémaphore** ou **CCS**, *Common Channel Signalling* (figure 4.42 droite).

Le réseau téléphonique commuté utilise une signalisation de type CAS, alors que le réseau téléphonique à intégration de service met en œuvre une signalisation de type CCS.

4.5 L'ÉTUDE SUCCINCTE D'UN PROTOCOLE DE TRANSMISSION (HDLC)

4.5.1 Généralités

HDLC (*High Level Data Link Control*) est un protocole ligne dit de **point à point**. Dérivé de SDLC (*Synchronous Data Link Control*) d'IBM, il a été normalisé par le CCITT (UIT-T) en 1974.

L'unité de transfert d'HDLC est la trame (*Frame*), chaque trame est délimitée par un caractère spécifique : le fanion ou *Flag*. Ce caractère est le seul caractère spécial utilisé par le protocole. Le fanion est aussi employé pour maintenir, en l'absence de données à transmettre, la synchronisation entre les trames. La figure 4.43 schématise une liaison HDLC, les symboles « F » représentent les fanions envoyés durant les silences pour maintenir la synchronisation. L'entité primaire désigne celui qui a initialisé la communication. Quand chaque entité peut initialiser la communication et émettre des commandes, le mode de fonctionnement est dit **équilibré**.

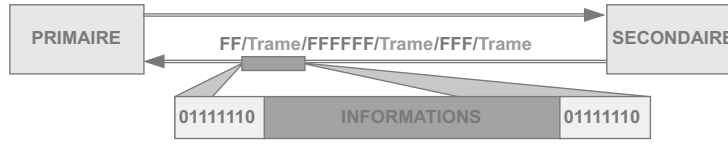


Figure 4.43 La liaison HDLC.

HDLC est un protocole qui utilise un mode de signalisation dans la bande. À cet effet, on distingue trois types de trames (figure 4.44).

Les trames d'information ou trames **I** assurent le transfert de données ; les trames de supervision ou trames **S** (*Supervisor*) le contrôlent (accusé de réception...), les trames non numérotées ou trames **U** (*Unnumbered*) supervisent la liaison. Les trames U sont, en principe, des trames de signalisation.

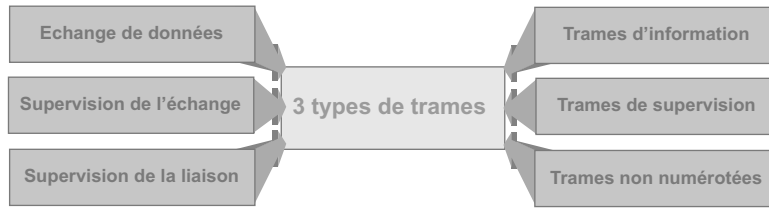


Figure 4.44 Les fonctions et trames correspondantes d'HDLC.

4.5.2 La structure de la trame HDLC

Le type de la trame émise (information, supervision ou contrôle de liaison) n'est pas distingué par un caractère particulier mais par une combinaison de bit (**protocole orienté bit**) Ce champ de bits est dit champ de commandes ou de contrôle. La structure de la trame est donnée par la figure 4.45.



Figure 4.45 La structure générale de la trame.

Utilisé à l'origine dans une relation maître/esclave, un seul champ d'adresse était alors nécessaire. Il désignait le terminal auquel on transmettait des données, ou le terminal qui transmettait des données. L'échange ne pouvant avoir lieu qu'entre un terminal (esclave) et la machine maître, il n'y avait aucune nécessité d'un second champ d'adresse.

Le fanion, constitué de huit éléments binaires (01111110), délimite la trame : fanion de tête et fanion de queue, lequel peut faire office de fanion de tête de la trame suivante. La transparence est réalisée selon la technique dite du **bit de bourrage**.

Le champ commande, 8 ou 16 bits selon que les compteurs de trames sont sur 3 ou 7 bits, identifie le type de trame. Le paragraphe suivant détaille et explique les différentes fonctions de ce champ. Le champ informations est facultatif, il contient les informations transmises.

Enfin, le champ **FCS** (*Frame Check Sequence*), champ de contrôle d'erreur, contient sur deux octets le reste de la division polynomiale (CRC) du message transmis (Adresse, Commande, Informations) par le polynôme générateur $x^{16} + x^{12} + x^5 + 1$. Le CRC, calculé à l'émission, est vérifié à la réception.

4.5.3 Les différentes fonctions de la trame HDLC

Le protocole HDLC distingue trois types de trames, identifiés par le champ de commande. La structure et la signification des sous-champs du champ de commande sont données par la figure 4.46.

Les trames d'information (I) contiennent un champ de données. Les champs notés N(s), N(r) correspondent, pour chaque extrémité de la liaison, à un compteur de trames d'information émises N(s) ou reçues N(r). Les trames de supervision (S) permettent de superviser l'échange de données. Le champ N(r) permet d'identifier la trame acceptée ou refusée. Les trames non numérotées (U, *Unnumbered*) gèrent la liaison (établissement, libération...). Elles sont dites non numérotées car elles ne contiennent aucun compteur. Les bits **S** et **U** identifient la commande.

© Dunod – La photocopie non autorisée est un délit

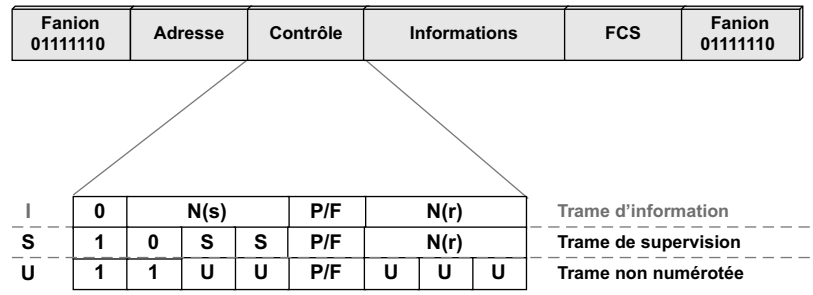


Figure 4.46 La structure du champ de commande (bits de poids faible devant).

Le champ de commande comporte trois champs :

– Un champ binaire qui identifie le type de trame (I, S, U) et la commande.
– Un bit de contrôle de la liaison P/F. Ce bit est positionné à 1 par le primaire lorsque celui-ci sollicite une réponse du secondaire (P = 1 pour *Poll sollicitation*). Le secondaire répond avec F = 1 (*Final*) à la sollicitation du primaire. C'est le cas, par exemple, en fin de fenêtre (figure 4.47), le bit P = 1 oblige le correspondant à répondre. Le secondaire répond par un acquittement avec F = 1, ou avec des trames d'information avec F = 0, sauf pour la dernière (F = 1).
– Des champs compteurs N(s), N(r). Chaque station maintient à jour deux compteurs, un compteur de trames émises, N(s) et un compteur de trames attendues. Le champ N(s) est utilisé pour la numérotation des trames émises, alors que le compteur N(r) sert à l'acquittement, il contient le numéro de la prochaine trame attendue : N(r) = x acquitte les (x – 1) trames précédentes.

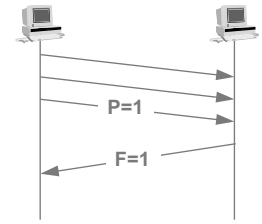


Figure 4.47 Utilisation du bit P/F.

La figure 4.48 détaille les principales commandes utilisées et précise les combinaisons de bits correspondantes.

Les modes de fonctionnement dépendent de deux données : la taille du champ de commande et la capacité d'initiative des stations secondaires. Le mode standard est caractérisé par un champ de commande sur 8 bits. La numérotation des trames sur 3 bits autorise une fenêtre théorique de huit trames, en pratique sept. Le mode étendu possède un champ de commande sur 16 bits, la numérotation des trames est sur 7 bits, ce qui porte la limite de la fenêtre à 128 trames, en pratique 127. Ce dernier mode est utilisé dans les réseaux locaux (taux d'erreur faible) et dans les liaisons satellites (temps de transit important).

Format	Commandes	Réponses		Champ Commande				
			Hex*.	8 7 6	5	4 3 2		1
I	INFORMATION		xx	N(r)	P/F	N(s)		0
S	RR		x1	N(r)	P/F	0 0	0	1
	RNR		x5	N(r)	P/F	0 1	0	1
	REJ		x9	N(r)	P/F	1 0	0	1
U	SABM		2F/3F	0 0 1	P	1 1	1	1
	SABME		6F/7F	0 1 1	P	1 1	1	1
	DISC		43/53	0 1 0	P	0 0	1	1
		UA	63/73	0 1 1	F	0 0	1	1
		FRMR	87/97	1 0 0	F	0 1	1	1
		DM	0F/1F	0 0 0	F	1 1	1	1

* les valeurs, exprimées en hexadécimal, dépendent de la position du bit P/F

I	**I**nformation	Trame d'information.
RR	**R**eceive **R**eady	Prêt à recevoir, accusé de réception utilisé lorsque le récepteur n'a pas de trame d'information à envoyer.
RNR	**R**eceive **N**ot **R**eady	Non prêt à recevoir, le récepteur demande à l'émetteur d'arrêter ses émissions, et acquitte les trames acceptées N(r) –1.
REJ	**Rej**ect	Rejet, demande de retransmission à partir de la trame N(r).
DISC	**DISC**onnect	L'un des ETTD prend l'initiative de la rupture de connexion.
SABM	**S**et **A**synchronous **B**alanced **M**ode	Commande permettant le passage en mode équilibré, il n'y a pas de notion de primaire et de secondaire. Chaque station peut émettre sans autorisation.
SABME	**S**et **A**synchronous **B**alanced **M**ode	Commande identique à la précédente, mais passage en mode étendu (numérotation modulo 128).
UA	**U**nnumbered **A**cknowledge	Acquitte une trame non numérotée.
FRMR	**Fram**e **R**eject	Informe de la réception d'une trame qui n'a pu être acceptée.
DM	**D**isconnect **M**ode	Indique que la station est déconnectée.

Figure 4.48 Les principales commandes d'HDLC.

La capacité d'initiative des stations caractérise deux modes : le mode normal et le mode asynchrone. Dans le mode *Normal Response Mode* (**NRM**), la commande est centralisée, les stations n'ont aucune initiative (relation maître/esclave). Le mode asynchrone peut être dissymétrique (**ARM**, le secondaire peut émettre sans invitation) ou symétrique (**ABM**, chaque extrémité est primaire en émission et secondaire en réception).

4.5.4 Le fonctionnement d'HDLC

L'établissement et la rupture de connexion

La liaison étant dans l'état logique déconnecté (figure 4.49), le primaire demande l'établissement d'une liaison par l'envoi de trames non numérotées (U) de type SABM (mode équilibré ou LAP-B, *Link Access Protocol Balanced*) ou SARM (mode maître/esclave ou LAP), le bit P est positionné à 1 (il aurait pu être à 0). Le secondaire, s'il accepte la connexion, répond par la trame non numérotée UA (*Unnumbered Acknowledge*), le positionnement du bit F, dans la réponse, est identique à celui du bit P (*Poll*) de la requête. La liaison est établie, l'échange d'information peut alors commencer.

© Dunod – La photocopie non autorisée est un délit

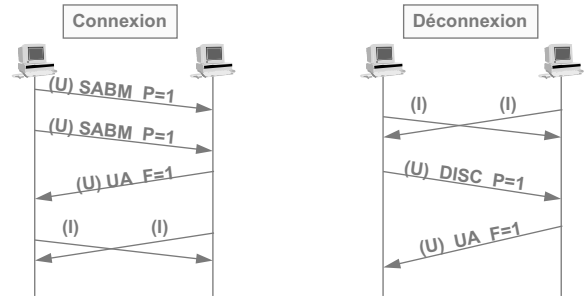


Figure 4.49 La gestion de la connexion sous HDLC.

La liaison est dans l'état logique connecté. Le primaire émet une demande de déconnexion DISC (figure 4.49), le bit P est positionné indifféremment à 1 ou à 0. Le secondaire accuse réception avec UA, la valeur du bit F correspond à celle du bit P de la trame DISC. La liaison est rompue. L'échange de fanions se poursuit pour maintenir la synchronisation tant que la liaison physique n'est pas rompue.

L'échange des données

La figure 4.50 illustre les différentes étapes d'un échange HDLC.

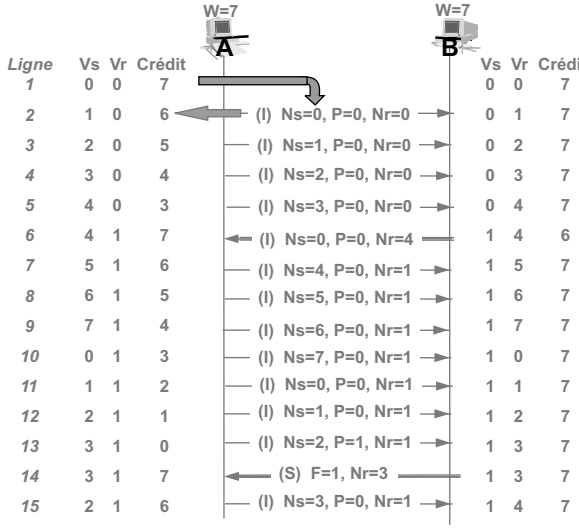


Figure 4.50 L'échange de données et la gestion de la fenêtre.

Chaque entité correspondante entretient deux compteurs dits **variables d'état**, le compteur V(s) indique le numéro de la prochaine trame à émettre, le compteur V(r) le numéro de la trame attendue. Après la phase de connexion, les compteurs sont initialisés à zéro de chaque côté, la fenêtre étant de 7 (dans cet exemple), chaque entité a un crédit d'émission de 7 (ligne 1). En ligne 2, la machine A émet une trame, les compteurs N(s) et N(r) contiennent respectivement les valeurs V(s) et V(r) de la ligne 1. Les valeurs V(s), V(r) et crédit de la ligne 2 correspondent aux valeurs, mises à jour

après émission de la trame pour la machine A et après sa réception pour la machine B. C'est-à-dire, que dans la figure, les valeurs des compteurs correspondent toujours aux valeurs mises à jour après réception ou émission d'une trame. Les lignes 3, 4, 5 n'appellent aucun commentaire particulier. En ligne 6, la machine B émet une trame. Son compteur V(r) contient la valeur de la trame attendue, ici 4, il correspond pour la machine B à un acquittement des [N(s) –1] trames émises, soit ici les trames 0, 1, 2 et 3. Les mémoires tampons sont libérées, la fenêtre est réinitialisée (crédit de 7).

Cette technique d'acquittement simultané à l'envoi de données, dite du *piggybacking*, optimise l'échange de données et évite un blocage de la fenêtre.

L'échange se poursuit, la fenêtre de A s'incrémente. En ligne 12, le crédit n'est plus que d'une trame, il sera nul à l'émission de la trame suivante (ligne 13). La trame émise demande alors un acquittement à B. N'ayant pas de données à envoyer, B acquitte les trames reçues, avec une trame de supervision RR (*Receive Ready*). Il indique à A que cette trame est la réponse à sa demande en positionnant le bit F à 1.

La gestion des temporisations

Deux temporisateurs (figure 4.51) sont gérés par les entités communicantes :

- La **temporisation de retransmission** (**T1** ou **RTO**, *Retransmission Time Out*) à chaque trame émise l'émetteur initialise le temporisateur T1. Si, à l'échéance de ce temporisateur ou délai de garde, l'émetteur n'a pas reçu de trame d'information ou d'acquittement de son correspondant, il réémet la trame supposée perdue.
- **La temporisation d'acquittement** (**T2**) correspond au délai maximum au bout duquel, le récepteur, s'il n'a pas de données à transmettre, doit envoyer un acquittement à son correspondant.

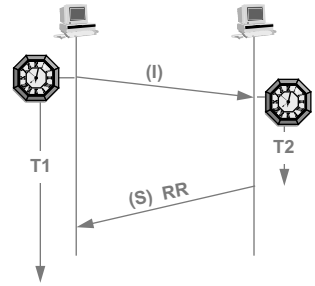


Figure 4.51 La gestion des temporisations.

La gestion des erreurs

La figure 4.52 illustre la reprise sur erreur. Supposons la trame 2 erronée, elle est ignorée par le récepteur. La trame 3 est alors reçue hors séquence, elle est rejetée. La machine B émet une trame de supervision de rejet (REJ, *Reject*) en indiquant à A à partir de quelle trame il doit reprendre la transmission [N(r) = 2]. Toutes les trames dont la valeur de N(s) est supérieure à 2 sont alors rejetées (rejet simple).

La machine A reprend la transmission à partir de la trame 2 (N(s) = 2). Si, suite à la trame erronée, A n'avait plus de données à émettre, B n'aurait pas détecté le déséquencement. C'est A qui, à l'échéance du temporisateur T1, aurait pris l'initiative de retransmettre la trame 2.

© Dunod – La photocopie non autorisée est un délit

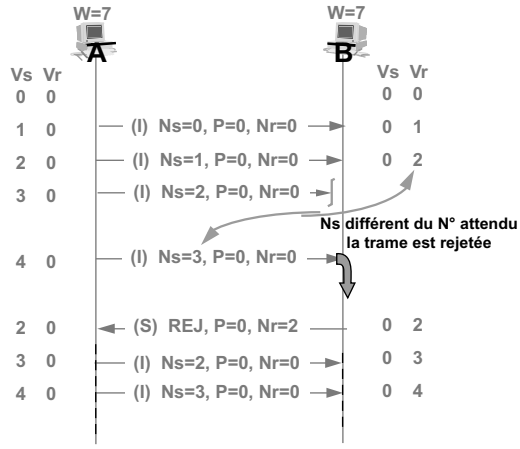


Figure 4.52 La gestion des erreurs.

La gestion du contrôle de flux

HDLC utilise le contrôle de flux implicite. La fenêtre est paramétrée à l'installation du logiciel. En cas de saturation des tampons de réception, le récepteur, ici dans la figure 4.53 la machine B, rejette la trame en excès et informe A de son incapacité temporaire à accepter de nouvelles données. Il émet la trame « S » **RNR** (*Receive Not Ready*) avec le compteur N(r) positionné au numéro de la trame reçue et rejetée.

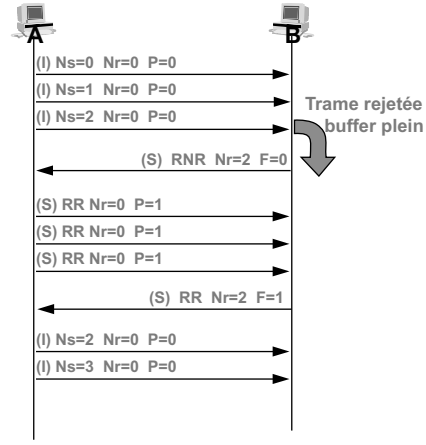


Figure 4.53 La gestion du contrôle de flux.

La machine A prend en compte cette demande et interroge (*poll*) régulièrement (tous les T1) la machine B, pour d'une part signaler sa présence et d'autre part formuler auprès de B une demande de reprise de transmission à l'aide de la trame « S » **RR**, *Receive Ready*, avec le bit P à 1.

Lorsque B peut reprendre la réception, il le signale à l'émetteur en accusant réception à l'aide de la trame « S » RR. Le compteur N(r) contient le numéro à partir duquel la retransmission doit reprendre. A avait positionné le bit P à 1, la réponse de B est émise avec le bit F à 1.

L'ambiguïté du bit P/F

Rappelons qu'à l'origine HDLC était utilisé comme protocole de ligne dans les systèmes informatiques importants. Dans ces systèmes, c'est l'ordinateur central qui contrôle le dialogue (politique d'accès centralisée), la relation est dite maître/esclave. L'ordinateur interroge les terminaux (*Polling*, P = 1), le terminal interrogé doit répondre, dans la dernière trame de sa réponse le bit F est mis à 1 (*Final*). Ces appellations ont été conservées.

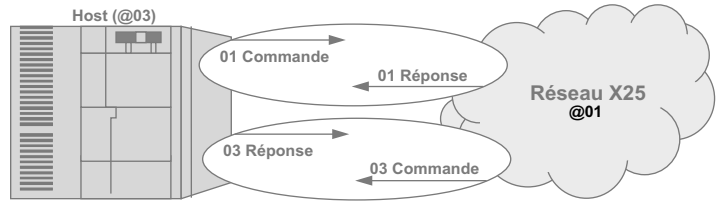


Figure 4.54 La gestion du bit P/F.

En mode équilibré, chaque extrémité de la liaison peut, en positionnant le bit P à 1, prendre l'initiative de solliciter une réponse de l'autre extrémité. Si les deux entités formulent, en même temps, une demande de réponse, le protocole ne distinguant pas le bit P du bit F, chaque entité prend la demande de l'autre comme la réponse à sa propre demande.

La version d'HDLC en mode équilibré est utilisée en protocole ligne, c'est-à-dire sur une liaison point à point : le champ adresse est inutile. Dans ces conditions, il est possible d'utiliser le champ adresse comme extension du champ de commande afin d'identifier le sens de la requête. Cette possibilité est utilisée pour contrôler le dialogue entre un réseau et son abonné (figure 4.54) :

– dans le sens Host/Réseau, le champ adresse contient la valeur binaire 01,
– dans le sens Réseau/Host, le champ adresse contient la valeur binaire 11.

Cette utilisation du champ adresse est conforme à l'usage traditionnel du champ adresse. En effet, le champ adresse contient l'adresse de l'extrémité considérée comme l'esclave dans l'échange. Pour interpréter correctement le champ adresse, il convient donc de bien définir si la trame est une commande ou une réponse (figure 4.48). Par exemple, lors de l'émission d'une commande vers le réseau (bit P = 1), le champ adresse contient la valeur « 01 » qui est l'adresse du réseau considéré alors comme l'esclave (figure 4.54).

4.5.5 Les différentes versions du protocole HDLC

Normalisé en 1976 (CCITT et ISO) HDLC a inspiré de nombreuses les variantes :

– mode **LAP** (*Link Access Protocol*), fonctionnement sur sollicitation du primaire ;
– mode **LAP-B** (B pour *Balanced*, mode équilibré), dans ce type de liaison, il n'y a pas de primaire prédéfini, chaque station peut être primaire ;
– mode **LAP-D** (D pour canal D), ce protocole similaire à LAP-B est utilisé pour la signalisation dans les réseaux téléphoniques numériques (RNIS, Réseau Numérique à Intégration de Service) ;

© Dunod – La photocopie non autorisée est un délit

– mode **LAP-M** (M pour Modem), dérivé de LAP-D, il est mis en œuvre pour des connexions PC-Calculateur hôte, ce protocole est utilisé entre modems conformes aux recommandations V.42 et V.42 bis ;
– mode **LAP-X**, mode semi-duplex dérivé de LAP-D, est utilisé dans le télétex.

Notons que **SDLC**, *Synchronous Data Link Control*, utilisé dans l'environnement **IBM SNA**, *System Network Architecture*, est parfois présenté comme un sous-ensemble d'HDLC car moins riche ; cependant, il est plus logique de présenter HDLC comme une évolution de SDLC. SDLC ne fonctionne qu'en mode non équilibré.

4.5.6 HDLC et les environnements multiprotocoles

Dans un contexte multi-applications, deux applications peuvent utiliser un protocole de communication *X* et un autre couple d'applications un protocole *Y* (figure 4.55), Le transport des informations de chacune des liaisons applicatives ne peut être réalisé par HDLC. En effet, HDLC est certes un protocole de liaison de point à point, mais ne pouvant distinguer les données des protocoles *X* ou *Y*, il ne peut être utilisé que dans un environnement monoprotocole.

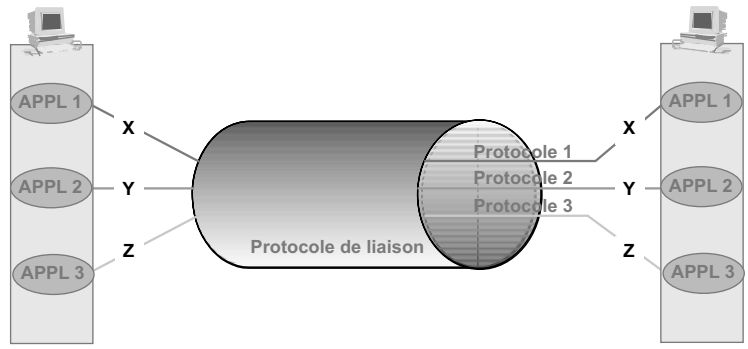


Figure 4.55 La liaison multiprotocoles.

Le protocole **PPP** (*Point to Point Protocol*), inspiré de HDLC remédie à cet inconvénient. À cet effet, un champ spécifique : Protocol_ID est inséré entre le champ commande et le champ données d'HDLC. PPP sera étudié au chapitre 9. Le format de trame représenté ci-dessous (figure 4.56) est dérivé de celui des trames UI (trame non numérotée d'HDLC), le champ adresse contient la valeur 0xFF et le champ commande 0x03 (trame UI), le champ Protocol_ID indique le protocole utilisé par les données transportées dans le champ données. On dit alors que le protocole *X* ou *Y* est encapsulé dans PPP.

Fanion 0x7E	Adresse 0xFF	Contrôle UI = 0x03	Protocol_ID 1 ou 2 octets	Données 0 à 1500 octets	FCS 2 octets	Fanion 0x7E

Figure 4.56 La trame PPP (format non numéroté).

4.6 CONCLUSION

HDLC, en version LAP-B, est utilisé dans les réseaux de type X.25. Les contrôles d'erreur et de flux sont effectués de point à point (nœud à nœud). Cette technique est efficace mais pénalise gravement

les performances d'HDLC. L'évolution des techniques réseaux (fibres optiques) rend les supports plus fiables (taux d'erreur plus faible) et autorise une simplification des protocoles. En confiant aux calculateurs d'extrémité (ceux qui sont connectés au réseau), les tâches de contrôle d'erreur et de contrôle de flux, la technique du relais de trames (*Frame Relay* ou LAP-F) permet des débits effectifs plus élevés (34 368 kbits/s).

La réalisation de liaisons point à point entre les systèmes d'information peut se révéler coûteuse au regard du temps d'utilisation. Aussi, indépendamment de la notion de protocole ou d'environnement multiprotocoles, il peut paraître intéressant d'examiner si une liaison peut être utilisée simultanément par plusieurs entités communicantes. C'est la notion de « mutualisation » des ressources ou de concentration de trafic que nous allons aborder au chapitre suivant.

EXERCICES

Exercice 4.1 Calcul de CRC

Calculez le CRC4 pour les données 1010010111, le polynôme générateur étant $x^4 + x^2 + x + 1$.

Exercice 4.2 Probabilité de recevoir un message erroné

On définit le taux d'erreur binaire ou TEB (T_e) comme le rapport du nombre de bits reçus en erreur au nombre total de bits reçus. Une transaction de 100 caractères ASCII est émise sur une liaison en mode synchrone à 4 800 bits/s avec un T_e de 10^{-4}.

Les erreurs sont supposées être distribuées aléatoirement, c'est-à-dire que la probabilité d'avoir un bit en erreur est la même pour tous les bits, et est égale à T_e. Déterminez la probabilité pour qu'un message reçu comporte au moins une erreur (P_e).

Exercice 4.3 Taux de transfert

Un fichier est transmis par blocs de 1 000 caractères codés en ASCII, avec un bit de parité (7+1), en mode synchrone sur une liaison à 9 600 bits/s. On suppose, en outre, que la transmission est effectuée en mode semi-duplex et la demande de retransmission instantanée. Calculez :

1. le taux de transfert des informations (TTI) ou débit effectif ;
2. le TTI avec erreur si on suppose un T_e de 10^{-4}.

Exercice 4.4 Échange de trames HDLC version LAP-B

La figure 4.57 représente les différentes étapes d'un échange LAP-B entre deux correspondants A et B. Il vous est demandé de le compléter. La colonne de droite vous indique l'action. Le « ? » signifie que c'est à vous d'indiquer l'action correspondante. Les valeurs des compteurs N(s) et N(r) indiquées dans les colonnes correspondent aux valeurs des variables d'état [V(s) et V(r)] mises à jour après l'action correspondante. La fenêtre est fixée à quatre dans les deux sens.

© Dunod – La photocopie non autorisée est un délit

Valeur des compteurs après l'échange (après émission et après réception)	A V(s)	A V(r)	Échange	B V(s)	B V(r)
Exemples de trames : Indiquer le type (I, U, S) Éventuellement la trame (REJ, SABME...) Les valeurs des compteurs Nr, Ns La valeur du bit P/F			(I) Ns=4 Nr=6 P=0 ⟶ (S) RNR Nr=3 P=0 ⟵		
Initialisation :	0	0		0	0
1) Ouverture en mode asynchrone normal					
2) Acceptation par B					
Échange :					
3) Trame d'information de A vers B					
4) Trame d'information de A vers B erronée					
5) Trame d'information de A vers B					
6) ?					
7) Trame d'information de A vers B					
8) Trame d'information de A vers B					
9) Trame d'information de B vers A					
10) Trame d'information de A vers B					
11) Trame d'information de A vers B					
12) Trame d'information de A vers B					
13) Trame d'information de A vers B					
14) ?					
Fermeture de la connexion :					
15) Demande de fermeture					
16) Acquittement par B					

Figure 4.57 L'échange LAP-B.

Chapitre **5**

Mutualisation des ressources

5.1 INTRODUCTION

Lors de la réalisation d'une liaison de transmission de données, le responsable réseau et télécoms d'une entreprise doit rechercher la meilleure solution en termes d'efficacité et de coût. Cet objectif d'optimisation des moyens de transmission et des coûts se concrétise par la recherche :

- du meilleur dimensionnement des moyens (nombre de lignes, nombre de terminaux...) ;
- du meilleur taux de transfert, obtenu par une éventuelle réduction du volume à transmettre (compression de données) ;
- de l'utilisation de protocoles efficaces (évolution d'HDLC vers le **Frame Relay)**
- d'une solution de partage des moyens entre plusieurs utilisateurs (mutualisation des ressources), c'est la concentration de trafic.

La concentration de trafic n'est réalisable que si chacune des sources d'information ne monopolise pas, de façon permanente, les ressources attribuées. La première étape de l'étude d'une solution de concentration consiste donc à évaluer, en le quantifiant, le trafic de chacune des sources puis à rechercher en fonction du type de relation à mettre en œuvre la meilleure solution.

5.2 LA QUANTIFICATION DE TRAFIC

5.2.1 Généralités

Prenons l'exemple d'une application de type conversationnel (échange questions/réponses entre un terminal et un ordinateur), si on examine le déroulement d'une session, limitée à un seul échange dans la figure 5.1, on constate que :

- la durée de la session est bornée dans le temps, le support libéré est alors utilisable par un autre utilisateur : c'est la **commutation** ;
- pendant la durée de la session le support n'est pas utilisé en permanence pour la transmission de données. Durant les instants de silence, le support est disponible pour un autre utilisateur ou une session différente : c'est la **concentration de trafic**.

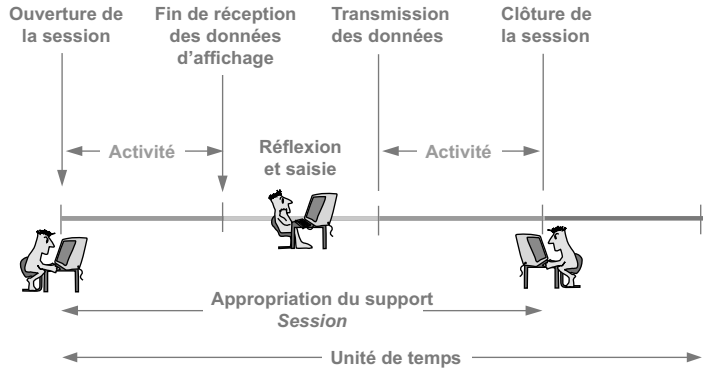


Figure 5.1 L'activité sur une ligne n'est pas permanente.

5.2.2 L'intensité de trafic et le taux d'activité

Évaluation des grandeurs

Ainsi, lors de l'étude d'un système de communication, deux critères essentiels, dépendant du type d'application, sont à prendre en compte (figure 5.2) :

– l'intensité de trafic qui caractérise la durée de la ou des session(s) ;
– le taux d'activité qui mesure l'utilisation effective du support.

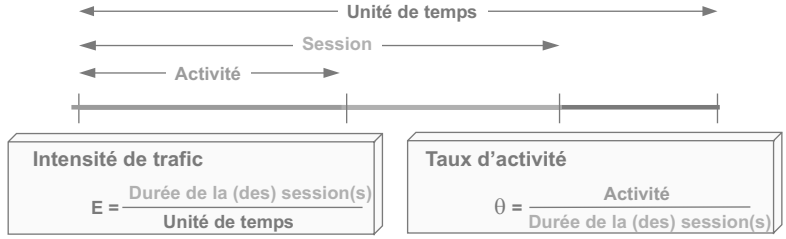


Figure 5.2 L'intensité de trafic et le taux d'activité.

L'intensité de trafic (E) et le taux d'activité (θ) varient de 0 à 1. On peut représenter la relation entre ces valeurs par un carré et déterminer quatre aires spécifiques (figure 5.3).

L'aire 1 correspond à une occupation de la ligne importante et une utilisation conséquente, le partage des ressources n'est pas envisageable.

L'aire 2 correspond aussi à une occupation de la ligne importante, mais à une utilisation faible. La bande passante de la ligne peut donc être partagée. La concentration ou le multiplexage, utilisation simultanée de la ligne par plusieurs correspondants, est envisageable.

L'aire 3 représente un secteur où la ligne est peu occupée, mais le trafic est important. Le partage de la bande n'est pas envisageable, mais le partage dans le temps de son utilisation est possible. La ressource peut être commutée d'un utilisateur à un autre (réseaux à commutation).

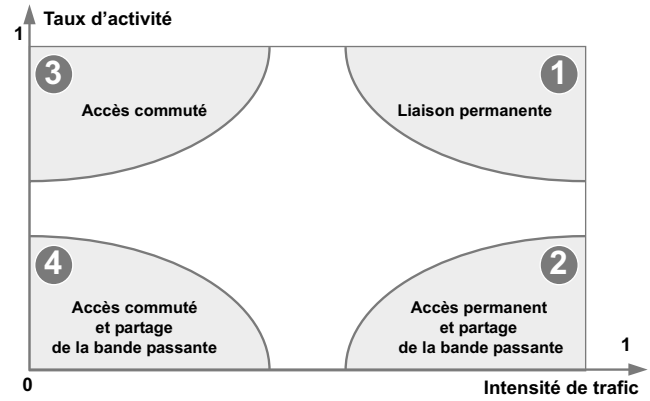


Figure 5.3 Les quatre aires définies par E et θ.

Dans la dernière aire, la ligne est peu occupée et faiblement utilisée, on peut imaginer un système de concentration de trafic auquel on accède via un réseau commuté, ce système servant d'interface avec un autre moyen où la bande pourra statiquement être partagée par plusieurs utilisateurs.

L'intensité de trafic et le dimensionnement des ressources

Lorsqu'un service est fourni à plusieurs utilisateurs et que ceux-ci ne l'utilisent pas en permanence, la question du dimensionnement des moyens d'accès se pose. C'est, par exemple, le cas des accès à Internet, le fournisseur d'accès (**ISP**, *Internet Service Provider*) doit déterminer le nombre de lignes et de modems qu'il doit mettre en service (figure 5.4).

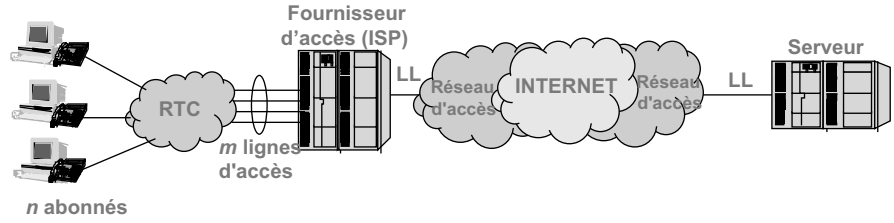


Figure 5.4 Détermination du nombre de lignes.

S'il dispose d'autant de lignes (m) que d'abonnés (n) aucun problème d'exploitation ne se présentera, mais il y aura vraisemblablement un « gâchis » de ressources. Si le nombre de lignes m est petit devant n, il y aura un taux de refus de mise en relation important. Le problème consiste donc à déterminer la valeur optimale du nombre de lignes nécessaires m pour que les abonnés aient une qualité de service acceptable (taux de refus faible et prédéterminé).

La relation entre intensité de trafic et ressources nécessaires a été étudiée par Erlang (mathématicien danois). Le dimensionnement des ressources nécessite de quantifier le trafic à écouler (intensité de trafic), puis en fonction d'un taux de refus prédéterminé (probabilité que toutes les ressources soient utilisées quand l'utilisateur $n+1$ désire se connecter) à définir le nombre de lignes m nécessaires.

© Dunod – La photocopie non autorisée est un délit

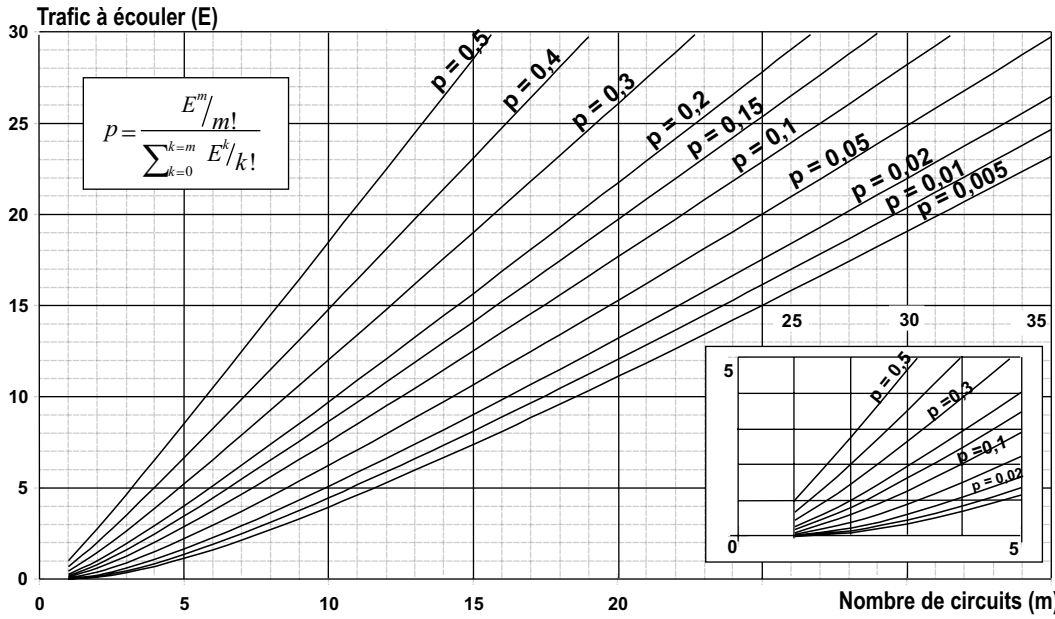


Figure 5.5 L'abaque d'Erlang dit à refus.

Ce problème peut être résolu par l'utilisation de tables dites **tables d'Erlang** ou d'abaques dits d'Erlang. La figure 5.5 représente un abaque d'Erlang. Connaissant le trafic (E), la probabilité de refus (ou taux de blocage) choisie (p), il est possible de déterminer le nombre de lignes nécessaire (m).

Le taux d'activité et la concentration de trafic

Lorsque la somme des activités (θ) de plusieurs utilisateurs est inférieure à 1, la rationalisation de l'utilisation des moyens conduit à envisager de leur faire partager un même support :

$$\sum_{i=1}^{i=n} \theta_i \leqslant 1$$

C'est la notion de concentration de trafic illustrée par la figure 5.6.

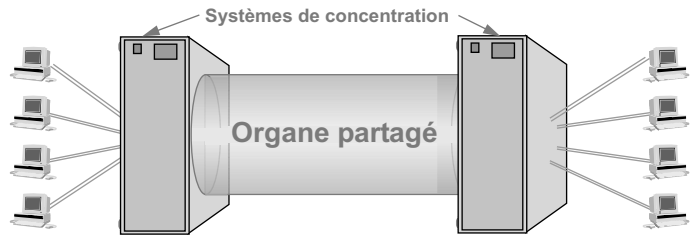


Figure 5.6 Principe de la concentration de trafic.

Selon la relation établie entre les *n* utilisateurs de l'organe partagé, on distingue (figure 5.7) :

– ceux qui permettent de relier *n* utilisateurs à un seul système (relation de 1 à *n* et de *n* à 1), ce sont les **concentrateurs** ;
– ceux qui n'autorisent qu'une relation de 1 à 1, ce sont les **multiplexeurs** ;
– enfin, ceux qui permettent une relation de 1 à 1 parmi *n* ou de 1 à *n*, ce sont les **réseaux**.

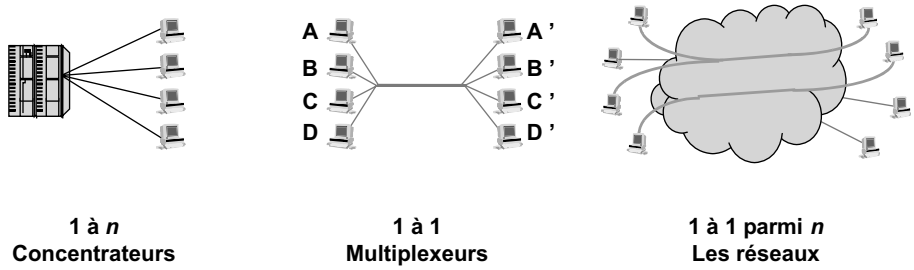


Figure 5.7 Les différents systèmes de concentration.

5.3 LES CONCENTRATEURS

5.3.1 Principe

Essentiellement utilisé en informatique traditionnelle, le concentrateur autorise l'utilisation d'une seule liaison pour l'accès de *n* terminaux à un ordinateur central (figure 5.8). Il analyse le contenu des blocs d'information reçus pour les diriger vers le seul terminal concerné, de ce fait, il n'est pas transparent aux protocoles.

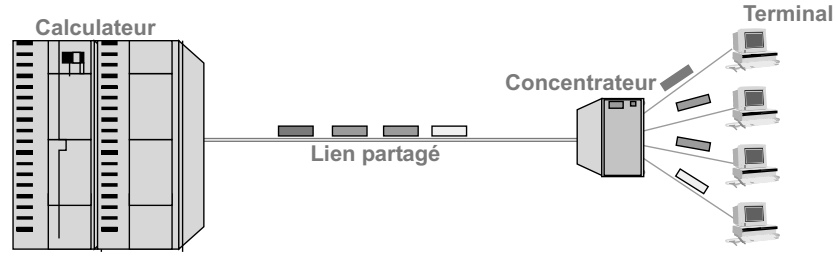


Figure 5.8 Principe de la concentration de terminaux.

Avec le développement des réseaux locaux, le concentrateur en tant qu'organe spécifique tend à disparaître. Un micro-ordinateur, désigné sous le terme de passerelle, assure la fonction de concentration. Un logiciel particulier, chargé sur un micro-ordinateur ou un poste de travail, émule le terminal passif traditionnel. Cette utilisation est illustrée par la figure 5.9.

© Dunod – La photocopie non autorisée est un délit

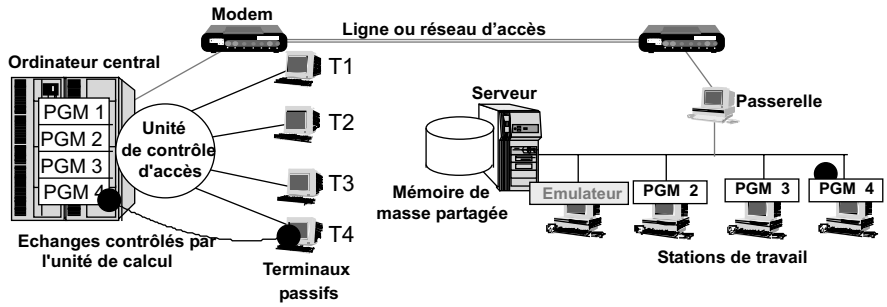


Figure 5.9 L'accès aux ordinateurs centraux via un réseau local.

5.3.2 Les fonctionnalités complémentaires, exemple d'application

Le concentrateur lorsqu'il reçoit un message l'analyse, interprète les données d'acheminement et retransmet, vers le destinataire, les informations reçues en effectuant éventuellement une conversion de protocole. C'est le cas notamment des points d'accès vidéotex. L'accès vidéotex est un exemple d'application correspondant à l'aire 4 de la figure 5.3, il est illustré figure 5.10 ou le **PAVI** (Point d'accès vidéotex) est un concentrateur dédié à ce type d'application.

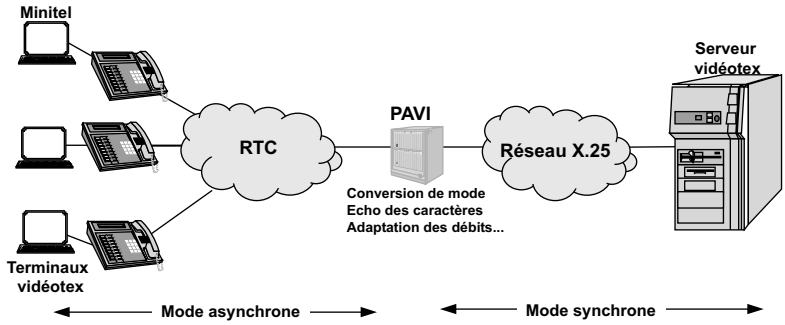


Figure 5.10 Une concentration particulière : l'accès vidéotex.

Le PAVI est un concentrateur qui, outre les fonctions de concentration, assure :

– La conversion de protocole, les caractères reçus en mode asynchrone en provenance du terminal Minitel (terminal asynchrone) sont regroupés en blocs de données (paquets) et émis en mode synchrone selon le protocole X.25[1] sur le réseau. De manière inverse, les données reçues sous forme de paquets par le PAVI, en provenance du serveur vidéotex, via le réseau X.25, sont désassemblées et transmises caractère par caractère au terminal Minitel (fonction **PAD**, *Packet Assembler Dissassembler*). Ce procédé évite que, sur le réseau X.25, on fasse 1 caractère = 1 paquet.

– La conversion de débit entre le terminal Minitel et le réseau X.25.

1. Le protocole X.25 est étudié au chapitre 14.

– L'écho distant du caractère, un terminal asynchrone n'affiche pas le caractère frappé sur le clavier mais celui reçu en écho de la machine hôte distante. Pour ne pas surcharger le réseau, c'est le PAVI qui assure l'écho de caractère.

Ainsi, un concentrateur peut assurer :

– l'écho de caractère (terminal asynchrone) ;
– le contrôle de la validité des informations ;
– la mise en forme des données ;
– la mémorisation des informations reçues (gestion de files d'attente) ;
– la gestion des terminaux (contrôleur d'écran, polling...).

5.4 LES MULTIPLEXEURS

5.4.1 Principe

Le multiplexeur est un équipement qui met en relation un utilisateur avec un autre par l'intermédiaire d'un support partagé par plusieurs utilisateurs. Un multiplexeur *n* voies simule, sur une seule ligne, *n* liaisons point à point. Chaque voie d'entrée est dénommée voie incidente, le support partagé voie composite (figure 5.11).

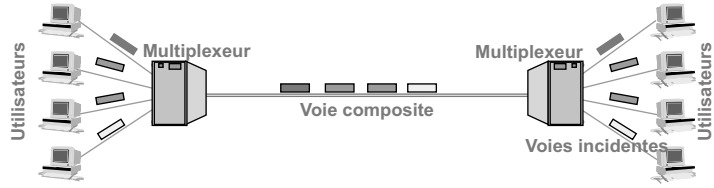


Figure 5.11 Principe du multiplexage.

L'opération de regroupement des voies incidentes sur un même support s'appelle le multiplexage. Le démultiplexage consiste à restituer à chaque destinataire les données qui lui sont destinées. La figure 5.12 représente une liaison par multiplexeur. Un MUX (abréviation utilisée pour désigner un multiplexeur) est un système symétrique, il comporte à la fois un organe de multiplexage et un organe de démultiplexage (liaison *full duplex*).

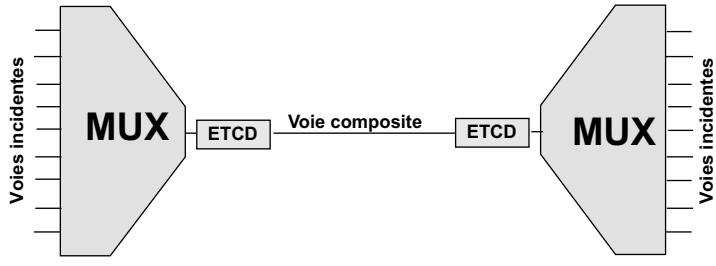


Figure 5.12 La représentation symbolique d'une liaison multiplexée.

© Dunod – La photocopie non autorisée est un délit

Le partage de la voie composite peut être un partage :

– de la bande disponible, chaque voie dispose en permanence d'une fraction de la bande disponible, c'est le **multiplexage fréquentiel** ou **spatial** ;
– du temps d'utilisation de la voie, chaque voie utilise durant un temps prédéterminé toute la bande disponible, c'est le **multiplexage temporel**.

5.4.2 Le multiplexage spatial

Principe

Le multiplexage fréquentiel (**FDM**, *Frequency Division Multiplexing*) correspond à une juxtaposition fréquentielle de voies et à une superposition des signaux dans le temps. La bande passante du support est divisée en canaux (voies). Chaque voie est modulée (transposition de fréquence) par une porteuse différente. Le démultiplexage correspond, à l'aide de filtres, à l'extraction de chacune des voies (voies spatiales) puis à la démodulation de chaque signal. La figure 5.13 illustre le principe d'un multiplexeur fréquentiel.

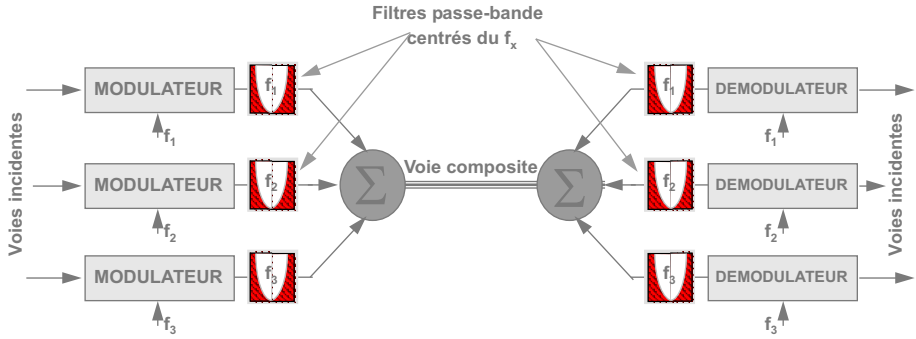


Figure 5.13 Principe du multiplexage fréquentiel.

Entre chaque voie ou canal, un espace de fréquence, dit **bande de garde**, sépare les canaux et évite l'intermodulation (figure 5.14), de plus, chaque voie dispose en permanence de la ressource qui lui est affectée ; si un utilisateur n'utilise pas son canal, la bande correspondante est perdue. L'efficacité d'un tel système reste faible (0,2 à 0,3), le multiplexage fréquentiel n'est plus utilisé qu'en association avec d'autres techniques.

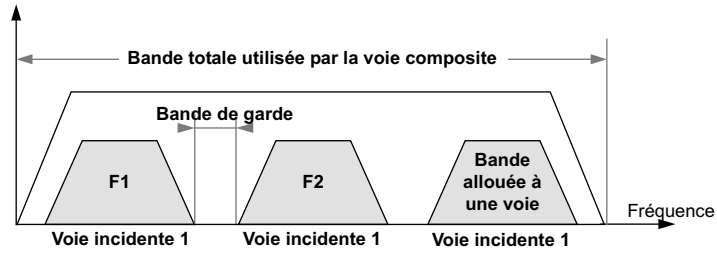


Figure 5.14 Le partage de fréquence par les différentes voies.

Avant l'apparition des techniques de numérisation, le multiplexage fréquentiel a été utilisé pour constituer les premiers réseaux de téléphonie. L'unité de base ou voie basse vitesse (une communication téléphonique, 300-3 400 Hz) a une largeur de bande de 4 kHz. Les voies basse vitesse sont multiplexées pour former un groupe de voies dit groupe primaire, ce dernier est lui-même multiplexé pour former un groupe secondaire... Ces regroupements ont formé la hiérarchie analogique comme indiquée dans la figure 5.15.

Groupe	Bandes de fréquences	Nombre de voies téléphoniques
Primaire	60 à 108 kHz	12
Secondaire	312 à 552 kHz	60
Tertiaire	812 à 2 044 kHz	300
Quaternaire	8 516 à 12 388 kHz	900

Figure 5.15 La hiérarchie analogique.

Le multiplexage de longueur d'onde

Les liaisons optiques mettent en œuvre un cas particulier du multiplexage fréquentiel (figure 5.16) : le multiplexage de longueur d'onde (**WDM**, *Wavelength Division Multiplexing*). À l'origine, seules les fenêtres courantes de 1 300 et 1 550 nm ont été utilisées autorisant, par exemple, l'exploitation de quatre longueurs d'ondes dans la fenêtre de 1 530 à 1 560 nm (bande C) soit une liaison à 10 Gbit/s (quatre canaux de 2,5 Gbit/s) sur une distance de 250 km. Cette technique est limitée par la dispersion chromatique (différence de coefficient de vélocité en fonction de la longueur d'onde).

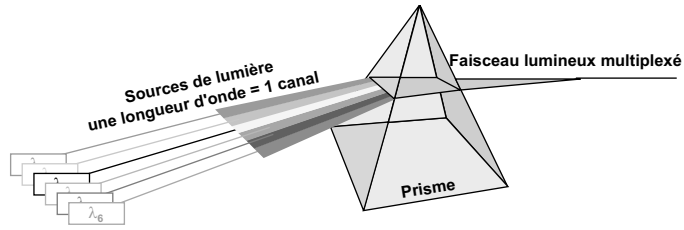


Figure 5.16 Principe du multiplexage de longueur d'onde.

Les réalisations actuelles autorisent le multiplexage de 4, 16 et 32 longueurs d'onde avec des trains numériques incidents de 2,5, 10 voire 40 Gbit/s (figure 5.17). Les technologies du type *Dense WDM* (**DWDM**) permettent de réduire l'écartement entre les canaux utilisés de 1,6 nm à 0,2 nm et laisse espérer l'utilisation de 1 000 longueurs d'onde dans un même multiplex. Aujourd'hui, on a pu réaliser des liaisons à 3 Tbit/s sur 7 300 km en utilisant 300 canaux à 10 Gbit/s et en laboratoire 10 Tbit/s sur 100 km avec 256 canaux à 40 Gbit/s. La figure 5.17 illustre un système de transmission en multiplexage de longueurs d'onde. Le faisceau lumineux est régénéré par un amplificateur optique à fibre dopée à l'erbium (**EDFA**, *Erbium Doped Fibre Amplifier*). Les pas de régénération sont d'environ 100 km pour les liaisons terrestres et de 50 à 80 km pour les liaisons océaniques. Une liaison terrestre de 450 km à 160 Gbit/s (10 faisceaux de 1,6 Gbit/s), sans aucune régénération, a déjà été réalisée.

© Dunod – La photocopie non autorisée est un délit

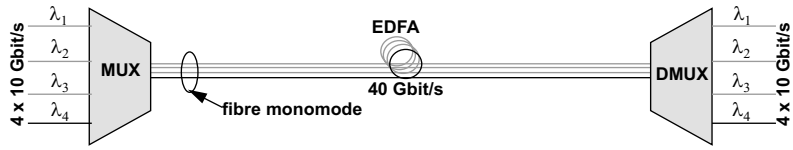


Figure 5.17 Principe d'une liaison WDM.

5.4.3 Le multiplexage temporel

Principe

Quand le taux d'activité est inférieur à un, entre deux épisodes de transfert, il existe des espaces de temps (silences) qui peuvent être utilisés par d'autres utilisateurs. Les multiplexeurs temporels relient une voie incidente d'entrée à une voie incidente de sortie durant un intervalle de temps prédéterminé. Cet intervalle de temps ou **IT**, réservé à un couple émetteur/récepteur, constitue une voie temporelle (figure 5.18).

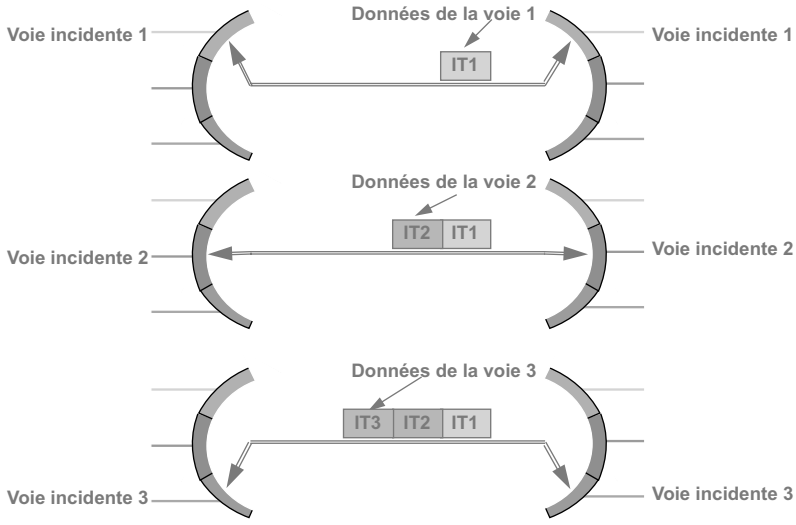


Figure 5.18 Principe du multiplexage temporel.

Dans le premier schéma de la figure 5.18, le couple de multiplexeurs met en relation les utilisateurs raccordés aux voies identifiées « voies incidentes 1 » ; l'intervalle de temps suivant, les utilisateurs raccordés aux voies 2, puis ceux raccordés aux voies 3. La restitution des différentes voies nécessite l'identification de celles-ci. Dans le système décrit, chaque voie est toujours scrutée à période constante, à chaque IT est donc associé une position dans la trame, c'est le multiplexage de position. Un IT de synchronisation permet d'identifier le début de trame, il assure le cadrage de la lecture des différentes voies (figure 5.19). L'ensemble des différentes voies et de (ou des) l'IT de synchronisation forme la trame multiplexée, couramment appelée le **multiplex**.

Un tel système transporte des bits, le multiplexeur n'interprète pas les données qu'il transporte, il est dit transparent au protocole. L'arrivée des données est indépendante du fonctionnement du

multiplexeur. Les informations qui arrivent pendant la période de scrutation des autres voies incidentes sont mémorisées (figure 5.19). Les multiplexeurs nécessitent de la mémoire et introduisent un retard de transmission qui peut être important vis-à-vis du temps de transfert sur le support.

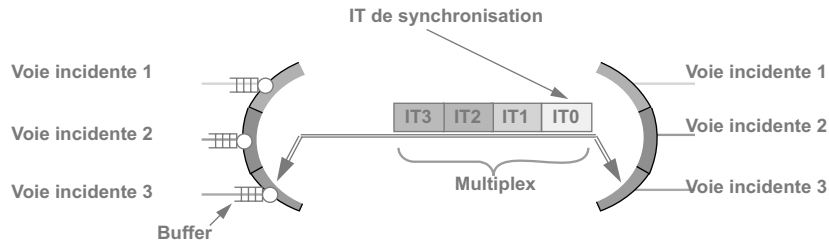


Figure 5.19 La structure élémentaire d'un multiplexeur.

Le multiplexage est dit caractère quand chaque IT est égal à un caractère. Dans un tel système, l'efficacité peut atteindre 0,8. Si on diminue encore le temps affecté, à un IT, jusqu'au niveau bit (1 IT = 1 temps bit, multiplexage bit), l'efficacité peut atteindre 0,9.

Notion de débit de cadrage

Dans un système de transmission, chaque source est indépendante. Même si on réalise à partir d'une horloge unique une distribution d'horloge, il est pratiquement impossible de garantir que les horloges de chaque système soient identiques (figure 5.20).

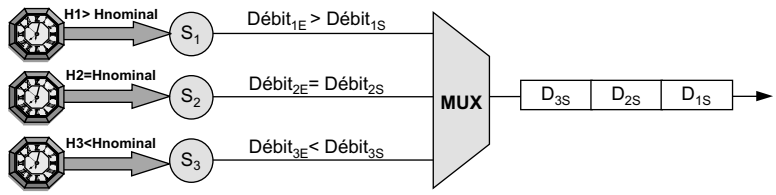


Figure 5.20 La distribution des horloges dans un réseau.

Le décalage des horloges provoque des inégalités de débit. Afin d'assurer l'égalité entre le débit incident et le débit correspondant dans le multiplex, il est nécessaire de prévoir, dans le multiplex de sortie, un surdébit pour permettre le cadrage des données (surdébit de cadrage). La figure 5.21 illustre le principe du mécanisme d'ajustement des débits par bit de cadrage.

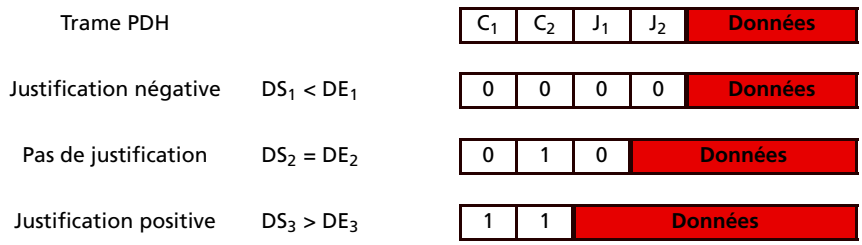


Figure 5.21 Principe de la justification dans les trames PDH.

© Dunod – La photocopie non autorisée est un délit

Dans cet exemple, l'écart maximal des horloges a été supposé limité à 1 bit. La position des données dans la trame varie donc de ± 1 bit, par rapport à une position de référence. Les bits C_1 et C_2 indiquent, lorsqu'ils sont positionnés à 1, que le bit de justification correspondant (C_1 pour J_1 et C_2 pour J_2) contient 1 bit de donnée. Lorsqu'ils ne sont pas utilisés, les bits de justification J_1 et J_2 et d'indication (C_1 et C_2) sont à 0.

Les multiplexeurs statistiques

Bien que l'efficacité des multiplexeurs temporels soit nettement supérieure à celle des multiplexeurs spatiaux, l'utilisation de la ligne n'est pas optimale. En effet, la plupart des applications n'accèdent pas en permanence au support ; de ce fait, il existe des temps morts où la ligne est inexploitée. Pour améliorer l'utilisation du support, les multiplexeurs statistiques allouent dynamiquement la bande disponible.

Les intervalles de temps sont alloués en fonction des besoins respectifs des voies incidentes. Les multiplexeurs statistiques nécessitent des *buffers* importants pour stocker les données en attente d'émission.

Le multiplexage de position et le multiplexage d'étiquette

Dans le multiplexage de position, le débit de la source et celui du multiplex sont liés, le mode de transfert est dit synchrone (**STM**, *Synchronous Transfer Mode*). La bande non utilisée est perdue. Une bonne rentabilisation du système exigerait qu'il y ait décorrélation entre la bande utilisée par une voie et celle offerte par le système, c'est le mode de transfert asynchrone (**ATM**[2], *Asynchronous Transfer Mode*) qui caractérise les réseaux en mode paquet[3].

Dans ces réseaux, les données sont émises au rythme de la source, elles ne peuvent plus être repérées par leur position. Elles sont alors identifiées par un label ou étiquette. On parle alors de **multiplexage d'étiquette**.

Le multiplexage inverse

Le multiplexage inverse (**IM**, *Inverse Multiplexing*) consiste en l'agrégation de plusieurs liens bas débit pour obtenir un débit, vu de l'utilisateur, égal à la somme des débits des liens agrégés (figure 5.22). Cette pratique permet d'améliorer la granularité de l'offre des opérateurs.

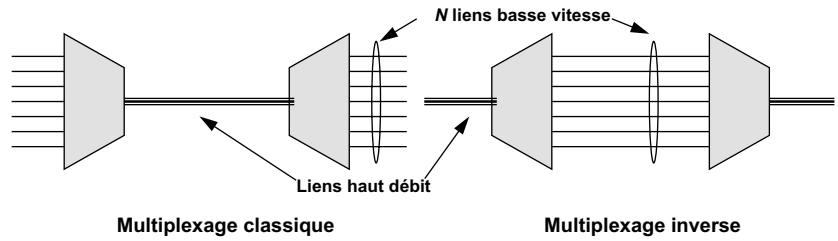


Figure 5.22 Principe du multiplexage inverse.

2. Il ne faut pas confondre le mode de transfert décrit ici avec le protocole du même nom qui n'est qu'un cas particulier du mode de transfert asynchrone (voir chapitre 14).
3. Les réseaux en mode paquet feront l'objet de l'étude du chapitre 6.

Exemple d'application : la trame MIC

➤ Principe

La numérisation de la voix autorise le multiplexage temporel de plusieurs communications téléphoniques (figure 5.23). En décalant les instants d'échantillonnage, la trame **MIC** (Modulation par impulsion et codage) regroupe 30 communications téléphoniques dans une même trame communément appelée E1, pour multiplex Européen d'ordre 1.

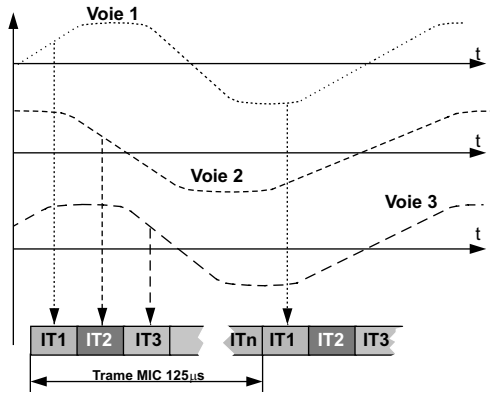


Figure 5.23 Principe de la trame MIC.

➤ Organisation de la trame

La trame MIC multiplexe 30 voies téléphoniques dans un conduit de 2 048 kbit/s, correspondant à un multiplex de 32 voies de 64 kbit/s. L'IT0 ou Mot de Verrouillage Trame (**MVT**) permet le repérage des IT dans la trame. L'IT 16 de la trame 0 contient les informations de supervision de la trame et de cadrage pour les multiplex d'ordre supérieur. L'IT16 des autres trames transporte la signalisation des communications (informations sur l'état du canal). La figure 5.24 représente la trame MIC européenne, les États-Unis et le Japon ont adopté une structure différente (voir chapitre 13, *Introduction aux réseaux de transport*).

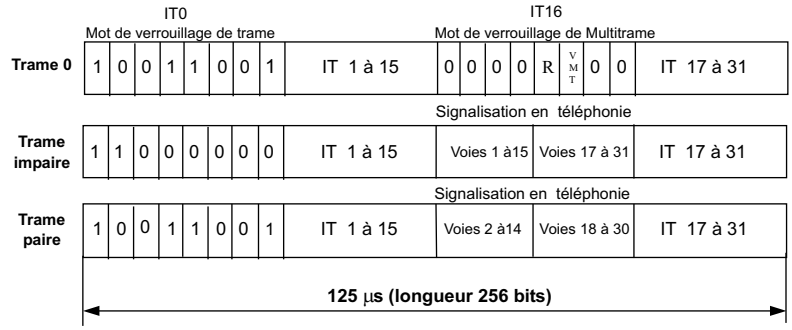
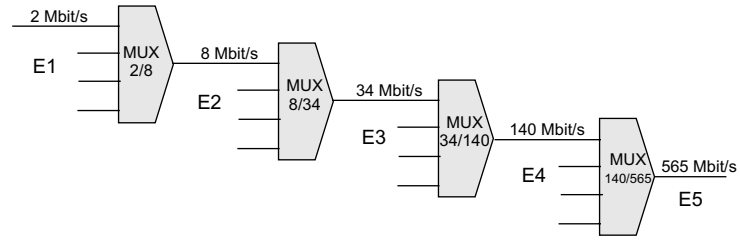


Figure 5.24 La trame MIC et les informations de signalisation.

© Dunod – La photocopie non autorisée est un délit

➤ La hiérarchie numérique

La hiérarchie numérique consiste à regrouper des multiplex pour constituer un nouveau multiplex d'ordre supérieur (figure 5.25). Le débit du multiplex de sortie est supérieur à la somme des débits incidents. En effet, le multiplexeur insère dans la trame des informations de service et des bits de justification pour compenser les écarts d'horloge des multiplex incidents (surdébit). Cette hiérarchie est désignée sous le terme de **hiérarchie numérique plésiochrone** (**PDH**, *Plesiochronous Digital Hierarchy*).



Niveau	Pays	Débit en kbit/s	Nombre de voies	Avis de l'UIT-T
Niveau 1	Europe (E1) Japon États-Unis (T1)	2 048 1 544 1 544	30 24 24	G.704
Niveau 2	Europe (E2) Japon États-Unis (T2)	8 448 6 312 6 312	120 96 96	G.742
Niveau 3	Europe (E3) Japon États-Unis (T3)	34 368 33 064 44 736	480 480 672	G.751
Niveau 4	Europe (E4)	139 264	1 920	G.751

Figure 5.25 La hiérarchie numérique PDH.

Constituant la base des réseaux numériques des années 1970, la hiérarchie plésiochrone a été remplacée à partir de 1986 par une nouvelle technique de multiplexage appelée **SDH** (*Synchronous Digital Hierarchy*). La hiérarchie synchrone autorise des débits supérieurs, elle offre plus de souplesse dans le démultiplexage, la gestion de flux, la maintenance et l'administration.

5.4.4 Comparaison multiplexeur/concentrateur

Le multiplexeur a une logique câblée indépendante du protocole, alors que le concentrateur possède une logique programmée donc fortement liée au protocole, comme, par exemple, l'analyse d'adresse du terminal destinataire.

On n'utilise qu'un seul concentrateur par liaison, alors que les multiplexeurs ne s'utilisent que par couple (multiplexage/démultiplexage). Un concentrateur établit une relation de 1 vers *n* et de *n* vers 1, un multiplexeur de 1 vers 1. La figure 5.26 fournit un exemple d'intégration de multiplexeurs et de concentrateurs dans un réseau d'entreprise.

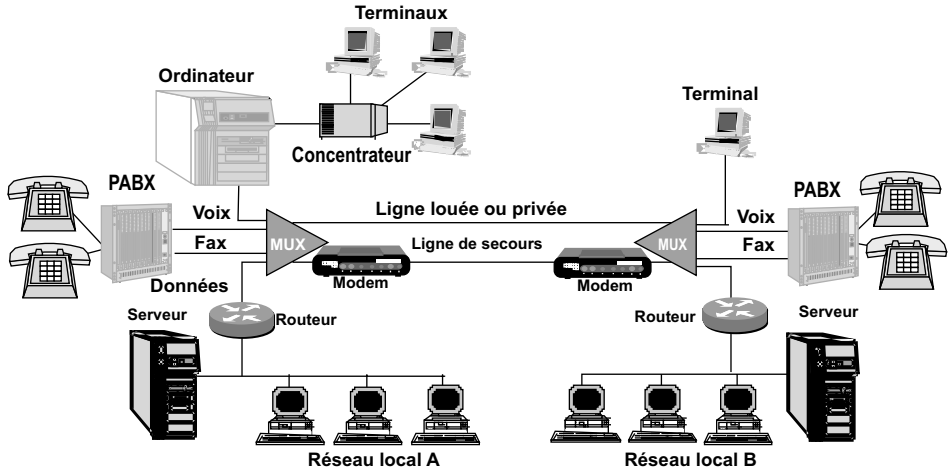


Figure 5.26 Exemple d'utilisation de concentrateurs et de multiplexeurs.

5.5 LE MULTIPLEXAGE ET L'ACCÈS À L'INTERFACE RADIO

5.5.1 Principe

L'accès partagé d'une liaison hertzienne est une application directe des techniques de multiplexage, non pour rationaliser l'utilisation d'un lien mais pour gérer une ressource rare : l'espace de fréquence. Le partage de la voie hertzienne peut être aléatoire ou organisée.

Dans les réseaux radio où chaque station doit pouvoir recevoir les messages de toutes les autres stations, une seule fréquence peut être utilisée. Le système Aloha, considéré comme l'ancêtre des systèmes de partage du support hertzien est de la première catégorie. Une station radio qui désire émettre émet, la station destinatrice acquitte immédiatement le message reçu. Si le message entre en collision avec celui d'une autre station, il n'est pas intelligible et ne sera donc pas acquitté. Il sera retransmis sur temporisation. Ce système est très simple, mais dès que le nombre de stations candidates au support augmente, l'efficacité du protocole chute. Le système peut être amélioré en distribuant à chacune des stations des intervalles de temps, cette technique est dite Aloha en tranches (*Slotted Aloha*). La durée d'une tranche correspond au temps de propagation aller retour entre les deux stations les plus distantes. Une station ne peut émettre des données qu'en début d'un slot, cette technique nécessite une synchronisation des stations par une station maître.

5.5.2 Les techniques d'accès multiple

Le partage de l'espace géographique

Lorsque le nombre d'interfaces communicantes devient important, l'accès au support devient difficile (nombre de communications à gérer, spectre de fréquence...), d'où l'idée d'organiser le partage de l'espace géographique ; cette technique est utilisée dans les réseaux cellulaires (réseaux locaux sans fils, chapitre 17, et réseaux de téléphonie sans fil, chapitre 20). L'espace est découpé en cellules, chaque cellule se voit attribuer une fréquence ou une bande de fréquences telle que celle-ci n'ait pas d'interférence avec les fréquences des cellules voisines. Généralement ces systèmes permettent la mobilité, le récepteur mobile pouvant se déplacer dans sa cellule, ou de cellule en cellule.

© Dunod – La photocopie non autorisée est un délit

Le partage de l'espace fréquentiel

Application directe du multiplexage fréquentiel, l'accès multiple par répartition de fréquence (**AMRF** ou **FDMA**, *Frequency Division Multiple Access*) divise une bande de fréquences en plusieurs sous-bandes. Chaque sous-bande allouée peut être utilisée indépendamment de l'autre. Elle peut être allouée de façon permanente (liaison satellite) ou temporaire (téléphonie mobile). À l'instar du multiplexage fréquentiel, les silences ne peuvent être récupérés par d'autres communications. La technique dite **FDD** (*Frequency Division Duplex*) autorise des communications *full duplex*, les deux systèmes communicants utilisent des fréquences différentes pour communiquer (figure 5.27).

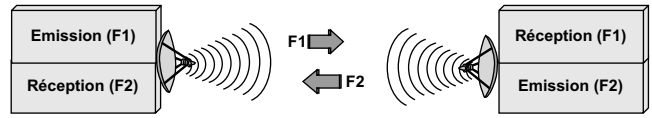


Figure 5.27 La liaison radio full duplex.

La technique d'AMRF est bien adaptée à la transmission de signaux analogiques. En particulier, elle est utilisée dans les satellites de diffusion d'émissions de télévision ou de radiodiffusion. La puissance des émissions reçues par les satellites est de l'ordre de quelques picowatts alors que celle d'émission varie de quelques watts à plusieurs centaines. Si réception et émission utilisaient la même fréquence, le récepteur serait ébloui par le signal émis. Ces systèmes utilisent donc deux fréquences (exemple, dans la bande C : 6 et 4 GHz) l'une montante (6 GHz, réception) l'autre descendante (4 GHz, émission). La figure 5.28 illustre le principe de la transposition de fréquence réalisée dans un satellite.

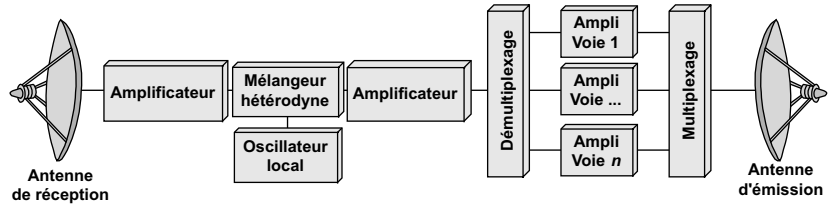


Figure 5.28 Principe de la transposition de fréquence dans un satellite.

Les signaux reçus par le satellite sont préamplifiés, une transposition de fréquence est ensuite réalisée. Les différents canaux sont alors séparés à l'aide de filtres (démultiplexage), puis amplifiés séparément (amplificateurs à faible bande et gain important) avant d'être de nouveau mélangés (multiplexage).

Le partage de l'espace temporel

L'accès multiple à répartition dans le temps (**AMRT** ou **TDMA**, *Time Division Multiple Access*) dérive du multiplexage temporel. Dans ce système, chaque station occupe l'ensemble du spectre de fréquence alloué pendant un certain temps (*Time slot*). Une station directrice synchronise l'accès au canal. Dans un système de communication entre plusieurs stations, chaque station découpe son propre intervalle de temps en sous-intervalles correspondant à une communication vers une autre

station du réseau. La synchronisation de l'ensemble des stations est l'une des difficultés de ce système. L'AMRT est utilisé par les systèmes GEO et EUTELSAT, le système Iridium et le GSM (*Global System Mobile*) combinent l'ARMF et L'AMRT (F/TDMA). La figure 5.29 représente la structure d'une trame TDMA, elle illustre le principe du partage du temps entre les différentes stations. Pour accéder à la multitrame, la station qui a des données à émettre formule une demande. Une trame lui est attribuée dans laquelle elle insère les données qu'elle a en attente.

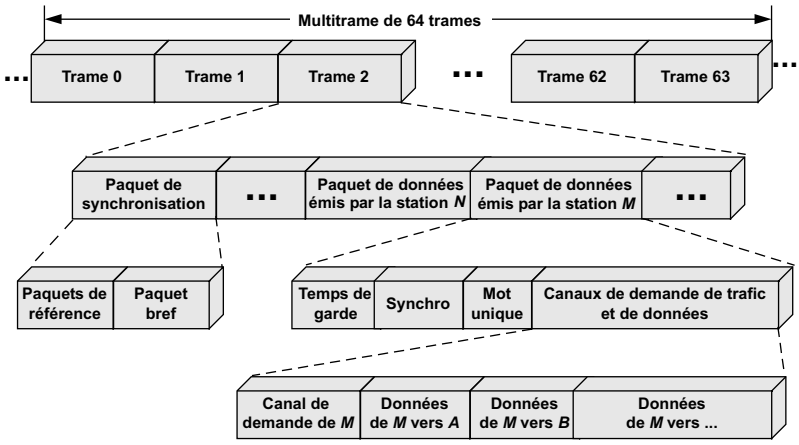


Figure 5.29 Principe d'une trame TDMA.

Les techniques d'étalement de spectre

Initialisées dans le domaine militaire pour assurer une certaine confidentialité aux communications, les techniques d'étalement de spectre (*Spread-spectrum*) autorisent le partage d'une bande de fréquence et augmentent la résistance aux interférences et signaux parasites. La figure 5.30 illustre le principe de la résistance aux perturbations des techniques d'étalement de spectre.

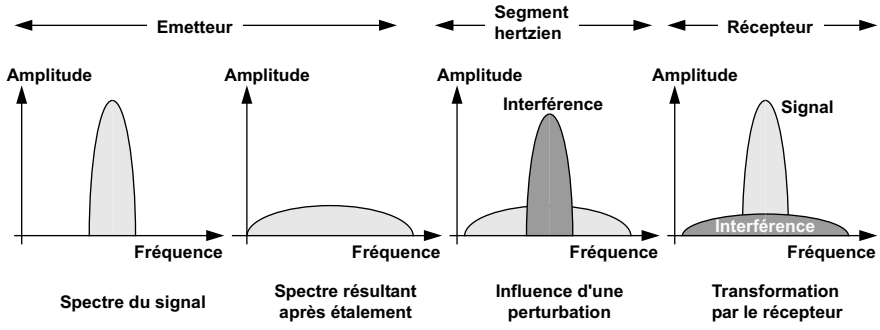


Figure 5.30 L'étalement de spectre et l'influence d'une perturbation.

Le signal d'origine occupe un spectre relativement réduit, le spectre est étalé soit par une technique dite à sauts de fréquence, soit par une technique dite à séquence directe, ces techniques sont étudiées ci-après. Lors de la restauration du signal d'origine, l'éventuelle perturbation verra au

© Dunod – La photocopie non autorisée est un délit

contraire son spectre étalé. De ce fait, l'énergie de la perturbation est très faible vis-à-vis de celle du signal d'origine, les deux peuvent donc être facilement différenciés.

➤ L'étalement de spectre à saut de fréquence

Dans cette technique (**FHSS**, *Frequency Hopping Spread Spectrum*) tout le spectre de fréquence disponible est occupé par l'ensemble des canaux. Cependant, périodiquement, selon une séquence pseudo aléatoire connue des couples émetteur-récepteur, la fréquence (canal) utilisée change. La figure 5.31 illustre ce principe.

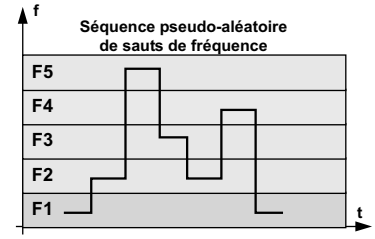


Figure 5.31 L'étalement de spectre à sauts de fréquence vue d'une station.

La bande de fréquence est subdivisée en sous-canaux, chaque canal est affecté durant un intervalle de temps prédéterminé et constant, selon une séquence pseudo aléatoire, à une station. La principale difficulté de ce système est la synchronisation des stations sur une séquence.

➤ L'étalement de spectre à séquence directe

L'étalement de spectre à séquence directe (**DSSS**, *Direct Sequence Spread Spectrum*) autorise chaque canal à utiliser l'intégralité de la bande de fréquence allouée mais chaque communication utilise un code unique (**AMRC**, Accès multiple à répartition par code ou **CDMA**, *Code Division Multiple Access*).

AMRC consiste à multiplier le signal binaire par une séquence binaire pseudo-aléatoire telle qu'à 1 bit du signal binaire correspondent *N* « bits » du signal émis. Le débit d'information est mesuré en bit/s, alors que le débit du signal émis s'exprime en chip/s (figure 5.32). En réception le signal reçu est multiplié par la même séquence, on retrouve ainsi le signal binaire d'origine. Un autre signal binaire utilisant la même porteuse mais étalé avec une séquence binaire non corrélée avec la précédente (codage dit orthogonal) sera considérée au décodage par le premier système comme du bruit de fond (voir figure 5.30).

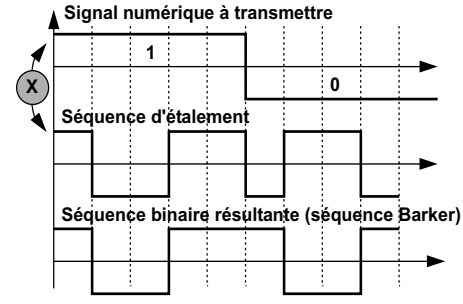


Figure 5.32 Principe de l'AMRC (CDMA).

Le DSSS autorise l'utilisation d'un même canal de fréquence par plusieurs sources (multiplexage). Cette technique n'augmente pas la capacité du canal, mais elle autorise un multiplexage efficace sans qu'il soit besoin de coordonner les différentes stations comme dans l'accès multiple à répartition dans le temps.

➤ Comparaison des différents systèmes

	FDMA	TDMA	F/TDMA	CDMA
Technique	Multiplexage fréquentiel.	Multiplexage temporel.	Chaque canal occupe une bande de fréquences pendant un certain temps (technique similaire au FHSS).	Chaque canal occupe toute la bande de fréquences, mais est codé différemment.
Avantages	Pas de synchronisation. Convient au numérique et à l'analogique.	Débit élevé.	Meilleure protection contre les écoutes.	Protection contre les écoutes. Bonne utilisation de la bande passante.
Inconvénients	Bande passante mal utilisée (bandes de garde).	Nécessite une synchronisation des horloges.	Synchronisation des sauts de fréquence.	Complexité du décodage.

Figure 5.33 Synthèse des modes de partage de l'espace hertzien.

5.6 LE CONCEPT DE RÉSEAU À COMMUTATION

5.6.1 Définitions

Les systèmes précédents n'offrent qu'une connectivité réduite, il s'agit de partager un canal de transmission, les réseaux permettent aussi un partage de la bande passante mais en offrant un service de connectivité totale. Un réseau peut être défini comme étant un ensemble de moyens matériels et logiciels géographiquement dispersés destinés à offrir un service, comme le réseau téléphonique, ou à assurer le transport de données. Les techniques à mettre en œuvre diffèrent en fonction des finalités du réseau et de la qualité de service désirée.

Le réseau illustré par la figure 5.34 est composé de nœuds. Les nœuds d'accès, situés à la périphérie du réseau, permettent le raccordement des usagers par une liaison dénommée **liaison d'abonné**. L'ensemble des moyens mis en œuvre pour raccorder un usager est souvent désigné par le terme de **boucle locale**[4]. Les nœuds sont généralement des routeurs au point d'accès et des commutateurs au cœur du réseau.

4. Une autre définition, plus restrictive, limite la boucle locale à la liaison cuivre qui relie l'abonné au PoP (*Point of Presence*).

© Dunod – La photocopie non autorisée est un délit

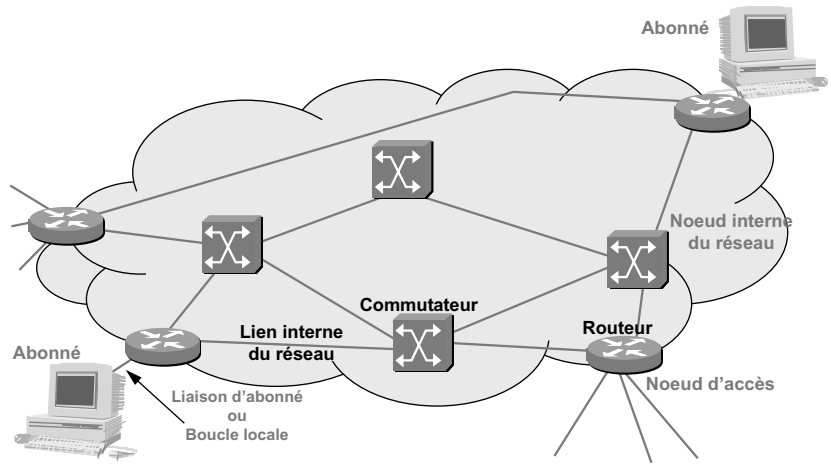


Figure 5.34 Le réseau : ensemble de ressources mises en commun.

5.6.2 La classification des réseaux

Le langage courant distingue les réseaux selon différents critères. La classification traditionnelle, fondée sur la notion d'étendue géographique, correspond à un ensemble de contraintes que le concepteur devra prendre en compte lors de la réalisation de son réseau. Généralement, on adopte la terminologie suivante :

- **LAN** (*Local Area Network*), réseau local d'étendue limitée à une circonscription géographique réduite (bâtiment...), ces réseaux destinés au partage local de ressources informatiques (matérielles ou logicielles) offrent des débits élevés de 10 Mbit/s à 10 Gbit/s.
- **MAN** (*Metropolitan Area Network*)**,** d'une étendue de l'ordre d'une centaine de kilomètres, les MAN sont généralement utilisés pour fédérer les réseaux locaux ou assurer la desserte informatique de circonscriptions géographiques importantes (réseau de campus).
- **WAN** (*Wide Area Network*)**,** ces réseaux assurent généralement le transport d'information sur de grandes distances. Lorsque ces réseaux appartiennent à des opérateurs, les services sont offerts à des abonnés contre une redevance. Les débits offerts sont très variables, de quelques kbit/s à quelques Mbit/s.

D'autres classifications, plus proches des préoccupations quotidiennes, peuvent être adoptées. Le critère organisationnel prédomine. Le réseau est accessible à tous moyennant une redevance d'usage, il est alors dit public ; s'il ne l'est qu'à une communauté d'utilisateurs appartenant à une même organisation, il est alors dit privé. Un réseau public peut être géré par une personne privée (opérateur de télécommunication de droit privé), et un réseau privé peut être sous la responsabilité d'une personne de droit public (réseau d'un ministère...). Un réseau privé est dit virtuel (**VPN**, *Virtual Private Network*) lorsque, sur une infrastructure partagée (réseau public ou privé), on développe des mécanismes tels que la communication ne soit possible qu'entre clients du VPN. Ces mécanismes peuvent être un identifiant de VPN ou un chiffrement des communications. Ne peuvent établir une communication que les clients utilisant le même identifiant ou possédant la même clé de chiffrement/déchiffrement, ils déterminent entre eux un groupe de communication assimilable à un réseau privée (figure 5.35).

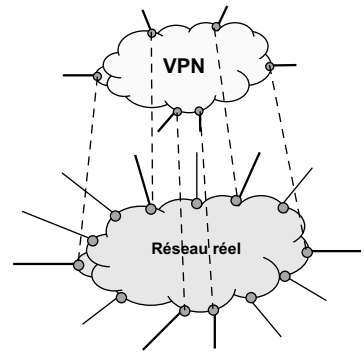


Figure 5.35 Vue logique d'un VPN.

Les réseaux se différencient, aussi, selon les modes de diffusion de l'information (figure 5.36). On distingue trois modes :

– La source diffuse ses informations vers des stations réceptrices. La relation est unidirectionnelle de 1 à *N* (réseau de diffusion). Les réseaux de radiodiffusion constituent un exemple de ce type de réseau. Les réseaux locaux sont aussi assimilés à cette catégorie.
– À l'inverse, un ensemble de stations peut envoyer les informations à un seul destinataire. La relation est aussi unidirectionnelle, mais de *N* à 1 (réseaux de collecte). Les réseaux de télémesure constituent un exemple de ce mode de fonctionnement.
– D'une manière plus générale, un abonné d'un réseau désire pouvoir atteindre tous les autres abonnés ou une partie de ceux-ci. Le réseau doit établir une relation de 1 à 1 parmi *N*. Ces réseaux de mise en relation sont dits **réseaux de commutation**, le réseau téléphonique (RTC) en est un exemple.

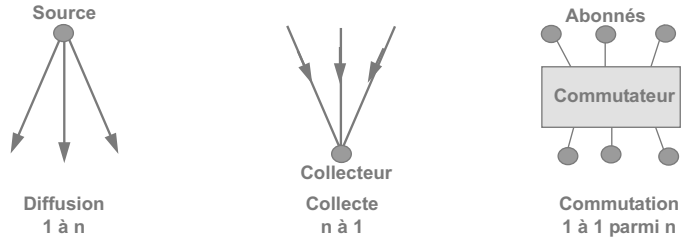


Figure 5.36 La classification selon les modes de diffusion de l'information.

Enfin, une autre distinction (approche temporelle) applicable à tous les réseaux décrit comment les différents nœuds (éléments actifs) d'un réseau sont synchronisés entre eux (figure 5.37) :

– Si chaque nœud a une horloge indépendante**,** le réseau est dit **plésiochrone**. Les horloges réception et émission sont différentes mais proches (plésio).
– Si les horloges des différents nœuds sont toutes asservies à une même horloge, le réseau est dit **synchrone**. L'horloge principale peut être une horloge atomique ou une horloge pilotée par les tops horaires d'un GPS.

© Dunod – La photocopie non autorisée est un délit

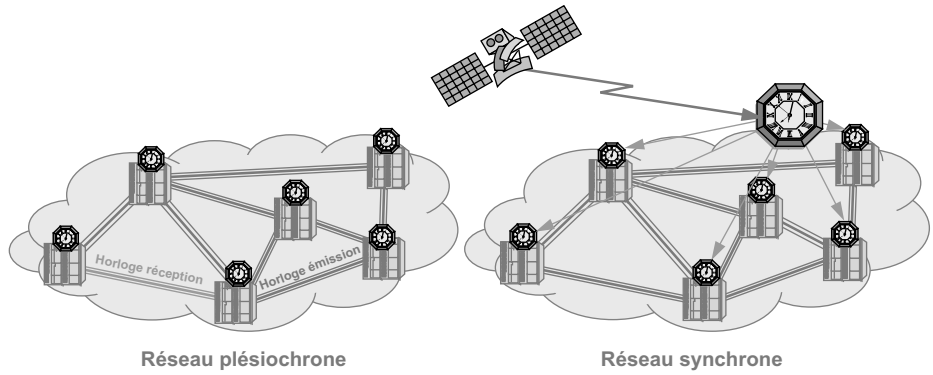


Figure 5.37 La distinction des types de réseaux selon le mode de synchronisation.

La synchronisation des réseaux et les problèmes en relation avec la distribution des horloges constituent un problème majeur de conception d'un réseau. L'étude de ces techniques sort du cadre de cet ouvrage.

5.6.3 La topologie physique des réseaux

La topologie d'un réseau décrit la manière dont les nœuds sont connectés. Cependant, on distingue la **topologie physique**, qui décrit comment les machines sont raccordées au réseau, de la **topologie logique** qui renseigne sur le mode d'échange des messages dans le réseau (**topologie d'échange**).

Les topologies de base

Les topologies de base sont toutes des variantes d'une liaison point à point ou multipoint (figure 5.38).

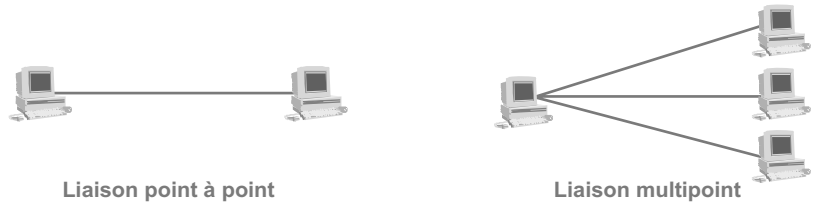


Figure 5.38 Les modes de liaisons élémentaires.

La plus simple des topologies de base, le **bus,** est une variante de la liaison multipoint. Dans ce mode de liaison, l'information émise par une station est diffusée sur tout le réseau. Le réseau en bus est aussi dit **réseau à diffusion** (figure 5.39). Dans ce type de topologie, chaque station accède directement au réseau, d'où des problèmes de conflit d'accès (contentions ou collisions) qui nécessitent de définir une politique d'accès. Celle-ci peut être centralisée ou distribuée comme dans les réseaux locaux.

Les réseaux en bus sont d'un bon rapport performance/prix. Ils autorisent des débits importants (>100 Mbit/s sur 100 m). Il est possible d'y insérer une nouvelle station sans perturber les communications en cours.

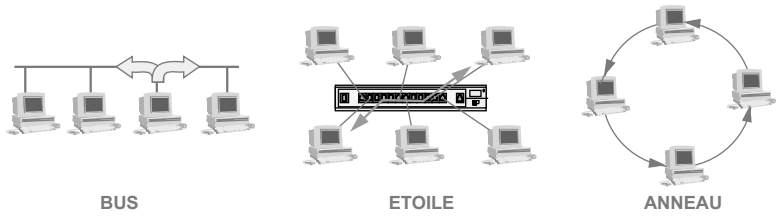


Figure 5.39 Les topologies de base.

La topologie étoile est une variante de la topologie en point à point. Un nœud central émule *n* liaisons point à point (figure 5.39). Tous les nœuds du réseau sont reliés à un nœud central commun : le concentrateur. Tous les messages transitent par ce point central. Le concentrateur est actif, il examine chaque message reçu et ne le retransmet qu'à son destinataire. Cette topologie correspond, par exemple, au réseau téléphonique privé d'une entreprise où le commutateur téléphonique met en relation les différents postes téléphoniques de l'installation. La topologie étoile autorise des dialogues internœuds très performants. La défaillance d'un poste n'entraîne pas celle du réseau, cependant le réseau est très vulnérable à celle du nœud central.

Dans la topologie en anneau, chaque poste est connecté au suivant en point à point (figure 5.39). L'information circule dans un seul sens, chaque station reçoit le message et le régénère. Si le message lui est destiné, la station le recopie au passage (au vol). Ce type de connexion autorise des débits élevés et convient aux grandes distances (régénération du signal par chaque station). L'anneau est sensible à la rupture de la boucle. On peut remédier aux conséquences d'une rupture de l'anneau en réalisant un double anneau[5].

Les topologies construites

Dérivés des réseaux en étoile, les réseaux arborescents (figure 5.40 gauche) sont constitués d'un ensemble de réseaux étoiles reliés entre eux par des concentrateurs jusqu'à un nœud unique (nœud de tête). Cette topologie est essentiellement mise en œuvre dans les réseaux locaux (Starlan, 10 base T...). Ces réseaux, en raison de la concentration réalisée à chaque nœud, sont très vulnérables à la défaillance d'un lieu ou d'un nœud (figure 5.40 centre).

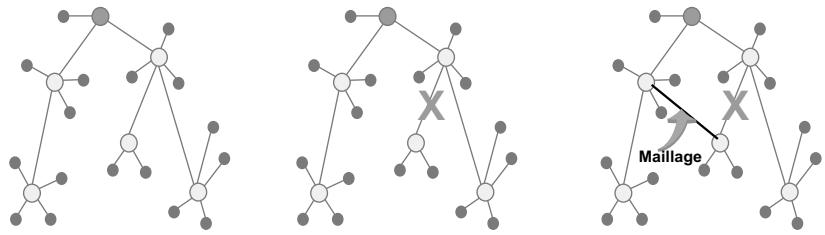


Figure 5.40 De la topologie hiérarchique à la topologie maillée.

Pour palier cet inconvénient on peut imaginer créer des chemins de secours qui peuvent être temporaires ou permanents. Le réseau est alors dit **maillé** (figure 5.40 droite). Un réseau maillé est

5. La technique du double anneau est mise en œuvre dans les réseaux métropolitains comme le FDDI (voir chapitre 16).

© Dunod – La photocopie non autorisée est un délit

un réseau dans lequel deux stations, clientes du réseau, peuvent être mises en relation par différents chemins (figure 5.41). Ce type de réseau, permettant de multiples choix de chemins vers une même destination, est très résistant à la défaillance d'un nœud et autorise une optimisation de l'emploi des ressources en répartissant la charge entre les différents nœuds (voies). Chaque nœud est caractérisé par sa **connectivité**, c'est-à-dire par le nombre de liens qui le réunit aux autres nœuds du réseau.

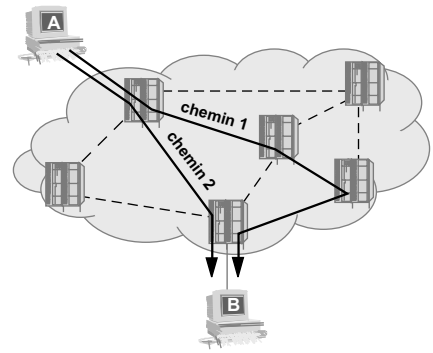


Figure 5.41 Le réseau maillé.

5.6.4 Les réseaux à commutation

Introduction à la commutation

Le concept de réseau à commutation est né de la nécessité de mettre en relation un utilisateur avec n'importe quel autre utilisateur (relation de 1 à 1 parmi n ou interconnexion totale) et de l'impossibilité de créer autant de liaisons point à point qu'il y a de paires potentielles de communicants.

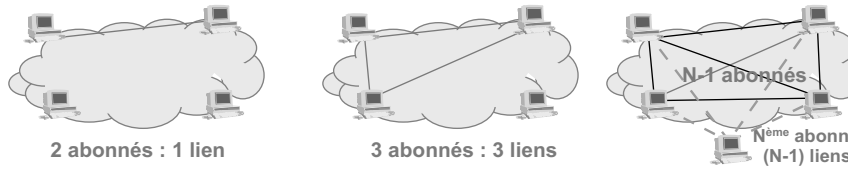


Figure 5.42 L'interconnexion totale.

Ainsi, pour réaliser l'interconnexion totale de deux stations (figure 5.42), il suffit d'une liaison, pour trois stations trois liens... D'une manière générale, dans un réseau de N stations, pour relier la station N aux $N-1$ stations déjà connectées il faut $(N-1)$ liens. Soit, pour les N stations, $N \cdot (N-1)$ liens. En comptant de cette manière, on commet l'erreur de compter deux fois chaque lien (le lien de A vers B est le même que le lien de B vers A). Le nombre total de liens nécessaires dans un système de N nœuds est donc de :

$$\text{Nombre de liens} = \frac{N(N-1)}{2}$$

Si on applique cette formule au réseau téléphonique, compte tenu qu'il existe environ $300 \cdot 10^6$ abonnés dans le monde et que chaque abonné peut être mis en relation avec n'importe quel autre abonné, la terminaison de réseau chez chaque abonné devrait comporter $45 \cdot 10^{15}$ lignes !

Ce chiffre montre, s'il en était besoin, la nécessité de trouver un système qui permette, à partir d'une simple ligne de raccordement (liaison d'abonné), d'atteindre simplement tout autre abonné du réseau par simple commutation d'un circuit vers cet abonné. Ce système porte le nom de **réseau à commutation**, dans le réseau illustré par la figure 5.43, le commutateur met en relation les utilisateurs A et B.

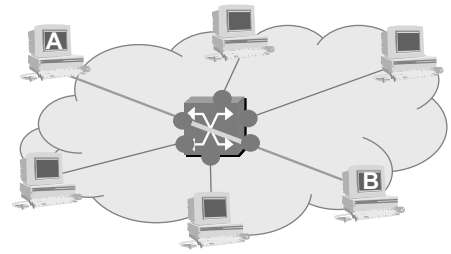


Figure 5.43 Principe d'un réseau à commutation.

Dans ce contexte où la ressource est rare vis-à-vis de la demande potentielle (si simultanément tous les abonnés du réseau désiraient joindre un autre abonné...), il est indispensable de rechercher des techniques particulières pour optimiser le partage des ressources, c'est l'objectif des techniques de commutation. Selon la technique employée pour « relier » deux utilisateurs, on distingue la commutation de circuits, de messages ou de paquets.

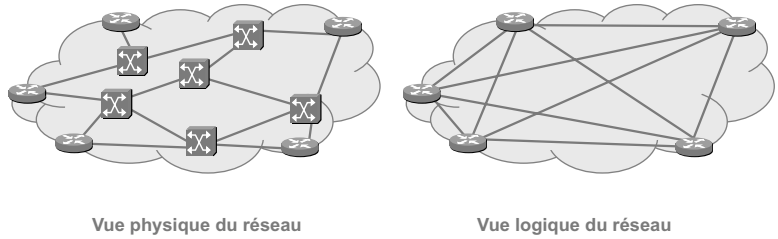


Figure 5.44 Conséquence de la commutation sur la vision du réseau.

Un réseau à commutation assure une connectivité totale. Dans ses conditions, la topologie logique ou interconnexion totale, vue du côté des utilisateurs, est différente de la topologie physique réelle (figure 5.44).

La commutation de circuits

Dans les réseaux à commutation de circuits, un lien physique, entre une source et une destination, est établi par juxtaposition de différents supports physiques afin de constituer une liaison de bout en bout (figure 5.45). La mise en relation physique est réalisée par les commutateurs avant tout échange de données et est maintenue tant que les entités communicantes ne la libèrent pas expressément. Le taux de connexion est important, alors que le taux d'activité peut être faible.

La constitution d'un chemin physique, emprunté par la suite par toutes les données transférées, garantit le respect du séquencement des informations. Elles sont reçues dans l'ordre où elles ont été émises. Cependant, les deux entités correspondantes doivent être présentes durant tout l'échange

© Dunod – La photocopie non autorisée est un délit

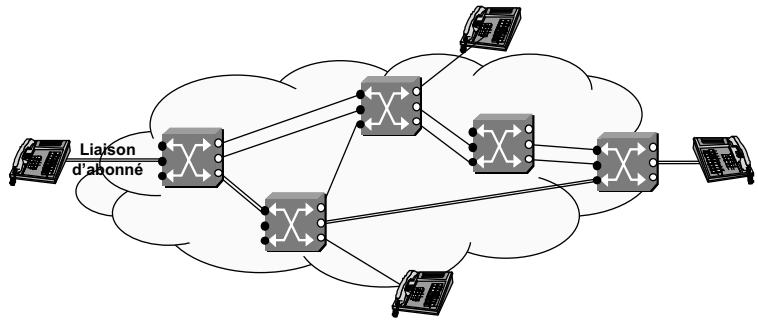


Figure 5.45 Le réseau à commutation de circuits.

de données, il n'y a pas de stockage intermédiaire. Les débits de la source et du destinataire doivent être identiques. Les abonnés monopolisent toute la ressource durant la connexion. Dans ces conditions, la facturation est généralement dépendante du temps et de la distance (exemple : le Réseau téléphonique commuté ou **RTC**).

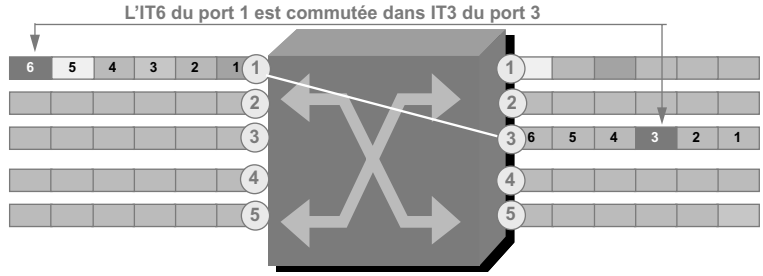


Figure 5.46 La commutation temporelle.

Archétype des réseaux, la commutation de circuits ou commutation spatiale est aujourd'hui remplacée par une commutation par intervalle de temps (IT) entre des multiplex entrants et des multiplex sortants (commutation temporelle, figure 5.46). La commutation de circuits (commutation temporelle) est mise en œuvre dans les réseaux téléphoniques, nous l'étudierons plus en détail au chapitre 20.

La commutation de messages

En commutation de circuits, la régulation de trafic est réalisée à la connexion, s'il n'y a plus de ressource disponible, de bout en bout, la connexion est refusée. Pour éviter d'avoir à surdimensionner les réseaux, la commutation de messages n'établit aucun lien physique entre les deux systèmes d'extrémité. Si le lien internœud est occupé, le message est mis en attente (figure 5.47). Chaque bloc d'information (message) constitue une unité de transfert (fichier, écran de terminal...) acheminée individuellement par le réseau. Le message est mémorisé, intégralement, par chaque nœud, et retransmis au nœud suivant dès qu'un lien se libère. Le transfert réalisé, le lien est libéré. Assurant une meilleure utilisation des lignes, la commutation de messages autorise un dimensionnement des réseaux inférieur à celui des réseaux à commutation de circuits. En cas de fort trafic, il n'y a pas

blocage du réseau mais seulement un ralentissement (attente de la libération d'un lien). La mémorisation intermédiaire de l'intégralité des messages nécessite des mémoires de masse importantes et augmente le temps de transfert. Les réseaux à commutation de messages ne sont pas adaptés aux applications interactives.

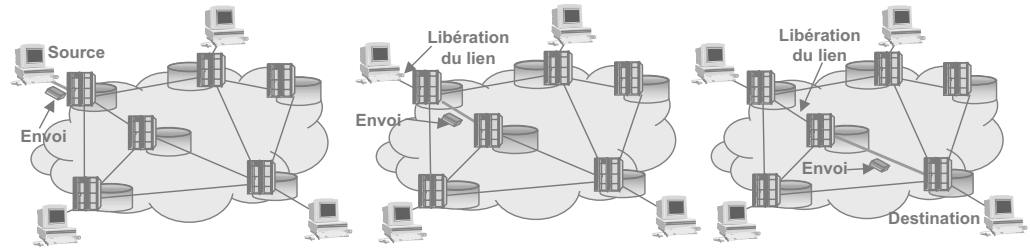


Figure 5.47 Principe de la commutation de messages.

Les réseaux à commutation de messages assurent, par rapport à la commutation de circuits :

– le transfert, même si le correspondant distant est occupé ou non connecté ;
– la diffusion d'un même message à plusieurs correspondants ;
– le changement de format des messages ;
– l'adaptation des débits et éventuellement des protocoles.

La commutation de messages ne permet qu'un échange **simplex et asynchrone**, elle est plus un service qu'une technique réseau. La commutation de messages est aujourd'hui le support logique des réseaux de télex et des systèmes de messagerie modernes.

La commutation de paquets

La commutation de messages, en monopolisant un circuit durant toute la transmission d'un message, provoque une attente non négligeable des messages d'autres sources. En découpant le message en fragments (paquets), la commutation de paquets permet l'entrelacement des unités de données (figure 5.48) offrant ainsi, à chaque source, l'impression de disposer en permanence de la voie de communication (multiplexage).

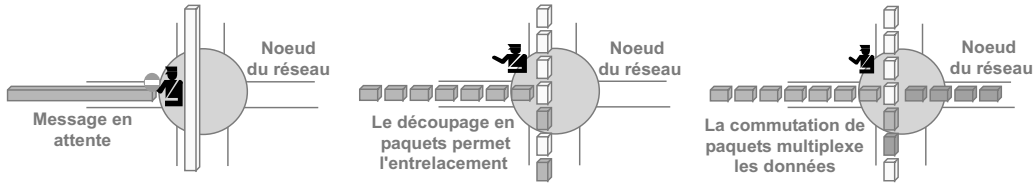


Figure 5.48 De la commutation de messages à la commutation de paquets.

Afin d'optimiser au maximum l'utilisation des liens, chaque paquet est acheminé dans le réseau indépendamment du précédent. Contrairement à la commutation de messages, il n'y a pas de stockage d'information dans les nœuds intermédiaires. Chaque nœud, recevant un paquet, le réémet immédiatement sur la voie optimale. De ce fait, le séquencement des informations n'est plus garanti. Pour reconstituer le message initial, le destinataire devra, éventuellement, réordonnancer les différents paquets avant d'effectuer le réassemblage (figure 5.49).

© Dunod – La photocopie non autorisée est un délit

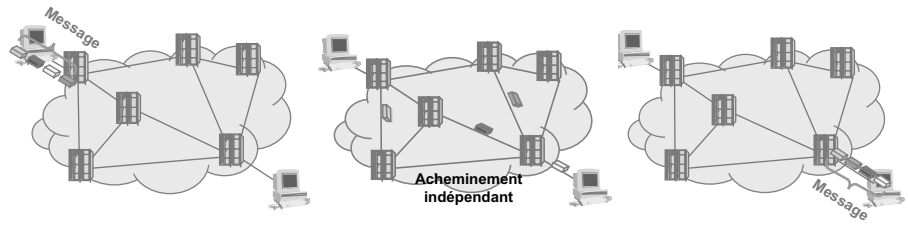


Figure 5.49 Principe de la commutation de paquets.

Ce mode de transfert optimise l'utilisation des ressources, les paquets de différentes sources sont multiplexés sur un même circuit. Cependant, chaque paquet doit contenir les informations nécessaires à son acheminement ou un label identifiant le flux (multiplexage par étiquette). La ressource offerte est banalisée et non attribuée à une communication particulière comme dans la commutation de circuits (figure 5.50).

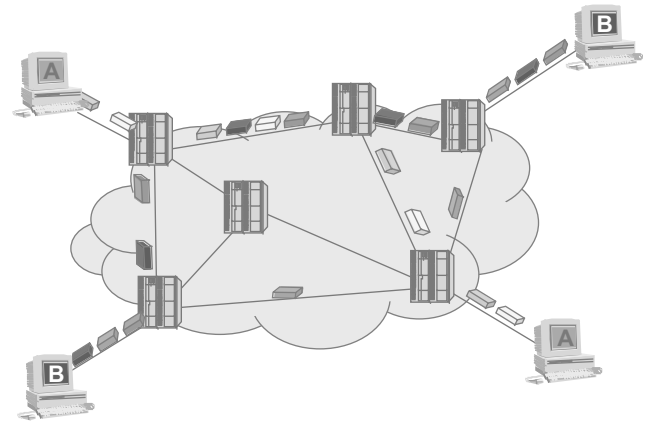


Figure 5.50 Le multiplexage des sources dans le réseau.

La commutation de paquets et le multiplexage par étiquette sont des techniques similaires. Elles se différencient essentiellement par le fait que l'une admet des unités de données de taille variable (commutation de paquets), l'autre des unités de données de taille fixe (multiplexage par étiquette). Le multiplexage par étiquette est aussi nommé **commutation de cellules**. Cette dernière technique est utilisée par le protocole **ATM** (voir chapitre 14).

5.7 CONCLUSION

Les multiplexeurs sont un moyen simple de partager un support, mais d'un usage limité. Outre leur connectivité réduite (relation de 1 à 1), ils ne sont pas adaptés aux mises en relation occasionnelles ni aux transferts sporadiques de données. Les réseaux apportent une solution à ces problèmes, ils assurent une connectivité ouverte (1 à 1 parmi n, voire m parmi n) et une mise en relation à la demande. Les services téléphoniques utilisent les techniques de la commutation de circuits, ils seront étudiés aux chapitres 20 et 21. Les réseaux de données constituent le modèle type de l'application des réseaux à commutation de paquets, l'étude de cette technique de partage statistique de la bande passante fait l'objet du chapitre suivant.

EXERCICES

Exercice 5.1 Intensité de trafic et taux d'activité

Commentez le rapport entre les valeurs de l'intensité de trafic (E) et le taux d'activité (θ), déduisez-en une solution de mutualisation des ressources, donnez un type d'application type.

Exercice 5.2 Application numérique (E et θ)

Caractérisez une liaison de données sachant que :

- le nombre de sessions à l'heure de pointe est de 1 ;
- la durée d'une session est de 10 minutes ;
- l'échange concerne des messages qui au total représentent 120 000 caractères (ASCII, 8 bits) ;
- le débit de la ligne est de 2 400 bits/s.

Déterminez :

1. l'intensité du trafic de la ligne (E) ;
2. le taux d'activité (θ) ;
3. le type d'application possible.

Exercice 5.3 Trame MIC

La trame MIC comporte 32 IT, l'IT0 sert à la synchronisation de la trame, l'IT16 au transport de la signalisation téléphonique (figure 5.51).



Figure 5.51 L'organisation de la trame MIC.

L'IT16 est scindée en deux quartets (bit a, b, c, d). Le premier quartet de la trame 1 transporte la signalisation téléphonique de la voie 1 (IT1), le second celle de la voie 17 (IT17). De même, le

premier quartet de la trame 2 transporte la signalisation téléphonique de la voie 2 (IT2), le second celle de la voie 18 (IT18)... Cette signalisation est dite par canal associé ou voie par voie (CAS).

1. Quelle est, dans ce système, la fréquence de récurrence d'une trame ?
2. Déduisez-en le débit d'une voie, si le signal de voix échantillonnée est supposé être quantifié sur 256 niveaux.
3. Quelle est la fréquence de récurrence du motif de signalisation d'une voie de communication ?
4. Déduisez-en la bande allouée à la signalisation d'une voie.

Exercice 5.4 Multiplexeur

Un multiplexeur temporel (par intervalle de temps ou IT) supporte « *N* » voies basse vitesse à 64 000 bits/s chacune (MIC de premier niveau).

1. Sachant que les informations véhiculées résultent d'une numérisation du son sur 256 niveaux de quantification, déterminez la longueur de l'IT, exprimée en bits, sur la liaison composite.
2. Sachant que l'on souhaite transmettre en simultané 30 communications, déterminez le rythme d'occurrence des trames et leur longueur (IT0 est utilisée pour la synchronisation de la trame, l'IT16 pour la signalisation des communications).
3. Quel est le débit de la liaison multiplexée correspondante ?
4. Quelle est l'efficacité de ce multiplexeur ?

Chapitre **6**

Les réseaux à commutation de paquets

6.1 GÉNÉRALITÉS

Afin d'optimiser l'utilisation des liens, la commutation de paquets découpe le message en fragments (paquets) de petite taille. Chaque paquet est acheminé dans le réseau indépendamment du précédent. Lorsqu'un nœud reçoit un paquet, en fonction de la destination du paquet, il le réémet immédiatement sur la voie la plus optimale et ceci indépendamment de la voie qu'il a attribuée aux précédents paquets de même destination. De ce fait, le séquencement des informations n'est plus garanti. Les paquets de différentes sources sont multiplexés sur un même circuit, ce mode de transfert optimise l'utilisation des ressources. Cependant, chaque paquet doit contenir les informations nécessaires à son acheminement ou un label identifiant le flux (multiplexage par étiquette). La ressource offerte est banalisée et non attribuée à une communication particulière comme dans la commutation de circuits (figure 6.1).

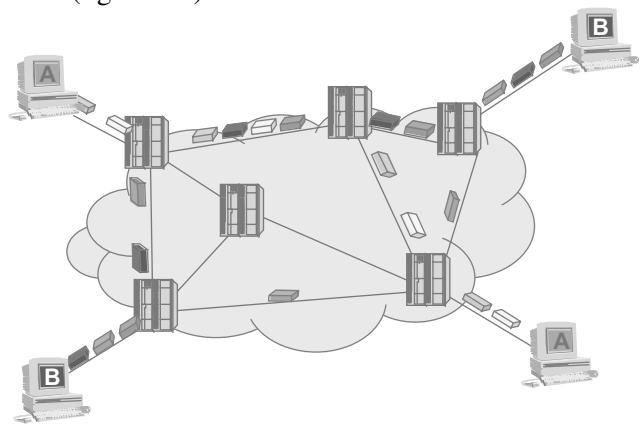


Figure 6.1 Le multiplexage des sources dans le réseau.

Pour assurer la délivrance des données au bon destinataire, celles-ci doivent contenir des informations d'acheminement (adressage), mettre en œuvre des techniques de sélection des routes (routage), assurer à chacun un transfert fluide de ses données (contrôle de flux et de congestion)... L'étude de toutes ces techniques fait l'objet du présent chapitre.

6.2 LES PERFORMANCES DE LA COMMUTATION DE PAQUETS

Supposons que dans le réseau illustré par la figure 6.2, tous les paquets d'un même message empruntent la même route. En admettant que le temps de transfert sur le support et que le temps de traitement dans les nœuds soient nuls, seul alors le temps d'émission des paquets sur le support intervient pour déterminer les performances.

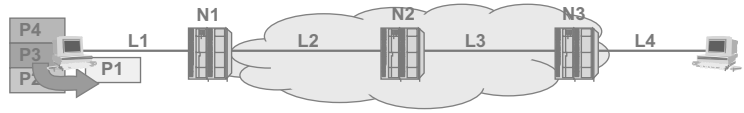


Figure 6.2 La performance d'un réseau à commutation de paquets.

Le message de longueur L (en bits) est découpé en p paquets émis sur les différents supports à un même débit de D bit/s. À l'instant t_0, le paquet 1 est émis sur le lien 1. Ce paquet est reçu par le nœud 1 à $t_0 + tp$ où tp est le temps de transmission d'un paquet. En admettant que le temps de traitement dans le nœud soit nul, le paquet est réémis immédiatement sur le nœud 2, pendant que le paquet 2 peut être émis sur le lien 1...

Si N est le nombre de nœuds, le paquet 1 arrive à destination à	$(N + 1)\ tp$
Si p est le nombre de paquets, le dernier paquet est émis quand les (p–1) paquets précédents l'ont été, soit à	$(p - 1)\ tp$
Le dernier paquet arrive à (ce qui correspond à la fin du transfert)	$(p - 1)\ tp + (N + 1)\ tp$
Soit encore	$tp\ (p + N)$
En posant	$tp = L/pD$
On obtient le temps mis pour traverser le réseau (Tp)	$Tp = (L/pD)\ (p + N)$
Ou encore	$Tp = (L/D)\ (1 + N/p)$

Cependant, cette formule ne prend pas en compte les données protocolaires (H) qu'il convient d'ajouter à chaque paquet, ce qui augmente la longueur effective du message transféré, d'où :

$$Tp = \left(\frac{L + pH}{D}\right)\left(1 + \frac{N}{p}\right)$$

La courbe de la figure 6.3 traduit graphiquement ce résultat. Les valeurs sont exprimées par rapport à la commutation de messages ($p = 1$ et $N > 0$), en formulant les hypothèses suivantes : $L = 1\ 500$ octets, $N = 5$.

➤ Discussion

– Le temps de transit dans le réseau est d'autant plus faible que le facteur N est petit. Ce qui conduit à rechercher des routes qui minimisent le nombre de nœuds traversés (algorithmes de routage) et à augmenter le maillage du réseau (augmentation de la probabilité de trouver une route plus directe).

– L'influence de la taille de l'en-tête de service est non négligeable. La figure 6.3 compare les performances en fonction de la taille des en-têtes ATM (5 octets), IPv4 (20 octets) et IPv6 (40 octets). Cette approche conduit à définir un rapport optimal entre la charge utile du bloc de données et les données de services.

– Notons qu'en cas d'erreur en commutation de messages, le message est intégralement retransmis. En commutation de paquets, seul le paquet erroné ou, si on utilise un mécanisme d'anticipation, tous les paquets depuis le paquet erroné sont retransmis.

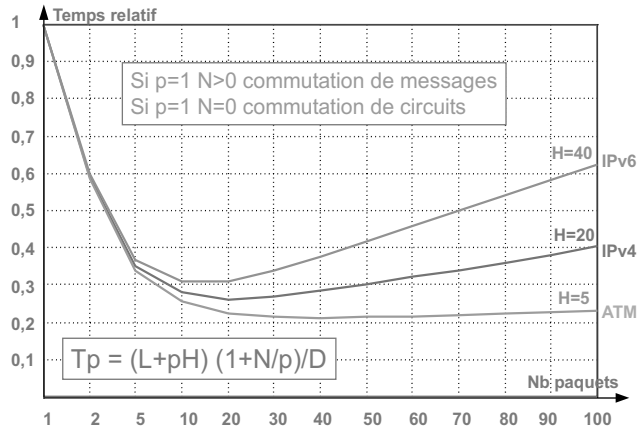


Figure 6.3 L'évolution du temps de transit en fonction du nombre de paquets.

6.3 DU MODE DATAGRAMME AU MODE CONNECTÉ

6.3.1 Principe

Rappelons qu'en commutation de paquets, à chaque paquet, le nœud recherche la route optimale. Dans ces conditions, le séquencement des paquets n'est pas garanti. La reprise sur erreur et le contrôle de flux nécessitant une stabilité de route ne sont, par conséquent, pas réalisables. Le réseau est dit *best effort* (pour le mieux), l'unité de données porte alors le nom de **datagramme**. La figure 6.4 met en évidence l'impossibilité d'une reprise sur erreur dans les réseaux en mode datagramme.

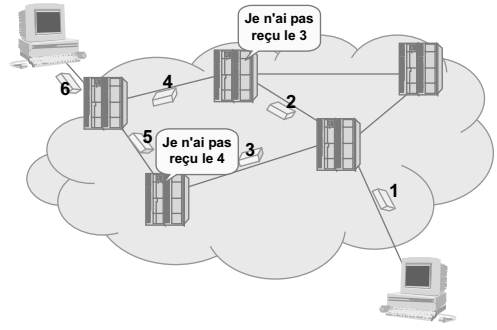


Figure 6.4 La diversité des routes n'autorise pas la reprise sur erreur.

Entre le mode datagramme qui optimise l'utilisation des ressources mais ne garantit pas l'acheminement des données et la commutation de circuits, pourrait-on imaginer (figure 6.5) une solution

© Dunod – La photocopie non autorisée est un délit

qui garantisse le séquencement des données, permette la reprise sur erreur et autorise un contrôle de flux (commutation de circuits) tout en optimisant l'utilisation du réseau (commutation de paquets) ?

	Commutation de circuits	Commutation de paquets
Établissement d'un circuit	Préalable à l'échange de données	Pas de circuit pré-établi
Garantie du séquencement	**Oui**	Non
Optimisation des ressources	Non, Circuit dédié	Oui, Circuit partagé
Indépendance des débits	Non	**Oui**

Figure 6.5 Comparaison entre la commutation de paquets et de circuits.

Le cumul des avantages de l'un et de l'autre conduit à imaginer un système qui, dans un réseau en mode paquet, garantisse le séquencement des paquets. Ainsi, la commutation de paquets décline deux modes de mise en relation (figure 6.6).

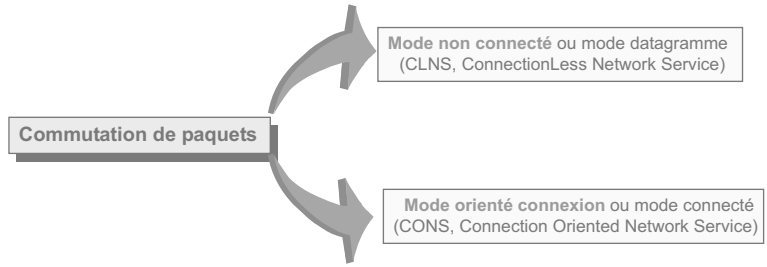


Figure 6.6 Les modes de mise en relation.

Le premier, le mode datagramme ou mode non connecté est le mode naturel de la commutation de paquets. Le second met en œuvre un mécanisme de stabilité de route qui consiste à « baliser » un chemin que suivront ensuite tous les paquets. Ce second mode de fonctionnement est dit mode orienté connexion ou plus simplement mode connecté. Le circuit émulé porte le nom de circuit virtuel (**CV**).

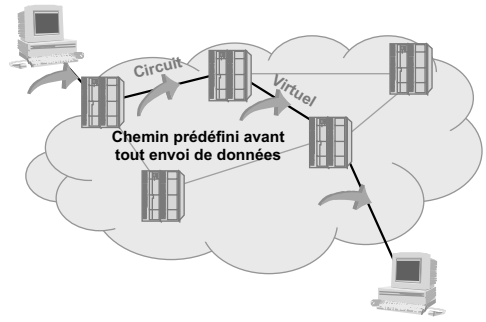


Figure 6.7 Le mode orienté connexion construit un circuit virtuel dans le réseau.

6.3.2 Les modes de mise en relation

Le mode non connecté (CLNS)

En **mode non connecté** (**CLNS**, *ConnectionLess Network Service*), les informations transitent dans le réseau indépendamment les unes des autres. Le destinataire n'est pas nécessairement à l'écoute, les informations sont, dans ce cas, perdues. Dans un tel mode de fonctionnement, les routes empruntées par les différents blocs d'information peuvent être différentes, le séquencement des informations ne peut être garanti (figure 6.8).

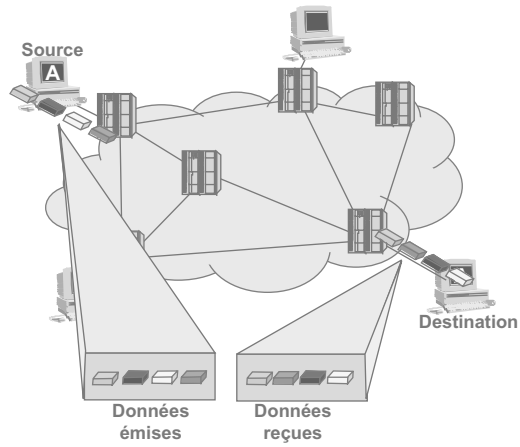


Figure 6.8 Le réseau en mode datagramme.

Les mécanismes réseaux sont allégés au détriment d'une complexité dans les organes d'extrémités qui doivent être capables de réordonnancer les différents blocs d'information.

La possibilité d'un routage différent pour chaque bloc d'information (paquet) d'un même utilisateur permet de répartir la charge du réseau (routage adaptatif). Chaque bloc est acheminé indépendamment du précédent, il doit par conséquent contenir l'adresse du destinataire. Aucune réservation de ressource n'est effectuée préalablement à tout envoi de données. De ce fait, en cas de surcharge du réseau, des blocs d'information peuvent être perdus.

Le mode orienté connexion (CONS)

En commutation de circuits, une liaison physique est préalablement établie avant tout échange de données. En **mode orienté connexion** (**CONS***, Connection Oriented Network Service*), une liaison virtuelle est construite par un mécanisme particulier (figure 6.9). Lors de la phase d'établissement de cette liaison, les différentes ressources nécessaires au transfert (*buffers*, voies...) sont réservées. Lorsque l'échange est terminé, une phase de déconnexion libère les ressources. La liaison peut être permanente (**CVP**, Circuit virtuel permanent ou **PVC***, Permanent Virtual Circuit*) ou établie appel par appel (**CVC**, Circuit virtuel commuté ou **SVC***, Switched Virtual Circuit)*.

À l'établissement du circuit virtuel, un message spécifique (paquet d'établissement) est acheminé dans le réseau. Son passage est enregistré dans chaque nœud traversé et est identifié par un numéro appelé Numéro de voie logique (**NVL**). Dans l'exemple, illustré par la figure 6.9, la source émet le paquet d'établissement. Celui-ci contient les informations utiles à son acheminement dans le réseau (adresses source et destination) et un label attribué par la source pour identifier par la suite le flux

© Dunod – La photocopie non autorisée est un délit

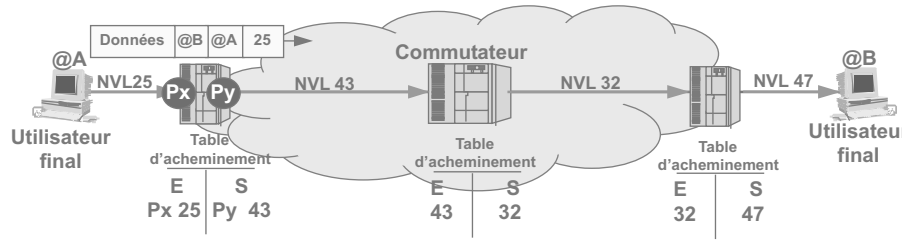


Figure 6.9 Établissement d'un circuit virtuel.

de données. Dans cet exemple le label ou Numéro de voie logique attribué est 25. Le nœud d'accès au réseau mémorise qu'il a reçu par son port *Px* un flux identifié par le NVL 25 ; en fonction de l'adresse destination et de l'état du réseau, il achemine le paquet sur son port *Py*. Compte tenu qu'il avait déjà précédemment identifié sur cette voie 42 autres communications, il substitue le label 43 (43^{e} flux) au label 25 de la source. Il mémorise ces informations dans sa table d'acheminement. Par la suite, tout paquet entrant par le port *Px* et identifié par le NVL 25 sera acheminé sur le port *Py* avec le label 43. Chaque nœud jusqu'à destination procède de même. Le circuit virtuel est établi, il résulte de la concaténation des voies logiques 25, 43, 32 et 47.

Durant la phase d'établissement du circuit, les différentes ressources nécessaires au transfert de données sont réservées (buffers, voies...). Ensuite, tous les messages empruntent la route préétablie, le séquencement des informations est garanti (chemin identique). À la fin de l'échange, une phase de déconnexion libère les ressources.

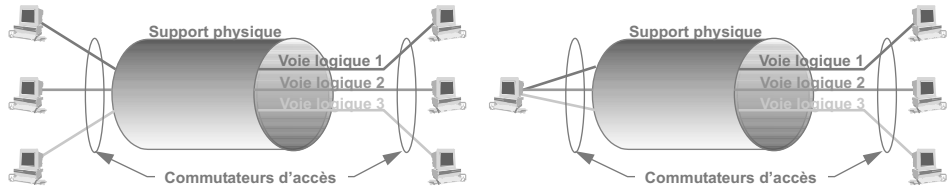


Figure 6.10 Le multiplexage de voies logiques sur une voie physique.

Le système du circuit virtuel (figure 6.10) autorise d'une part, le partage d'un même lien physique par plusieurs entités communicantes indépendantes et, d'autre part, la communication d'un même système avec plusieurs autres systèmes, chaque communication étant identifiée localement par son numéro de voie.

Circuit virtuel commuté ou permanent ?

Un circuit virtuel commuté est une liaison établie à la demande, il autorise l'établissement d'une relation avec n'importe quel autre abonné du réseau, la connectivité est ouverte. Un circuit virtuel permanent est établi (configuré) une fois pour toutes, la connectivité est réduite.

En principe, tous les protocoles réseaux en mode connecté offrent les deux possibilités. Cependant, dans les réseaux haut débit, compte tenu de la puissance de calcul nécessaire à l'établissement d'un circuit virtuel commuté, les opérateurs n'offrent, actuellement, que le service en CVP (Circuit

virtuel permanent ou PVC, *Permanent Virtual Circuit*). La définition d'un tel mode de raccordement à un réseau est toujours précédée d'une analyse des besoins de connectivité de l'entreprise.

Cette connectivité est décrite dans une table dite matrice de communication. La matrice de communication indique, pour chaque liaison, le volume du flux de données estimé afin de définir les caractéristiques de chaque abonnement. Dans l'exemple de la figure 6.11, seul le besoin de communication a été indiqué. Dans le réseau résultant, si A veut communiquer avec E, ses messages devront transiter par C et D, cette solution est souvent adoptée quand les flux de ce type (A vers E) sont faibles.

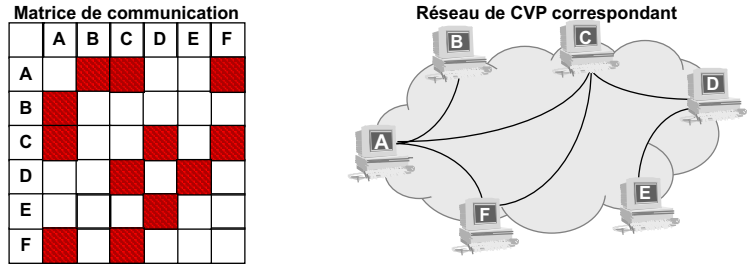


Figure 6.11 Matrice de communication et réseau logique correspondant.

Définir un ensemble de relations à base de circuits virtuels permanents, en interdisant à chaque correspondant de se mettre en relation avec tout autre abonné du réseau, définit, dans un réseau, un espace d'échange réservé et protégé, c'est une première approche des réseaux privés virtuels (**VPN**, *Virtual Private Network*).

Réseau en mode connecté ou en mode datagramme ?

Un service en mode connecté ou non connecté ne dépend pas du service support utilisé, mais des protocoles mis en œuvre sur ce support. Y a-t-il une procédure d'établissement de route ? Le mode de relation est dit alors mode connecté. Les données sont-elles envoyées sans établissement préalable de route ? Le réseau est alors dit en mode datagramme.

Définir, pour un réseau, le type de protocole à utiliser, résulte d'un choix essentiellement fondé sur les performances et la qualité de service que l'on désire obtenir. La figure 6.12 compare, succinctement, les deux modes de mise en relation.

6.4 LA NOTION D'ADRESSAGE

6.4.1 Définition

Une adresse est une suite de caractères désignant sans ambiguïté un point physique de raccordement à un réseau ou identifiant un processus, une machine.

On désigne par technique d'adressage l'ensemble des moyens utilisés pour identifier les correspondants. Pour assurer la communication, le système d'extrémité source doit fournir au réseau l'adresse du système d'extrémité destinataire (adresse destinataire), et celui-ci doit pouvoir identifier son correspondant (adresse source).

© Dunod – La photocopie non autorisée est un délit

Critères	Mode orienté connexion	Mode non connecté
Mise en relation nécessaire	Obligatoire.	Non.
Délai de connexion Délai de déconnexion	Oui, pouvant être important.	Non, puisque pas de connexion.
Type de circuit offert	Permanent durant tout l'échange.	Pas de circuit réservé, mode datagramme.
Allocation de ressources	Oui, statique (à la connexion).	Non.
Contrôle de flux possible	Oui.	Non.
Séquencement des informations	Oui (garanti par le réseau).	Non (à charge du destinataire).
Reprise sur incident	Oui.	Non.
Complexité	Couche réseau.	Couche transport.
Optimisation des réseaux	Non, circuits et ressources réservés durant toute la relation.	Oui, pas de ressource réservée, optimisation lors du routage.
Résistance à la défaillance	Non, en cas de défaillance, il faut reconstituer un circuit virtuel.	Oui, pas de chemin préétabli, en cas de défaillance d'un lien ou d'un nœud reroutage sur une autre voie.
Adressage	Simplifié, label attribué à la connexion.	Complet, chaque bloc de données (paquet) contient l'adresse complète source et destination.

Figure 6.12 Comparaison entre le mode non connecté et orienté connexion.

6.4.2 L'adressage physique

Généralités

Pour localiser sans ambiguïté un utilisateur final, il faut pouvoir identifier (figure 6.13) :

– le réseau auquel il est connecté ;
– le point par lequel il est raccordé au réseau, ce point identifie aussi l'installation locale de l'abonné ;
– le système cible dans l'installation locale.

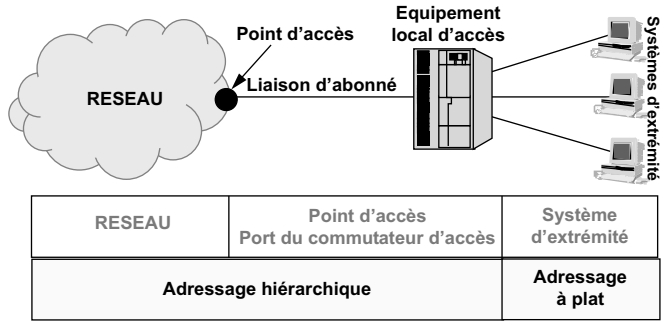


Figure 6.13 Les composantes d'une adresse.

L'ensemble de ces informations constitue l'adresse réseau. Les deux premiers champs de la figure 6.13 permettent de localiser l'installation de l'abonné, ils constituent l'adresse réseau proprement dite du destinataire, la structure en est généralement de type hiérarchique. Le troisième champ identifie le destinataire dans l'installation finale, c'est un simple identifiant sans signification particulière, cet adressage local est dit **à plat**.

L'adressage à plat ou global

Dans ce type d'adressage, l'adresse correspond à un numéro unique attribué sans aucune règle de structuration. Cet adressage est, par exemple, celui utilisé dans les réseaux locaux. À chaque entité raccordée est attribué un numéro différent et sans relation avec n'importe quel autre numéro (adresse) du réseau. D'origine Xerox, cet adressage destiné à distinguer les différents nœuds d'un même segment de réseau est normalisé par l'IEEE[1] (figure 6.14). Identifiant, dans les réseaux locaux, la machine raccordée au support, cet adressage est souvent désigné sous le terme d'adressage **MAC** (*Medium Access Control*).

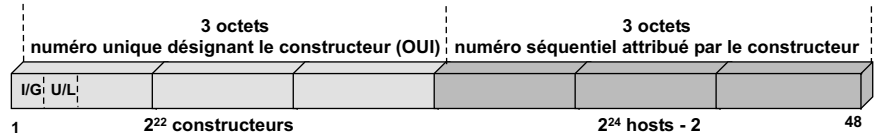


Figure 6.14 L'adressage MAC ou IEEE (réseaux locaux).

L'adressage MAC comporte deux champs. Le premier, champ attribué par l'IEEE, désigne le constructeur (**OUI**, *Organizationaly Unit Identifier*) de l'interface réseau (**NIC,** *Network Interface Card*). La liste des OUI attribués peut être obtenue dans la RFC 1340. Le second champ correspond à un numéro séquentiel attribué par le constructeur qui doit en garantir l'unicité.

L'adresse MAC peut identifier un point de raccordement unique (cas général), elle est alors dite *unicast*. Elle peut aussi désigner un groupe de machines raccordées à un segment du réseau, elle est alors, dite *multicast*. Une adresse MAC spécifique désigne toutes les machines du même réseau physique, cette adresse est dite adresse de diffusion généralisée ou *broadcast* (figure 6.15).

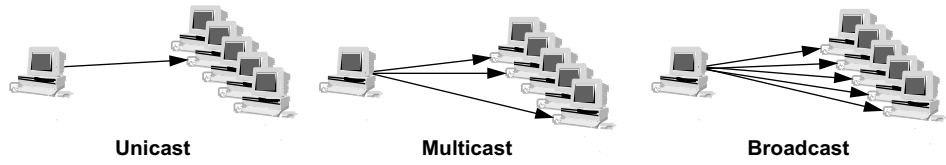


Figure 6.15 L'adressage et les points adressés.

1. Notons que l'IEEE a récemment introduit la notion d'identifiant d'interface sur 64 bits (24+40), cet identifiant d'interface est désigné sous le terme EUI-64 (*End-User Identifier*).

© Dunod – La photocopie non autorisée est un délit

L'adressage hiérarchique

Utilisée dans les grands réseaux d'interconnexion, l'adresse hiérarchique identifie un point d'accès au réseau. Son contenu est significatif, il désigne le réseau et les nœuds de ce réseau participant à l'acheminement des informations. Chaque nœud ne traite que la partie d'adresse correspondant à son niveau. Cette technique permet de réduire la portée du champ adresse des blocs de données au fur et à mesure de la progression des paquets dans le réseau.

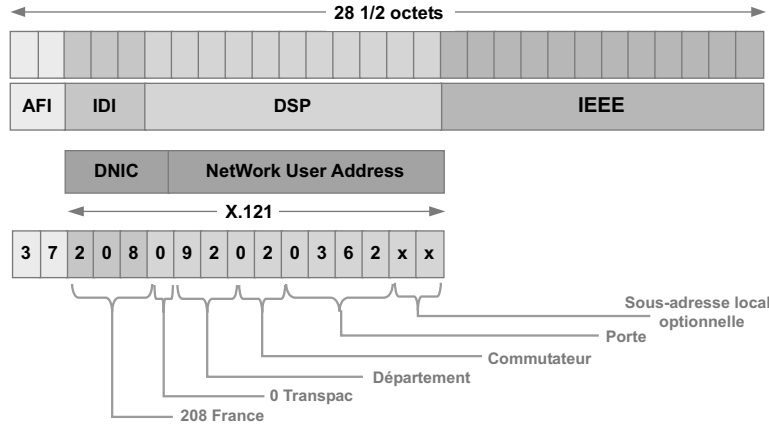


Figure 6.16 L'adressage X.121.

L'adressage défini par l'ISO dit adressage **NSAP**[2] (*Network Service Access Point*) représenté figure 6.16 comporte plusieurs champs :

- L'**AFI** (*Autority Format Identifier*) désigne l'autorité gestionnaire du domaine d'adressage et le format de représentation de l'adresse. La valeur 37 indique que l'adresse qui suit est au format X.121 et est codée en DCB[3].
- L'**IDI** (*Initial Domain Identification*) identifie le domaine d'adressage. Par exemple, dans la norme X.121 (AFI = 37), le numéro 208 est affecté à la France, le 2 représentant l'Europe.
- **DSP** (*Domain Specific Part*) correspond à l'adresse effective de l'abonné.
- Cette adresse peut éventuellement être complétée par l'adresse du terminal dans l'installation d'abonné, ici nous avons joint à cette adresse l'adresse IEEE du terminal.

La représentation X.121 (figure 6.16) divise l'adresse en deux champs :

- Le **DNIC**, *Data Network Identification Code* ou numéro de réseau, identifie le pays (France 208) et le réseau dans le pays par exemple : Transpac 0. La figure 6.17 fournit, en exemple, quelques numéros de réseau (DNIC) des principaux réseaux publics mondiaux.

2. En fait, il conviendrait de distinguer l'adresse NSAP qui indique où le service réseau est disponible, de l'adresse SNAP (*SubNetwork Point of Attachement*) qui identifie le point d'accès au réseau physique et constitue la véritable adresse réseau.

3. DCB, Décimal Codé Binaire, dans cette forme de représentation des données, chaque quartet d'un octet code un chiffre décimal, ce qui permet un codage et décodage facile.

– Le **NUA**, *Network User Address*, correspond au numéro de l'abonné dans le réseau. La figure 6.16 représente le format d'adressage utilisé pour les accès X.25 du réseau Transpac (France Telecom).

Code Pays	Pays	DNIC	Réseau
208 à 212	France	2080 2081 2082 2083	Transpac. NTI. Libre. Administrations.
234 à 238	Grande-Bretagne	2341 2342	IPSS. PSS.
240	Suède	2405	Telepak.
242	Norvège	2422	Norpak.
262	Allemagne	2624	Datex-P.
272	Irlande	2721	PTT.
302 à 307	Canada	3020 3025 3029	Datapac. Teleglobe. Infoswitch.
310 à 329	États-Unis	3106 3110	Tymnet. Telenet.

Figure 6.17 L'identification des principaux réseaux dans X.121.

Les techniques d'adressage

Selon les besoins d'identification, on dénombre les cas suivants (figure 6.18) :

– Absence de champ d'adresse, seules deux entités peuvent communiquer, c'est le cas d'une liaison en mode point à point où l'adresse est inutile.

– Adresse destinataire seule, l'émetteur n'a pas à être connu ou l'est déjà par un autre procédé ; ce mode d'adressage est utilisé dans les relations du type maître/esclave où le maître est toujours identifié. Seule l'adresse du terminal apparaît dans les échanges, elle désigne celui à qui le maître s'adresse (adresse destination) ou celui qui répond (adresse source).

– Adresse source uniquement, le récepteur n'est pas identifié, toutes les stations à l'écoute reçoivent les informations (messages de diffusion, *broadcast*).

– Adresse source/destination, cas le plus fréquent, l'adressage est alors dit distribué ou encore global distribué.

– L'adresse est absente du bloc de données, mais on lui a substitué un label. L'adressage est alors dit en cascade ou adressage de convention. La convention est établie pendant une phase d'initialisation, c'est le cas par exemple de l'attribution du numéro de voie logique dans le mode connecté.

© Dunod – La photocopie non autorisée est un délit

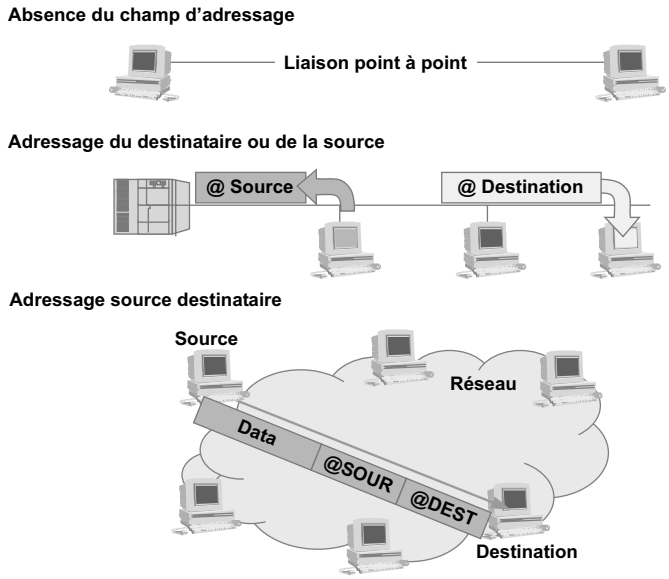


Figure 6.18 Type de relation et adressage.

6.5 LA NOTION DE NOMMAGE

6.5.1 Le nommage

La notion de nommage est complémentaire de celle d'adressage, l'un désigne l'objet, l'autre précise sa localisation. Indépendamment qu'il est plus aisé de manipuler des noms que des adresses, l'avantage du nommage est essentiellement de dissocier l'objet de sa localisation géographique. Le déplacement de l'objet nommé est transparent à l'utilisateur. De manière similaire à l'adressage, le nommage utilise deux modes de représentation :

- Le **nommage à plat ou horizontal**, ce type de nommage impose une démarche rigoureuse pour garantir l'unicité d'un nom sur l'ensemble du réseau. NetBios, protocole allégé mis en œuvre dans les réseaux locaux, utilise un nommage à plat.
- Le **nommage hiérarchique ou arborescent**, plus souple, organise le nommage en domaines. Cette technique autorise une représentation des objets calquée sur l'organisation de l'entreprise. Chaque nœud peut être un domaine dont la gestion peut être confiée à une autorité particulière. Ce mode de représentation et d'administration convient parfaitement à la gestion d'un annuaire très important comme celui d'Internet (figure 6.19).

6.5.2 La notion d'annuaire

La localisation d'un objet nommé nécessite de mettre en relation son nom et son adresse : résolution de nom. L'association nom/adresse est résolue selon deux techniques (figure 6.20) :

- la consultation d'un fichier local, le nommage est alors dit local ;
- la consultation d'une base de données centralisée ou répartie sur un système local ou des systèmes distants, le nommage est, alors, dit **décentralisé**.

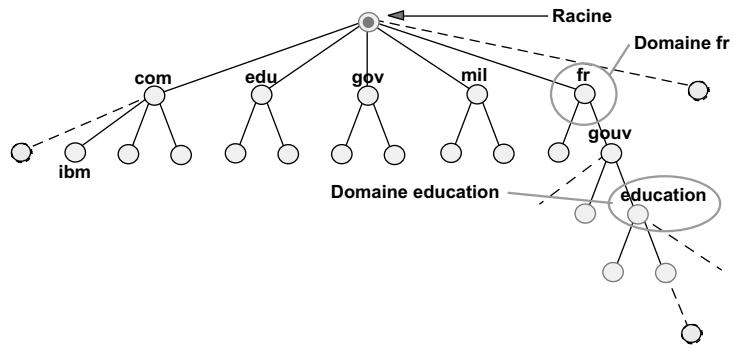


Figure 6.19 L'arbre de nommage d'Internet.

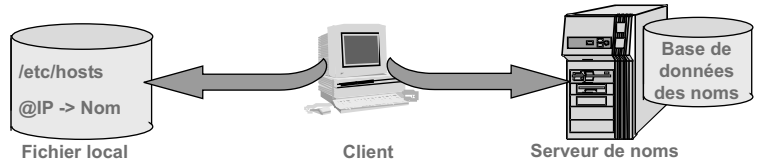


Figure 6.20 Principe de la résolution de nom.

6.6 L'ACHEMINEMENT DANS LE RÉSEAU

6.6.1 Définitions

Acheminer les informations, dans un réseau, consiste à assurer le transit des blocs d'un point d'entrée à un point de sortie désigné par son adresse. Chaque nœud du réseau comporte des tables, dites **tables d'acheminement** couramment appelées **tables de routage**, qui indiquent la route à suivre pour atteindre le destinataire (figure 6.21). En principe, une table de routage est un triplet <Adresse destination>/<Route à prendre>/<Coût>.

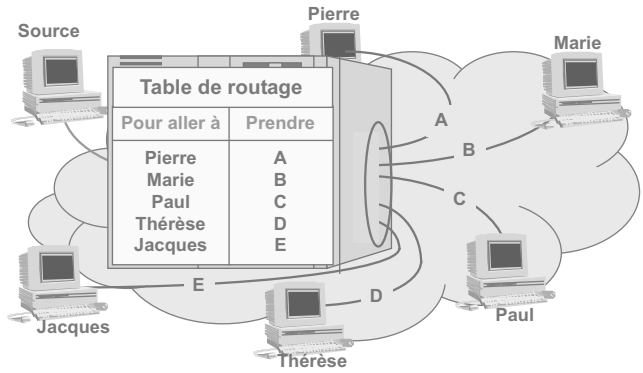


Figure 6.21 Principe d'une table de routage.

Il convient de distinguer la politique d'acheminement qui indique comment est choisie une route, du protocole de routage ou simplement routage qui décrit comment sont construites les tables

© Dunod – La photocopie non autorisée est un délit

d'acheminement, c'est-à-dire qu'il spécifie les échanges d'information entre nœuds, le mode de calcul de la route et du coût. Ces deux notions sont souvent confondues.

La politique d'acheminement peut être :

– **Déterministe,** lorsqu'un message arrive dans un nœud, il n'a pas le choix de la route. Une seule route est possible par rapport à la destination. Les tables de routage peuvent être fixées à la configuration du réseau et mises à jour périodiquement par le(s) centre(s) de gestion (gestion centralisée ou décentralisée).
– **Adaptative**, aucun chemin n'est prédéterminé, le chemin sera fixé au moment du routage en fonction de données sur l'état du réseau (charge, indisponibilité d'un nœud...). La gestion est alors généralement isolée. Le nœud assure la mise à jour de ses tables en fonction de sa connaissance de l'état du réseau.
– **Mixte**, le choix d'un chemin, adapté à l'état du réseau, est effectué au moment de l'établissement du lien entre les deux entités communicantes. Une fois ce chemin établi, tous les messages d'une même session empruntent le même chemin. La politique est adaptative à l'établissement et déterministe durant le reste de la session. Cette technique est utilisée dans les réseaux en mode orienté connexion. Le circuit virtuel est construit en politique adaptative et les données sont échangées en politique déterministe.

6.6.2 Les protocoles de routage

Les différents modes de routage

➤ Routage statique ou routage fixe

Le routage statique consiste à construire, dans chaque nœud, une table indiquant, pour chaque destination, l'adresse du nœud suivant. Cette table est construite par l'administrateur du réseau lors de configuration du réseau et à chaque changement de topologie. Simple, le routage fixe assure, même lorsque le protocole réseau est en mode datagramme, le maintien en séquence des informations. Aucun bouclage de chemin n'est à craindre, mais il n'existe pas de solution de secours en cas de rupture d'un lien.

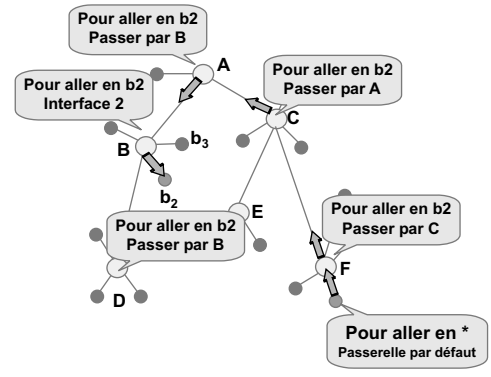


Figure 6.22 Le routage statique.

Le routage statique n'est pas optimal, il convient parfaitement aux petits réseaux et aux réseaux dans lesquels il n'existe pas de redondance dans les routes. La figure 6.22 illustre le contenu des tables de chacun des nœuds pour joindre b_2.

➤ Routage par diffusion (de 1 vers *n*)

L'information est routée simultanément vers plusieurs destinataires ou groupe d'utilisateurs. Le message doit être dupliqué en autant d'exemplaires que de destinataires. Cette technique oblige l'émetteur à connaître tous les destinataires, elle surcharge le réseau. En conséquence, on utilise, généralement, un adressage de groupe, (*multicast*) chaque nœud n'effectue, alors, que les duplications nécessaires aux sous-groupes ou destinataires finals qu'il dessert (figure 6.23).

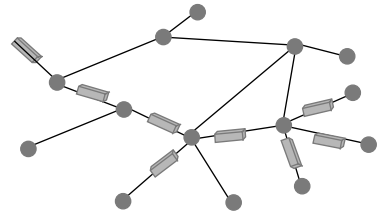


Figure 6.23 Principe du routage multicast.

➤ Routage par inondation (de 1 vers tous)

Dans le routage par inondation, chaque nœud envoie le message sur toutes ses lignes de sortie, sauf celle d'où provient le message (figure 6.24). Pour éviter une surcharge du réseau, chaque message comporte un compteur de sauts. Le compteur est initialisé à l'émission (nombre de sauts autorisés) et décrémenté par chaque nœud. Le message est détruit quand le compteur de sauts est à zéro. Pour éviter les bouclages, les messages sont numérotés, chaque nœud mémorise cet identifiant et détruit les messages déjà vus.

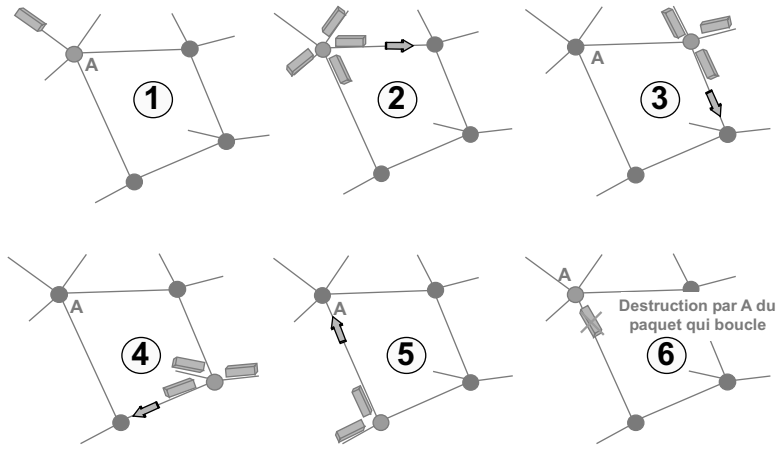


Figure 6.24 Le routage par inondation et la destruction des paquets qui bouclent.

© Dunod – La photocopie non autorisée est un délit

Ce système est très robuste, il résiste à la destruction de plusieurs lignes et garantit de trouver toujours le plus court chemin ; il est utilisé par certaines communications militaires et par quelques protocoles de routage pour diffuser les informations d'état du réseau.

➤ Routage par le chemin le plus court ou au moindre coût

Dans ce mode de routage, chaque nœud tient à jour des tables indiquant quel est le plus court chemin pour atteindre le nœud destination. Chaque lien a un coût affecté ou calculé. À partir de ces informations de coût, chaque routeur détermine le chemin optimal pour joindre une destination. Ce coût ou métrique peut être exprimé en :

– nombre de sauts ;
– en km, distance réelle ;
– en temps de latence dans les files d'attente ;
– en délai de transmission ;
– fiabilité...

Les algorithmes de routage au moindre coût diffèrent selon la manière dont ils prennent en compte ces coûts pour construire les tables de routage. Dans certains protocoles de routage, un nœud peut maintenir plusieurs tables de routage et ainsi acheminer les données en fonction d'une qualité de service requise.

Le routage au moindre coût

➤ Principe des algorithmes vecteur distance

Dans le routage vecteur distance ou routage de Bellman-Ford *(distance vector routing*), chaque nœud du réseau maintient une table de routage qui comporte une entrée par nœud du réseau et le coût pour joindre ce nœud. Périodiquement chaque nœud diffuse sa table de routage à ses voisins. Le nœud destinataire apprend ainsi ce que son voisin est capable de joindre.

À réception, le nœud compare les informations reçues à sa propre base de connaissance :

– Si la table reçue contient une entrée inconnue, il incrémente le coût de cette entrée du coût affecté au lien par lequel il vient de recevoir cette table et met cette nouvelle entrée dans sa table. Il a ainsi appris une nouvelle destination.
– Si la table contient une entrée qu'il connaît déjà et si le coût calculé (coût reçu incrémenté du coût du lien) est supérieur à l'information qu'il possède, il ignore cette information, sinon il met sa table à jour de la nouvelle valeur de cette entrée.

De proche en proche chaque nœud apprend la configuration du réseau et le coût des différents chemins. La convergence des différentes tables peut être assez longue. L'ensemble des schémas de la figure 6.25 illustre ce propos.

À l'initialisation, les routeurs n'ont connaissance que de leur propre existence. La table de routage de chacun ne comporte qu'une entrée, elle indique que le coût pour se joindre est nul (destination locale !). Dans cet exemple, le coût a été fixé à 1 pour tous les liens, le coût retenu par un nœud correspond donc au nombre de sauts. Périodiquement le contenu des tables est échangé, chaque nœud adresse à son voisin les informations Destination/Coût qu'il connaît.

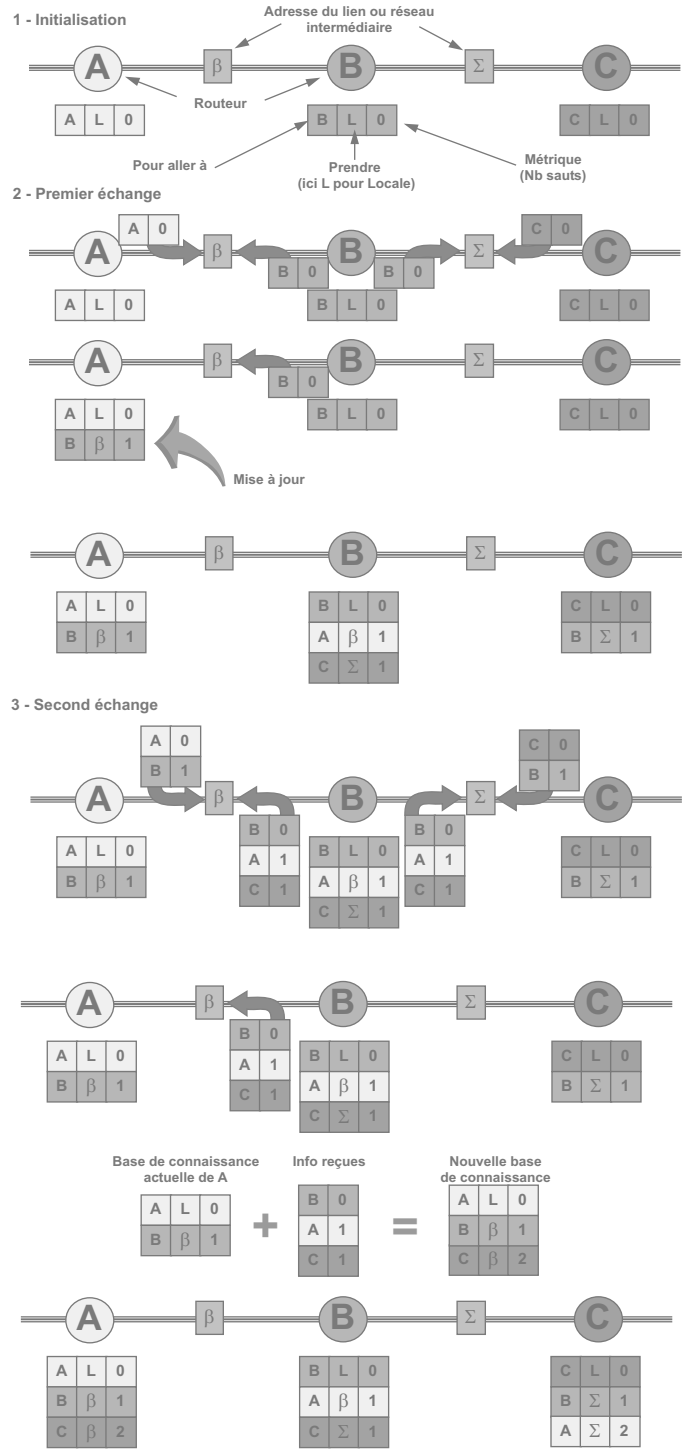


Figure 6.25 Échange des tables en routage vecteur distance.

Au premier échange, le nœud *A* apprend, qu'il peut joindre le nœud *B* en passant par le lien β pour un coût de 0 (contenu de la table du nœud *B* pour l'entrée *B*), coût auquel il convient d'ajouter le coût du transit sur le lien β soit ici 1. *A* n'a pas, en table, d'information concernant *B*, il met sa table à jour. Chaque nœud procède de même. En ne considérant que le nœud *A*, lors du second échange, *A* apprend qu'il peut joindre les nœuds *A*, *B* et *C* en passant par le lien β pour un coût respectif de :

- Pour *A*, de 1 (valeur reçue) + 1 (coût du lien β), soit 2, A a déjà une entrée pour cette destination avec un coût de 0, il conserve l'entrée de moindre coût.
- Pour *B*, de 0 + 1 soit 1, valeur déjà dans sa base connaissance, celle-ci est ignorée.
- Pour *C*, de 1 + 1 soit 2, *A* n'a aucune entrée concernant *C* dans sa table, il ajoute cette valeur.

Le même raisonnement est conduit pour chaque nœud. Les échanges ultérieurs n'apportent aucune connaissance nouvelle. Le routage dans le réseau a atteint sa stabilité (convergence des tables). Le routage par vecteur distance est, avec ses variantes, l'algorithme le plus utilisé. Mais indépendamment du fait que le temps de convergence peut être long, cet algorithme peut conduire à la création de boucles dans le réseau. La figure 6.26 illustre ce propos.

Supposons que le lien entre les nœuds *C* et *B* ne soit plus actif. Le nœud *B* ne recevant plus d'information en provenance de *C*, indique qu'il ne peut plus joindre *C* en portant le coût de la route Σ à l'infini. Ne pouvant atteindre cette destination *B* ne diffuse plus cette route. L'instant d'après, *B* reçoit la table de *A*, il apprend ainsi qu'il peut atteindre *C* en passant par β pour un coût de 2 + 1 soit 3, il met à jour sa table. Nous venons de créer une boucle, tout ce que *A* reçoit à destination de *C*, il l'envoie à *B*, tout ce que *B* reçoit à destination de *C,* il l'envoie en *A* !

À l'échange suivant, *A* apprend que joindre *C* en passant par β a maintenant un coût de 3 + 1 soit 4. Il met sa table à jour. À l'échange suivant, *B* passe le coût à 5, puis *A* à 6 jusqu'à ce que le coût devienne l'infini. Pour éviter la création d'une telle boucle, il faut d'une part limiter la valeur de l'infini. Le protocole RIP (*Routing Information Protocol*) fixe l'infini à 16, la convergence est alors plus rapide. Et d'autre part, il faut interdire aux nœuds de signaler qu'ils connaissent une destination au routeur par lequel ils l'ont apprise. Cette technique dite de l'horizon coupé ou *Split Horizon* interdit à *A* de signaler à *B* qu'il sait comment aller en *C* en passant par β.

➤ Principe des algorithmes dits à état des liens

Le principal défaut du routage vecteur distance provient du fait que les routeurs n'ont la connaissance d'un changement d'état du réseau que lorsque leur voisin le leur communique, ce qui peut être long. Pour pallier ce défaut, le routage à état des liens (*link state routing*) procède différemment (figure 6.27) :

- chaque nœud découvre ses voisins et détermine le coût du lien qui les relie ;
- le lien est testé régulièrement et en cas de modification de son coût, le nœud diffuse cette information dans le réseau, sous la forme (*A*, *B*, c), le lien du nœud *A* vers le nœud *B* a un coût de c ;
- chaque nœud entretien une table où figure, pour chaque lien, son coût (matrice de coûts). À l'aide de ces informations, chaque nœud peut reconstituer la cartographie complète du réseau ;
- à partir de la matrice des coûts, chaque nœud détermine alors sa table de routage (algorithme de Dijkstra).

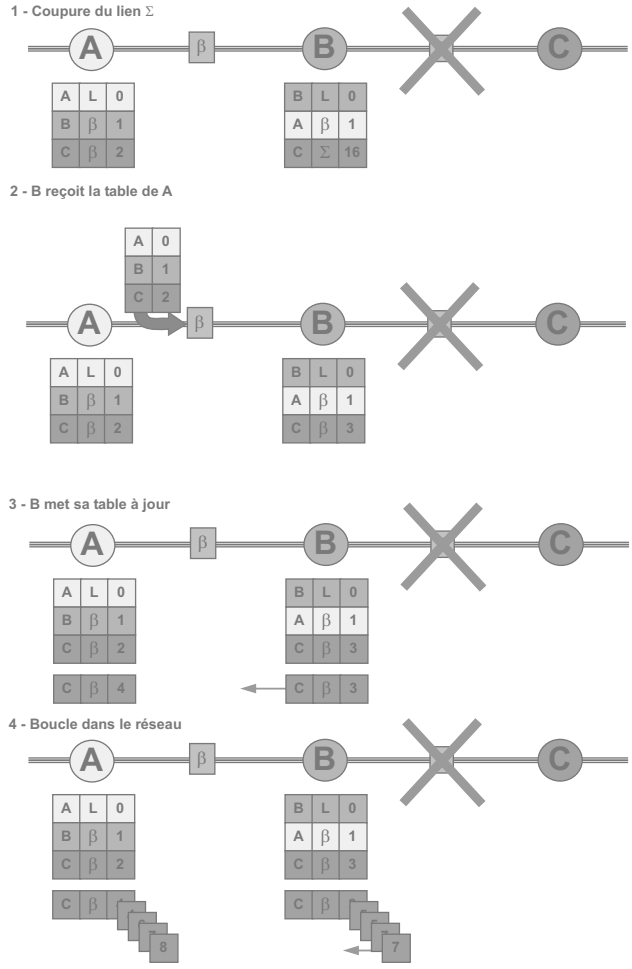


Figure 6.26 Notion d'horizon coupé.

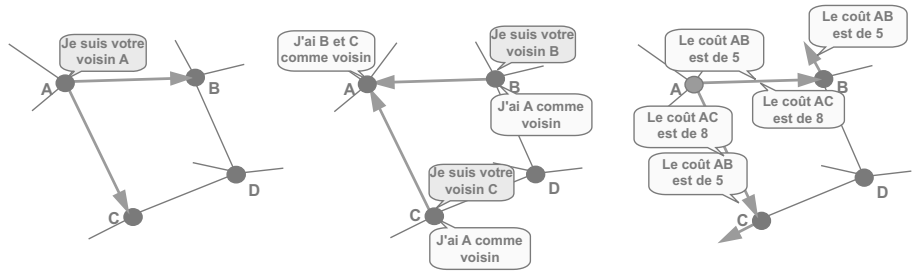


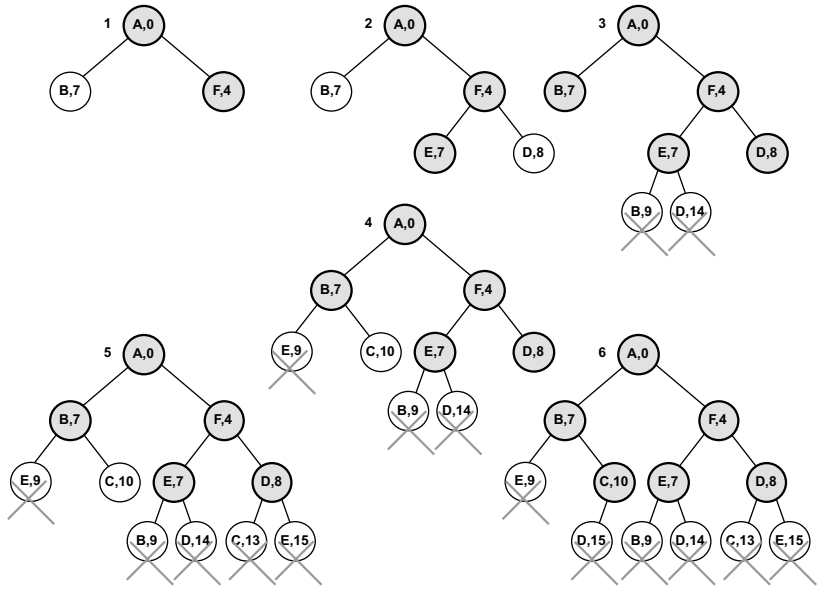
Figure 6.27 Principe des algorithmes à état des liens.

La figure 6.27 illustre le principe d'établissement des tables des routages, après découvertes des voisins, chaque nœud diffuse le coût des liens qui le rattachent à ses voisins. À partir de ces informations, il construit une matrice dite matrice des coûts (figure 6.28) qui va lui permettre de déterminer la route de moindre coût pour joindre chaque point du réseau.

$$M = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 4 \\ 7 & 0 & 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 & 7 & 4 \\ 0 & 2 & 0 & 7 & 0 & 3 \\ 4 & 0 & 0 & 4 & 3 & 0 \end{bmatrix}$$

de \ à	A	B	C	D	E	F
A	0	7	0	0	0	4
B	7	0	3	0	2	0
C	0	3	0	5	0	0
D	0	0	5	0	7	4
E	0	2	0	7	0	3
F	4	0	0	4	3	0

Figure 6.28 Exemple de matrice de coûts.



Routes validées	Routes découvertes		Routes en attente
A,0	AB,7 AF,4	(en attente, ➔) (validée)	AB,7
AF,4	FE,7 FD,8	(validée) (en attente ➔)	AB,7 FD,8
FE,7	EB,9 ED,14	(Fin et validation de AB,7) (Fin et validation de FD,8)	AB,7 FD,8
AB,7	BC,10 BE,9	(en attente, ➔) (Fin, on sait déjà aller en E pour 7)	BC,10
FD,8	DC,13 DF,15	(Fin et validation de BC,10) (Fin, on sait déjà aller en F pour 4)	BC,10
BC,10	CD,15	(Fin, on sait déjà aller en D pour 8)	Vide

Figure 6.29 Exemple de détermination de la table du nœud A.

Dans l'exemple de matrice de routage représentée figure 6.28, un coût nul signifie qu'il n'existe pas de lien entre les deux nœuds, la matrice est symétrique c'est-à-dire que nous avons admis que le coût de *A* vers *B* était identique à celui de *B* vers *A*. À titre d'illustration nous allons construire la table de routage du nœud *A* (figure 6.29 et 6.30). La figure 6.29 est déduite des informations de la matrice de la figure 6.28. Puisqu'il s'agit de déterminer la table de routage du nœud *A*, on se positionne en *A* et on examine qu'elles sont les directions joignables de *A* (de *A* on peut joindre *B* et *F*). On note alors le coût de chacune des directions et on ne retient que la route de moindre coût (lien AF). On réitère le raisonnement en partant maintenant de *F* (F est dit élu) et ceci jusqu'à ce que toutes les destinations aient été explorées. Les routes apparaissent dans le tableau avec le coût total pour joindre la destination depuis le nœud d'origine (*A*). Ainsi, « FE,7 » signifie : la route pour atteindre le nœud *E* en passant par F coûte 7 depuis la racine.

Une route (un lien) possède trois états :

– l'état validé (nœuds grisés figure 6.29), il n'existe, à partir de la racine, aucun autre chemin de moindre coût pour atteindre le nœud ;
– l'état découverte, il s'agit d'une nouvelle route pour joindre le nœud suivant à partir du nœud qui vient d'être validé ;
– l'état attente (nœuds blancs figure 6.29), après avoir été découverte une route peut être rejetée, s'il en existe déjà une de moindre coût pour joindre le nœud extrémité, ou être mise en attente.

La table de routage correspondante est donnée figure 6.30.

Nœud destination	Nœud suivant	Coût total
A	Local	0
B	B	7
C	B	10
D	F	8
E	F	7
F	F	4

Figure 6.30 La table de routage du nœud A.

Le routage à plat, routage hiérarchique

➤ Notion de domaine de routage

Le routage au moindre coût nécessite la diffusion, à travers le réseau, d'information concernant soit les tables de routage (*Vector distance*), soit l'état des liens (*Link status*). Ce trafic consomme de la bande passante au détriment des données à écouler. Plus le réseau est grand, plus le trafic de mise à jour est conséquent, plus les tables de routage sont importantes et plus le calcul des routes consomme du temps CPU. En routage hiérarchique (figure 6.31), le réseau est découpé en domaines appelés systèmes autonomes (**AS**, *Autonomus System*). Chaque domaine est identifié, les messages n'appartenant pas au domaine sont éliminés.

Ce mode de découpage des réseaux conduit à définir deux familles de protocoles de routage, notamment utilisés dans Internet :

– Les protocoles internes au domaine (**IGP**, *Interior Gateway Protocol*), qui assurent le routage dans un domaine, mais ignorent les nœuds des autres domaines.

© Dunod – La photocopie non autorisée est un délit

– Les protocoles externes au domaine (**EGP**, *External Gateway Protocol*), qui gèrent l'échange d'information entre domaines afin de découvrir la connectivité de chaque domaine.

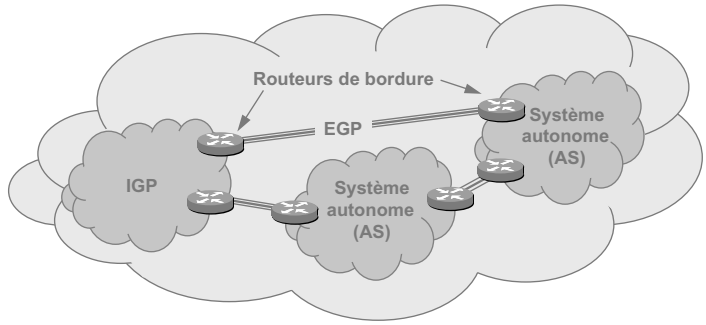


Figure 6.31 Le routage hiérarchique.

Chaque domaine est représenté et connu du reste du réseau par un nœud frontière, dit **routeur de bordure**, qui supporte à la fois un protocole intérieur au domaine et un protocole externe au domaine. Chaque domaine est autonome et peut mettre en œuvre un protocole de routage interne différent.

➤ Les principaux protocoles de routage

Les principaux protocoles de routage sont :

– **RIP** (*Routing Information Protocol*, RFC 1058 ; RIP-2, RFC 1723), du type vecteur distance, RIP a été le premier protocole de routage interne utilisé dans la communauté Internet, il est aujourd'hui remplacé par OSPF. Malgré une convergence lente et un trafic de gestion important, RIP reste le protocole de routage le plus employé.
– **OSPF** (*Open Short Path First*), d'origine IETF (RFC 2178), protocole interne à état des liens, il a remplacé RIP dans Internet. Pour éviter l'inondation, les informations d'état sont diffusées sur une adresse de multicast réservée à OSPF.
– **IS-IS** (*Intermediate System to Intermediate System*), le protocole de routage interne de l'ISO (ISO 10589), est aussi un protocole à état des liens.
– **IGRP** (*Interior Gateway Routing Protocol*), protocole propriétaire de la société Cisco du type vecteur distance, IGRP utilise une métrique construite qui prend en compte le délai d'acheminement, le débit, la fiabilité, la charge du réseau et la **MTU** (*Maximum Transfer Unit*).
– **EGP** (*Exterior Gateway Protocol*, RFC 827) a été le premier protocole externe utilisé dans Internet.
– **BGP** (*Border Gateway Protocol*, RFC 1771) protocole qui définit les échanges à l'intérieur du domaine (iBGP) et entre systèmes de bordure (eBGP).

Le routage et commutation

➤ Comparaison

Lorsque la décision d'acheminement est prise en fonction d'une adresse destination (mode datagramme ou paquet d'établissement dans le mode connecté), on parle de **routage** ; l'opération est

réalisée par un **routeur**. La table d'acheminement est dite **table de routage** (figure 6.32). Cette décision d'acheminement est prise, pour chaque datagramme, par chacun des routeurs traversés (*Hop by hop routing*). Il n'y a aucun contexte d'acheminement mémorisé. De ce fait, ce type de réseau résiste à la défaillance d'un nœud (réseau de type *Soft state* ou réseau sans état). Cependant, la prise de décision à chaque nœud traversé pénalise les performances et donc l'efficacité du transfert de données.

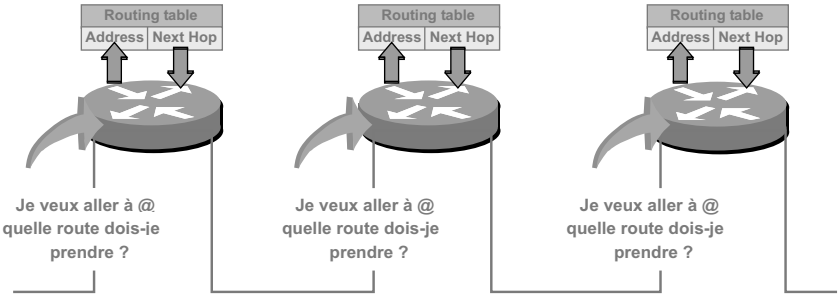


Figure 6.32 Le routage à travers le réseau.

Lorsque l'adresse destination n'intervient pas dans le processus de décision d'acheminement, on parle alors de commutation. En mode connecté (figure 6.33) préalablement à tout envoi de données, un circuit virtuel est construit par une opération de routage, la table de commutation est alors renseignée, les données sont ensuite commutées. La **table de commutation** contient un identifiant de flux attribué lors de la phase d'établissement (étiquette) et la voie à prendre. Dans la figure 6.33, ce qui arrive avec l'étiquette A par le port x et acheminé sur le port y avec l'étiquette B.

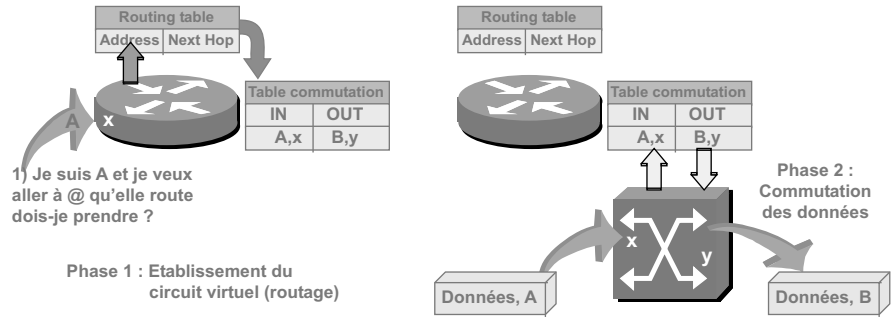


Figure 6.33 Après la phase d'établissement (1), la commutation (2).

La décision de commutation est plus rapide que la décision de routage, les protocoles récents dits à haut débit comme le Frame Relay ou l'ATM (*Asynchronous Transfer Mode*) utilisent ce principe. Devant l'efficacité de ce mode d'acheminement dans les réseaux, l'IETF a défini, pour les protocoles réseaux en mode non connecté, le protocole **MPLS** (*MultiProtocol Label Switching*) qui offre un service de type circuit virtuel à des protocoles en mode datagramme.

➤ Signalisation et établissement des routes

Le mode d'établissement des routes et les critères de sélection de celles-ci sont directement liés au mode de signalisation utilisé dans le réseau. Si le protocole réseau utilise une signalisation

© Dunod – La photocopie non autorisée est un délit

dans la bande, la demande d'établissement de route est transportée dans une unité de données du protocole de transfert. Elle doit donc être traitée par la même entité de programme. Le processus d'établissement des routes rentre en concurrence directe avec celui de commutation. Ce système pénalise les performances (figure 6.34).

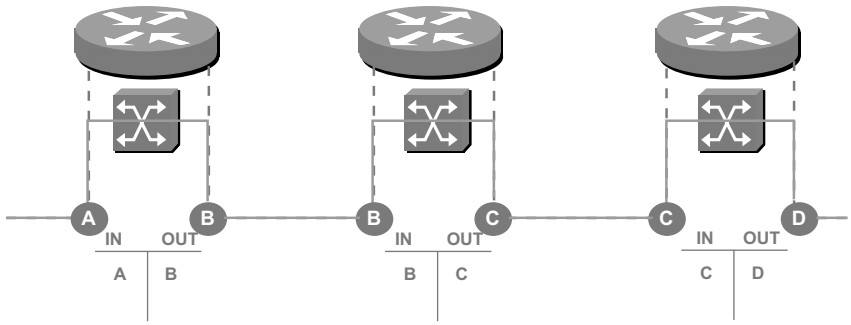


Figure 6.34 La commutation et la signalisation dans la bande.

Lorsque le réseau utilise une signalisation par canal sémaphore, le protocole de signalisation et celui de transfert sont indépendants. Établissement de routes et commutation sont traités par des entités de programme différentes. Indépendamment du gain en performance, l'indépendance des protocoles permet l'utilisation d'un protocole de signalisation beaucoup plus riche en information, notamment celui-ci pourra transporter des informations en relation directe avec la qualité de service exigée par le flux pour lequel la construction d'un circuit virtuel est demandée (figure 6.35). Les protocoles dits haut débit comme ATM et Frame Relay utilisent ce mode de signalisation.

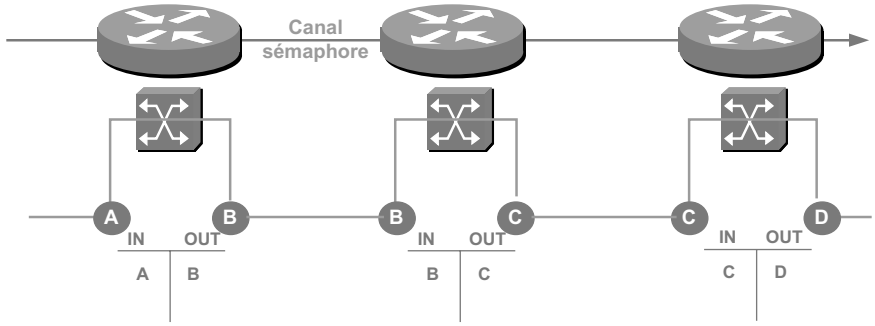


Figure 6.35 La commutation et la signalisation hors bande.

➤ Du routage à la commutation

Les réseaux en mode datagramme ne disposent d'aucun mécanisme d'établissement de route ce qui leur confère une grande souplesse notamment une grande résistance à la défaillance. Cependant, le mode connecté, en garantissant le séquencement des informations et optimisant le processus d'acheminement, présente des avantages certains notamment pour le transfert des flux multimédia. La figure 6.36 réalise une comparaison succincte des deux modes en mettant en évidence les points forts de chacun d'eux.

Critères	Mode connecté	Mode non connecté
Mise en relation	Oui	NON
Connexion/Déconnexion	Oui	NON
Circuit offert	Permanent durant tout l'échange	Pas de circuit réservé Best effort
Résistance à la défaillance	Non, réseau à état (Hard State)	Oui, réseau sans état (Soft State)
Garantie du séquencement	OUI	Non
Optimisation du réseau	Non	Oui
Optim. de l'acheminement	OUI	Non
	Commutation	Routage

Figure 6.36 La comparaison des modes de mise en relation.

Aussi, ne serait-il pas possible d'imaginer un protocole réseau qui réalise une synthèse entre ces modes en offrant dans un environnement datagramme les performances du mode connecté ? C'est l'objectif de **MPLS** (*MultiProtocol Label Switching*) qui autorise un acheminement commuté des datagrammes. À cet effet, un protocole de distribution d'identifiants de route ou labels prédétermine des routes en établissant une correspondance entre une destination IP et un label. En fonction de son adresse destination, chaque datagramme se voit affecter à l'entrée du réseau, par le routeur de périphérie d'entrée (*Edge Label Switching Router* ou **eLSR**), un identifiant de route (label). Il est ensuite acheminé dans le réseau par rapport à cet identifiant et non plus en fonction de l'adresse destination. Comme dans les réseaux en mode connecté, l'identifiant n'a qu'une valeur locale. Le routeur de sortie supprime le label et achemine le datagramme vers sa destination. L'ensemble forme un réseau MPLS (figure 6.37).

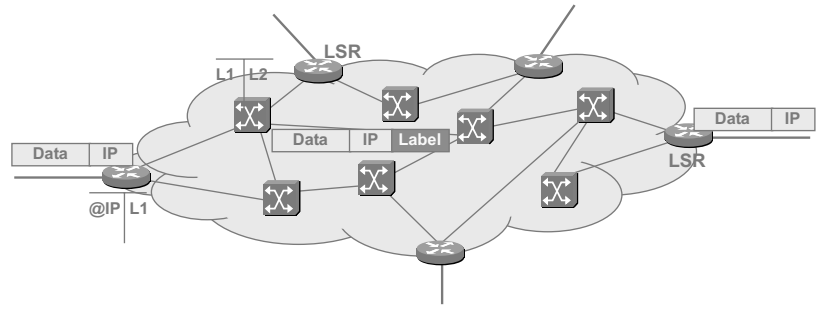


Figure 6.37 Principe de la commutation MPLS.

6.7 L'ADAPTATION DE LA TAILLE DES UNITÉS DE DONNÉES

6.7.1 La notion de MTU

Lors du transfert d'un bloc de données dans un réseau, chaque élément du réseau (routeur ou commutateur) doit mémoriser les blocs en entrée, les traiter et les délivrer à la file d'attente de sortie.

© Dunod – La photocopie non autorisée est un délit

Ces différents traitements nécessitent de la mémoire. La ressource étant limitée, il est nécessaire de fixer une taille maximale aux unités de données admises dans un réseau.

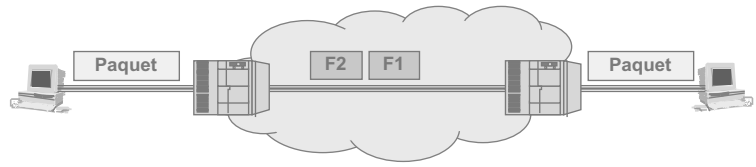


Figure 6.38 La fragmentation d'un paquet.

On appelle **MTU** (*Maximum Transfer Unit*) ou unité de transfert maximale, la taille maximale des données admises dans un réseau en-tête compris. Si un bloc a une taille supérieure à la MTU, il devra être fragmenté en plusieurs blocs pour pouvoir être acheminé dans le réseau (figure 6.38).

6.7.2 La segmentation et le réassemblage

Dans les réseaux en mode non connecté, les fragments sont susceptibles d'arriver sans respect de l'ordonnancement. Le réassemblage ne peut être réalisé dans le réseau, c'est le destinataire qui devra reconstituer l'unité de données d'origine. Pour garantir le réassemblage correct du message initial, il est nécessaire d'identifier tous les fragments d'un même datagramme et de les numéroter pour les réordonner.

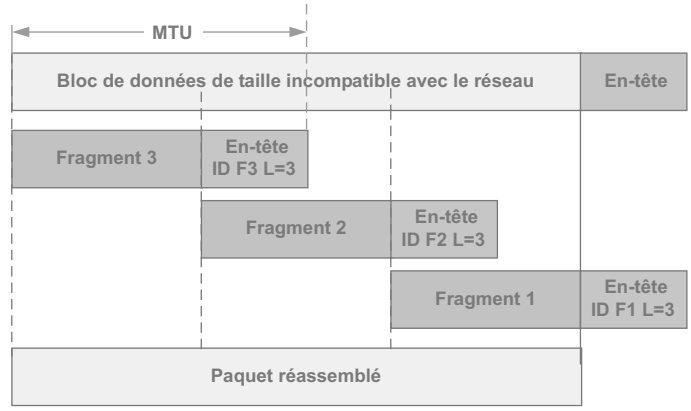


Figure 6.39 Les informations de fragmentation en mode non connecté.

Chaque fragment (figure 6.39) comporte les informations nécessaires à son acheminement (adresse). Une donnée d'identification est recopiée dans chaque fragment (ID). Le réassemblage nécessite aussi de connaître la longueur totale du paquet d'origine (*L*) et de disposer d'une information sur l'ordonnancement (F1, F2...). Outre le temps nécessaire aux opérations de fragmentation, en mode non connecté, la reprise sur erreur dans le réseau étant impossible, la perte d'un seul fragment implique la retransmission de tout le datagramme. Pour ne pas pénaliser le réseau, les protocoles en mode non connecté offrent généralement des services de découverte de la MTU.

Dans les réseaux en mode connecté, tous les fragments suivent le même chemin, le séquencement est garanti. Dans ces conditions, les informations nécessaires au réassemblage peuvent être réduites

à un seul bit (bit *More*, données à suivre). Le bit More est positionné à 1 dans tous les fragments sauf le dernier. Le réassemblage peut être réalisé par le réseau, la fragmentation est alors dite transparente (figure 6.40)

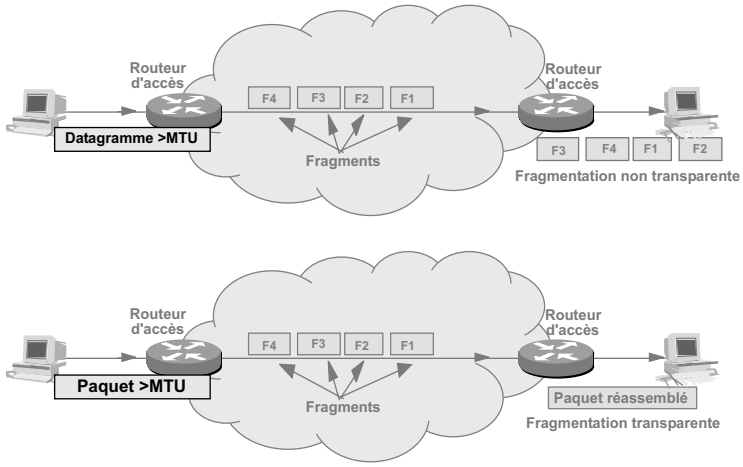


Figure 6.40 La fragmentation transparente et non transparente.

6.8 LA CONGESTION DANS LES RÉSEAUX

6.8.1 Définition

Basé sur un trafic sporadique et aléatoire, le partage statistique des ressources d'un réseau fragilise celui-ci. À une augmentation de trafic soumis, correspond une augmentation du temps d'attente avant traitement dans les nœuds. Vu des sources, le débit diminue, le temps de transit dans le réseau croît (congestion légère). Les paquets retardés peuvent, dans ce cas, ne pas être acquittés dans les délais, ce qui provoque leur retransmission et contribue à augmenter la charge du réseau, plus de paquets ne sont pas acquittés à temps, plus les files d'attente débordent... Le réseau s'effondre, c'est la congestion sévère (figure 6.41).

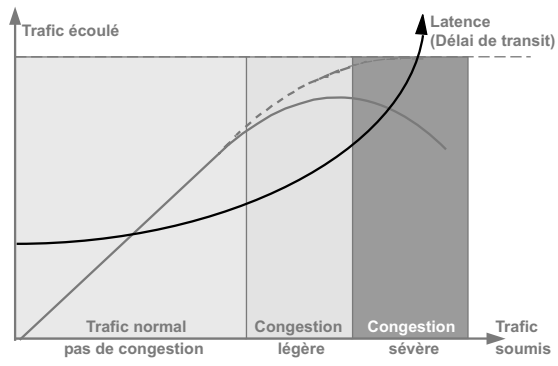


Figure 6.41 L'écoulement du trafic dans un réseau.

© Dunod – La photocopie non autorisée est un délit

En présence d'une surcharge du réseau, les mécanismes de reprise sur erreur des protocoles ont tendance à réagir ensemble. L'indépendance des sources n'est plus vraie, la congestion s'installe.

Indépendamment du blocage du réseau, si on veut garantir une certaine qualité de service, il est nécessaire de mettre en œuvre des mécanismes spécifiques pour d'une part, prévenir l'état de congestion et, d'autre part, si celui-ci apparaît, le résoudre (guérison). Ces mécanismes constituent le contrôle de congestion.

6.8.2 Les mécanismes de prévention de la congestion

La *congestion* résulte d'un trafic à écouler supérieur aux capacités du réseau, la solution la plus simple, pour se prémunir contre celle-ci, consiste à ne pas admettre, dans le réseau, plus de trafic que celui-ci est capable d'assimiler. Plusieurs solutions sont envisageables :

– asservir le débit des sources sur les capacités de traitement de chacun des nœuds, c'est le **contrôle de flux** ;
– ne pas admettre plus de trafic dans le réseau que celui-ci n'est capable d'en écouler, c'est le **contrôle d'admission** ;
– éviter la propagation de rafales de données au cœur du réseau en réalisant un **lissage de trafic**.

Le contrôle de congestion et contrôle de flux

Les notions de contrôle de flux et de contrôle de congestion sont différentes. Le contrôle de flux s'intéresse aux échanges entre deux nœuds alors que le contrôle de congestion cherche à limiter le nombre de paquets en transit dans le réseau (figure 6.42). Cependant, en limitant la longueur des files d'attente dans les nœuds intermédiaires, le contrôle de flux participe à la prévention de la congestion.

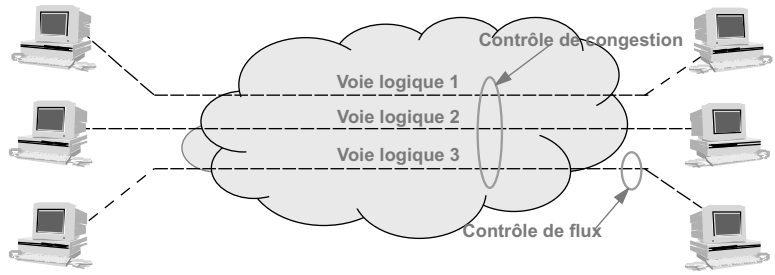


Figure 6.42 Distinction entre contrôle de flux et contrôle de congestion.

Le contrôle de flux reste un mécanisme insuffisant. Dans les réseaux modernes, compte tenu du débit, la taille de la fenêtre est importante et le contrôle de flux devient inefficace, il a par conséquent été abandonné.

Le contrôle d'admission

Les réseaux en mode circuit sont naturellement protégés contre la congestion. En cas de manque de ressource dans le réseau, la connexion est purement et simplement refusée. Ce mode de prévention

se heurte au principe de mutualisation des ressources. Une politique plus souple peut être utilisée : le contrat de service ou **SLA** (*Service Level Agreement*) dont un exemple est fourni figure 6.43.

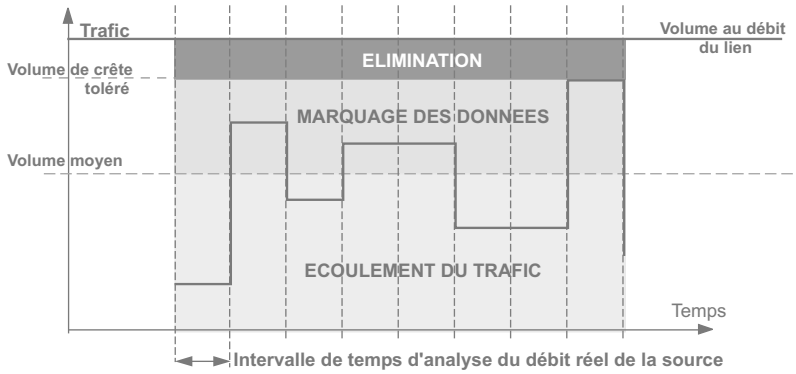


Figure 6.43 Principe du contrat de service.

Chaque abonné du réseau spécifie, à l'abonnement ou à la connexion, la description du trafic qu'il va soumettre au réseau. Une fonction de surveillance vérifie en permanence que le flux respecte le contrat. Trois zones de fonctionnement peuvent alors être définies. La première correspond à un trafic garanti. Ce trafic, dit **trafic moyen** est toujours écoulé par le réseau quel que soit son état. La seconde zone correspond à un volume excédentaire mais toléré, les données remises au réseau sont acheminées mais identifiées (*Cell tagging*). En cas de congestion, elles seront éliminées. Enfin, la troisième zone définit un volume excédentaire mais hors contrat, ce trafic est purement et simplement refusé par le réseau. C'est le nœud d'accès au réseau qui assure le contrôle d'admission (**CAC**, *Connection Admission Control*).

Le lissage de trafic

Même si chaque source respecte son contrat de service, la congestion peut résulter de la simultanéité de soumission de rafales par les différentes sources. Pour éviter cet afflux sporadique, on effectue, à l'entrée du réseau, un lissage du trafic (technique du seau percé, *Leaky bucket algorithm*). Dans ce système, les données sont mises en file d'attente et délivrées régulièrement. Le mécanisme du seau percé est un mécanisme de prévention, ce n'est pas un mécanisme de résolution ; la figure 6.44 illustre ce principe.

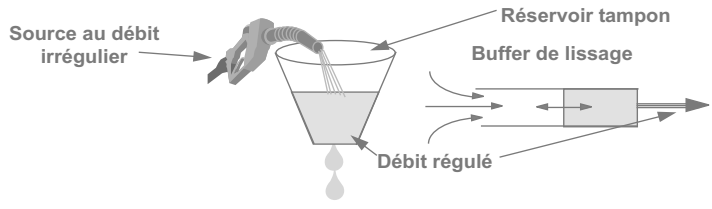


Figure 6.44 La technique du sceau percé.

© Dunod – La photocopie non autorisée est un délit

La figure 6.45 illustre la mise en œuvre du contrôle d'admission et de lisage de flux tel qu'ils sont mis en œuvre dans les réseaux Frame Relay.

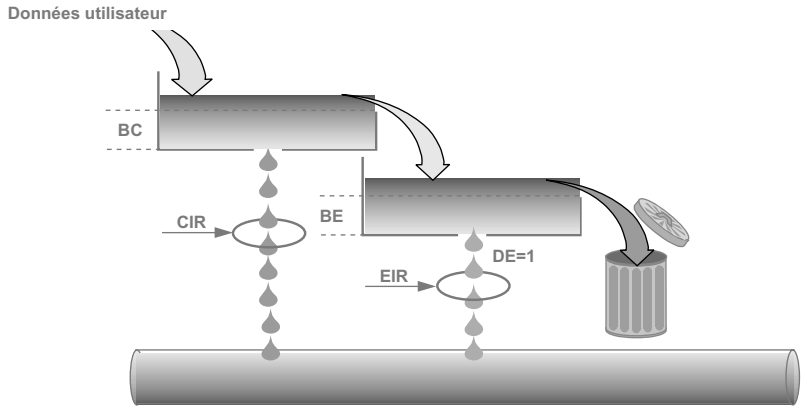


Figure 6.45 Le contrôle d'admission et le lissage de trafic.

Le Frame Relay définit deux niveaux d'analyse du trafic. Le premier est un trafic garanti correspondant à un débit moyen (**CIR**, *Committed Information Rate*) et à un volume associé (**Bc**, *Committed Burst size*). Le deuxième niveau correspond à un volume toléré qui n'est acheminé que si le réseau le permet, le débit excédentaire associé est dénommé **EIR** (*Excess Information Rate*) et correspond à un volume dit **Be** (*Excess Burst size*). Les données écoulées dans cet intervalle de trafic sont marquées (positionnement du bit **DE** ou *Discard Eligibility*) et éliminées en cas de congestion.

6.8.3 La résolution ou la guérison de la congestion

Quels que soient les mécanismes de prévention utilisés, rien ne permet de garantir qu'un état de congestion ne peut apparaître. Plusieurs politiques peuvent être mises en œuvre pour réduire la congestion : elles visent toutes à éliminer le trafic en excès. Ces solutions dérivent des principes suivants :

– mettre en attente le trafic excédentaire dans une file d'attente de moindre priorité ;
– identifier le trafic excédentaire (*Cell tagging*) et l'éliminer en cas de congestion ;
– éliminer tout le trafic ;
– envoyer à la source ou aux sources responsables une demande de ralentissement.

Le traitement de l'état de congestion provoque une diminution des performances globales du réseau et peut engendrer des phénomènes oscillatoire si les mécanismes de correction sont mal dimensionnés et non progressifs.

Dans les réseaux en mode datagramme, c'est aux systèmes d'extrémités (systèmes clients) que revient la tâche de contrôler le trafic dans le réseau.

6.9 LA VOIX DANS LES RÉSEAUX EN MODE PAQUET

6.9.1 Intérêt et contraintes

L'intégration voix/données consiste à transporter la voix sur un réseau en mode paquet en mixant les flux (figure 6.46). Elle allège les infrastructures réseaux, puisqu'une seule infrastructure supporte l'ensemble des trafics et optimise l'utilisation du réseau par récupération des silences. La fédération des ressources en une entité unique banalise l'infrastructure locale, simplifie l'administration, permet d'envisager de nouveaux services et, enfin, diminue les coûts, le trafic voix étant facturé au coût de la donnée généralement bien inférieur à celui des services voix.

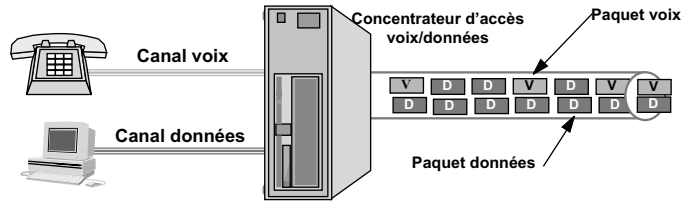


Figure 6.46 Principe des réseaux voix/données.

La voix est un flux temps réel, **isochrone** et *full duplex*. L'adaptation du trafic voix à un réseau de données doit garantir l'intelligibilité et l'interactivité ce qui nécessite :

- de modéliser le flux voix comme un flux de données (paquétisation) ;
- d'adapter les mécanismes réseaux aux contraintes temps réel (temps de traversée, correction de gigue) ;
- de transformer le flux d'information constant en un flux périodique réduit (compression).

6.9.2 Le principe de la paquétisation de la voix

La numérisation de la voix fournit un flux de 1 octet toutes les 125 μs, le mode paquet nécessite l'ajout d'information d'acheminement. Il est donc inconcevable de faire sur le réseau 1 octet = 1 paquet. Par conséquent, il convient d'attendre un certain nombre d'octets, de les rassembler en un seul paquet avant de les acheminer sur le réseau. La paquétisation introduit donc un délai, dit **délai de paquétisation**, valant $N \cdot 125$ μs si le paquet contient N octets (figure 6.47).

Le délai de paquetisation introduit un retard d'autant plus important que le paquet est grand. La taille du paquet résulte d'un compromis entre l'optimisation de la transmission, le retard introduit par le délai de paquétisation et l'influence de la perte d'un paquet sur l'intelligibilité de la voix. La figure 6.48 illustre le bilan temps d'une liaison voix sur un réseau en mode paquet.

Outre les informations de voix, une liaison voix doit assurer le transport des informations de signalisation. Ainsi, une unité de données de voix devra comporter les informations relatives au contenu du paquet (données, voix, signalisation), à l'identification de la communication et éventuellement des informations temporelles.

© Dunod – La photocopie non autorisée est un délit

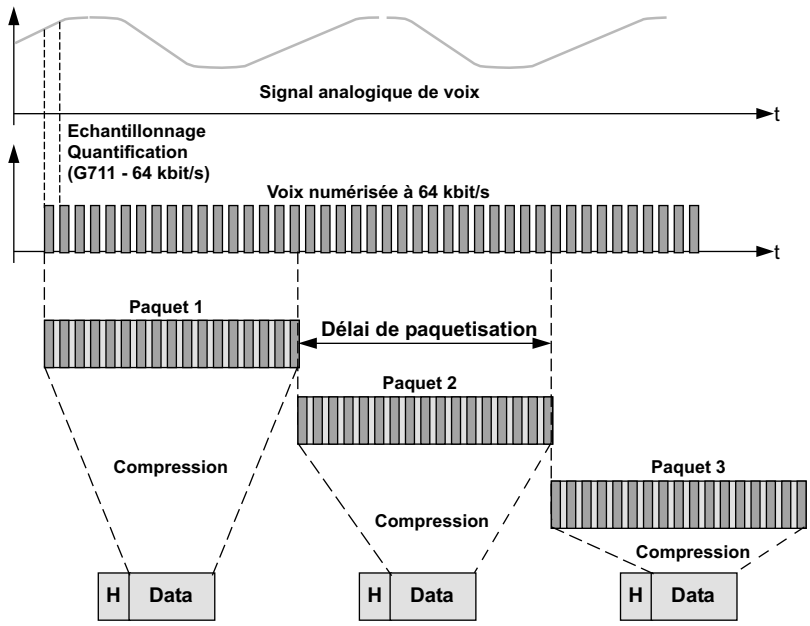


Figure 6.47 Principe de la paquétisation de la voix.

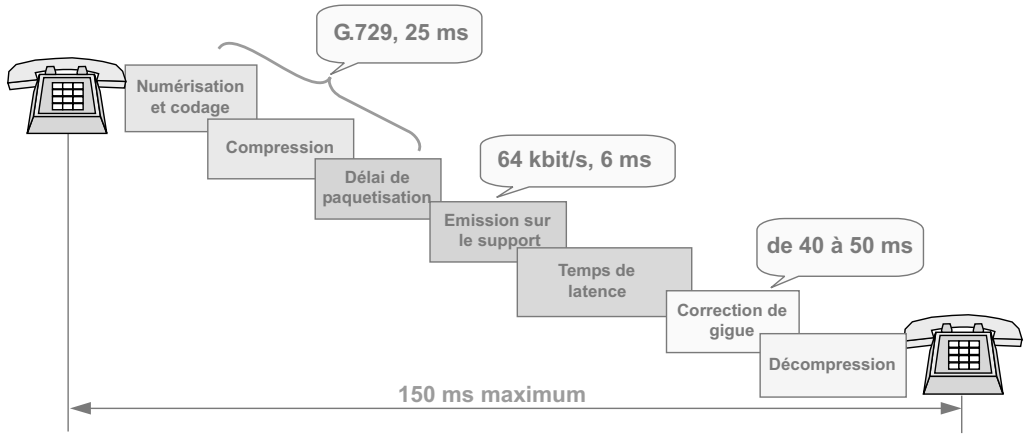


Figure 6.48 Le bilan temporel d'une liaison voix.

6.10 CONCLUSION

Les techniques réseaux sont en perpétuelle évolution, le besoin grandissant en bande passante, les contraintes spécifiques à chaque type de flux dopent une recherche très active de la part des constructeurs.

Dans quel cadre doivent se faire les développements, selon quels principes, telles sont les questions auxquelles la normalisation doit répondre pour fournir un cadre de développement et garantir l'interopérabilité des systèmes.

EXERCICES

Exercice 6.1 Évaluation du nombre de liaisons

Déterminez le nombre de liaisons nécessaires à la réalisation d'une interconnexion totale entre 100 équipements.

Exercice 6.2 Table de routage

En reprenant la matrice de routage de la figure 6.28, établissez la table de routage du nœud B et déterminez la topologie du réseau.

Exercice 6.3 Temps de transfert sur un réseau

Deux réseaux LAN de type Ethernet (MTU 1 500 octets) sont interconnectés par un réseau de type WAN. Déterminez le temps nécessaire à l'envoi d'un message de 1 480 octets dans les conditions suivantes :

- le protocole réseau nécessite 20 octets d'en-tête (Hn) ;
- le protocole de ligne utilisé sur les liens du WAN rajoute 8 octets d'en-tête (Hl).

et dans les différents modes suivants :

1. En mode commutation de circuits.
2. En mode commutation de messages (dans les mêmes conditions, c'est-à-dire par blocs de 1 500 octets). Le réseau comporte cinq nœuds hors organes d'extrémité.
3. En mode commutation de paquets (mode non connecté, mais les datagrammes seront supposés emprunter le même chemin). Le réseau comporte cinq nœuds hors organes d'extrémité. Faire le calcul pour une MTU de 57, 168, 316 octets. Rappelons que le LAN transmet au routeur des trames de MTU 1 500 octets, c'est le routeur qui a en charge l'adaptation des unités de données au réseau (segmentation).

Le débit des liens sera supposé de 64 kbit/s, les temps de traitement et des stockages intermédiaires seront considérés comme nul. On ne tiendra pas compte des temps d'émission sur les réseaux locaux, seul sera pris en compte le temps de traversée du WAN. Quels commentaires pouvez-vous faire ?

Exercice 6.4 Routage et commutation

Quelles différences faites-vous entre commutation, routage et brassage ?

Exercice 6.5 Commutation de circuits et de paquets

Comparez la commutation de circuits aux modes de mises en relation de la commutation de paquets (complétez la figure 6.49).

Caractéristiques	Commutation de circuits	Commutation de paquets	
		Mode orienté connexion (circuit virtuel, CV)	Mode datagramme
Circuit dédié			
Débit disponible			
Optimisation de l'utilisation de la bande passante			
Établissement du circuit (connexion) lors de la séquence d'appel			
Adressage			
Information de routage			
Routage			
Conséquence d'une défaillance de routeur			
Quand peut apparaître la congestion ?			
Contrôle de congestion			
Principe de facturation			

Figure 6.49 La commutation de circuits et la commutation de paquets.

Partie **II**

L'architecture protocolaire

7 Les architectures protocolaires 213
7.1 Introduction 213
7.2 Les concepts de base 214
7.3 L'organisation du modèle de référence 219
7.4 L'étude succincte des couches 225
7.5 Les architectures constructeurs 243
7.6 Conclusion 244
EXERCICES 245

8 Introduction à TCP/IP 247
8.1 Généralités 247
8.2 L'adressage dans le réseau logique 253
8.3 Le routage dans le réseau IP 264
8.4 L'adressage dans IPv6 266
8.5 Conclusion 270
EXERCICES 271

9 L'architecture TCP/IP et le niveau liaison 273
9.1 Généralités 273
9.2 Les protocoles de liaison (point à point) 274
EXERCICE 286

10 Le protocole IP et les utilitaires réseaux 289
10.1 Généralités 289
10.2 La structure du datagramme IP 289
10.3 Le contrôle de la fragmentation sous IP 294
10.4 Les utilitaires de la couche réseau 295
10.5 D'IPv4 à IPv6 305
10.6 IP et la mobilité 309
10.7 L'encapsulation GRE 315
10.8 Conclusion 316
EXERCICE 317

11 Les protocoles de transport : TCP et UDP 319
11.1 Généralités 319
11.2 Les mécanismes de base de TCP 320
11.3 Le message TCP et les mécanismes associés 330
11.4 Les options de TCP 332
11.5 Le mode datagramme (UDP) 335
11.6 Conclusion 335
EXERCICES 337

12 TCP/IP et les applications 339
12.1 Introduction 339
12.2 Les notions d'annuaire 339
12.3 Le transfert de fichiers 348
12.4 L'émulation de terminal (Telnet) 351
12.5 Les notions de Middleware 353
12.6 Conclusion 358
EXERCICES 360

Chapitre 7

Les architectures protocolaires

7.1 INTRODUCTION

Le développement rapide des moyens de calcul et l'importance croissante des systèmes d'information ont engendré la multiplicité des techniques réseaux. La complexité croissante des besoins de communication et la diversité des solutions adoptées ont très vite fait apparaître la nécessité de définir un modèle complet de communication ou **architecture protocolaire réseau**.

Historiquement, chaque grand constructeur avait défini la sienne : SNA (*System Network Architecture*) pour IBM, DSA (*Distributed System Architecture*) pour BULL... Ces architectures propriétaires incompatibles entre elles ne permettent pas l'interopérabilité des systèmes. Aussi, convenait-il de définir des techniques de mises en relation en spécifiant une architecture normalisée. C'est ce qu'entreprit l'ISO (*International Standardization Organization*) en définissant une architecture de communication normalisée, couramment appelée modèle de référence ou modèle **OSI** (*Open System Interconnection*)[1].

L'architecture réseau assure à l'utilisateur l'accès aux ressources informatiques et lui procure un service identique que les ressources soient locales ou distantes, et cela de manière transparente pour l'utilisateur (figure 7.1).

Connecter en transparence des équipements provenant de constructeurs différents pour qu'ils s'échangent des informations nécessite que ceux-ci utilisent non seulement des techniques de connexion compatibles (raccordement, niveau électrique...), mais aussi des protocoles d'échange identiques et une sémantique de l'information compréhensible par les partenaires de la communication. Ces problèmes, de nature différente, peuvent être résolus chacun par une solution spécifique.

1. C'est une habitude franco-française de traduire le terme ISO en *International Standardization Organization* ; en fait le nom officiel de l'ISO est : « *International Organization for Standardization* » et c'est parce que le nom de l'Organisation internationale de normalisation donnerait lieu à des abréviations différentes selon les langues (« IOS » en anglais et « OIN » en français), qu'il a été décidé d'emblée d'adopter un mot dérivé du grec *isos*, signifiant « égal ». La forme abrégée du nom de l'organisation est par conséquent toujours ISO (extrait du site officiel de l'ISO - `www.iso.org`).

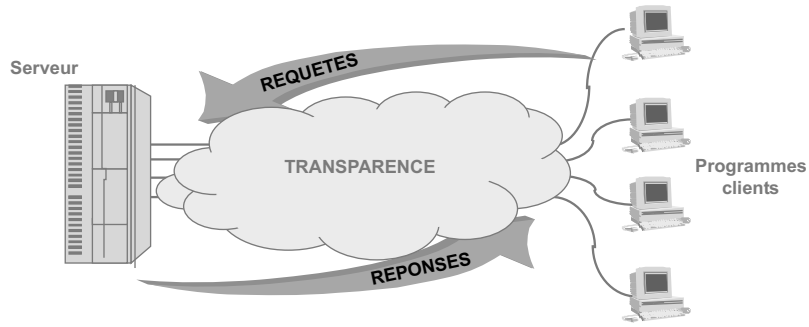


Figure 7.1 L'architecture garantit la transparence.

Aussi, pour éviter une description trop complexe, le système a été découpé en entités fonctionnelles appelées couches. Une **couche** est donc un ensemble homogène destiné à accomplir une tâche ou à rendre un service. L'approche en couche garantit une évolutivité facile du système. La prise en compte d'une nouvelle technologie ne remet en cause que la couche concernée. Le modèle de référence est une architecture en couches.

7.2 LES CONCEPTS DE BASE[2]

7.2.1 Principe de fonctionnement d'une architecture en couches

Considérons le modèle simplifié à trois couches représenté figure 7.2.

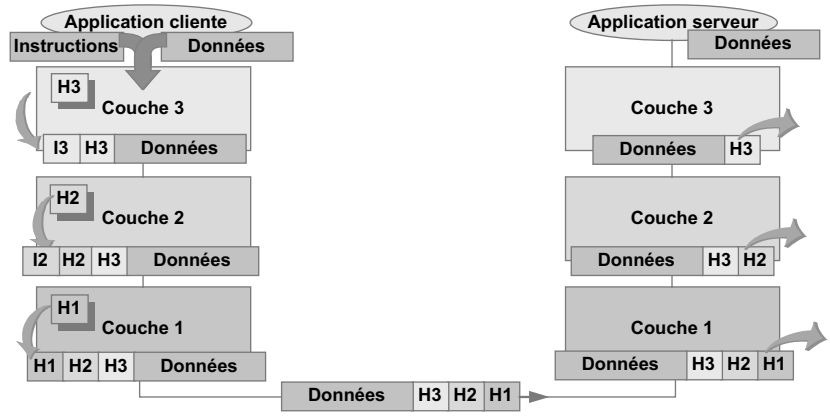


Figure 7.2 Principe général de fonctionnement d'un modèle en couches.

Pour communiquer l'application cliente remet à la couche supérieure, ici la couche 3, des données à destination de l'application serveur ainsi que les instructions décrivant le service attendu

2. Tous les modèles architecturaux utilisent les mêmes principes. Dans les paragraphes qui suivent, nous emploierons, pour décrire ces principes, la terminologie utilisée par l'ISO dans la description de son modèle de référence.

et celles nécessaires à l'acheminement des données vers l'application serveur. La couche 3 interprète les instructions reçues et confectionne une structure de données à destination de la couche 3 distante, dite couche homologue. Cette structure de données est constituée d'une part des informations nécessaires à la couche 3 distante pour traiter ces données appelées en-tête de niveau 3 (H3 pour *Header* de niveau 3) et des données elles-mêmes ; l'ensemble formant une unité de données de niveau N. Les règles d'échange entre données de même niveau constituent un protocole de niveau N.

Puis, la couche 3 remet cette unité de données et des instructions (I3) à la couche inférieure qui procède de même... Enfin les données sont émises sur le support physique. En réception la couche la plus basse extrait l'en-tête protocolaire (H1), l'interprète, et remet les données à la couche supérieure qui procède de même jusqu'à remise des données à l'application distante.

7.2.2 La terminologie

Protocole et service

L'échange précédent, illustré figure 7.2, montre deux types de dialogues (figure 7.3) :

– un dialogue vertical qui correspond aux transferts d'informations d'une couche à une autre (couches adjacentes), ce dialogue est réalisé à l'aide de **primitives de service** ;
– un dialogue horizontal qui, par l'intermédiaire de messages échangés (protocole) à travers le réseau, transfère, entre couches distantes de même niveau (**couches homologues**), les données d'un système à un autre. Ce dialogue constitue le **protocole de niveau N**.

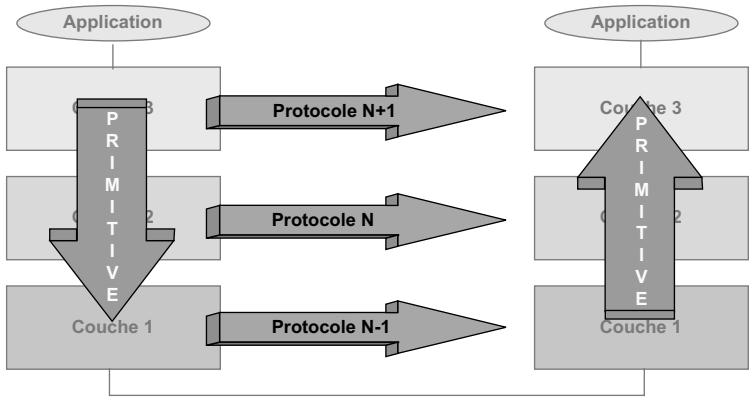


Figure 7.3 Les protocoles et les primitives de service.

L'encapsulation de données

La couche (N+1), en remettant les données à la couche N, a requis les services de niveau N, à l'aide d'une primitive de service de niveau N (figure 7.4). Peu importe à (N+1) de savoir comment ces services sont rendus. L'unité de données protocolaire de niveau (N+1), données et en-tête, est transportée dans une unité de données de niveau N (protocole N). Les données de niveau (N+1) sont dites **encapsulées** dans le protocole N, on parle aussi de **tunnel de niveau N**.

© Dunod – La photocopie non autorisée est un délit

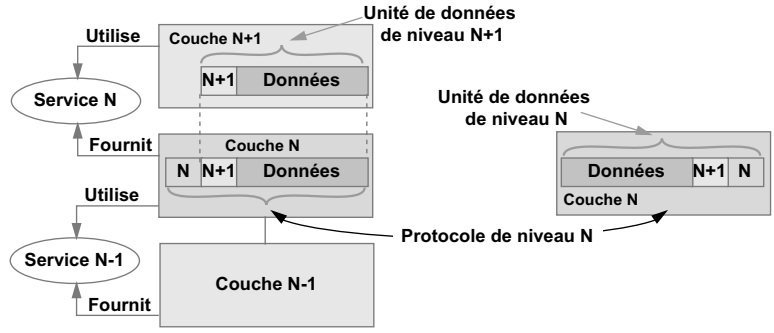


Figure 7.4 Le service et l'encapsulation de données.

Le point d'accès au service (SAP)

Une couche (N) procure le service (N) au moyen d'un protocole de niveau (N). Le service de la couche (N) est fourni par une entité de niveau (N) qui est une occurrence d'un élément actif de la couche (N). La figure 7.5 illustre ce principe.

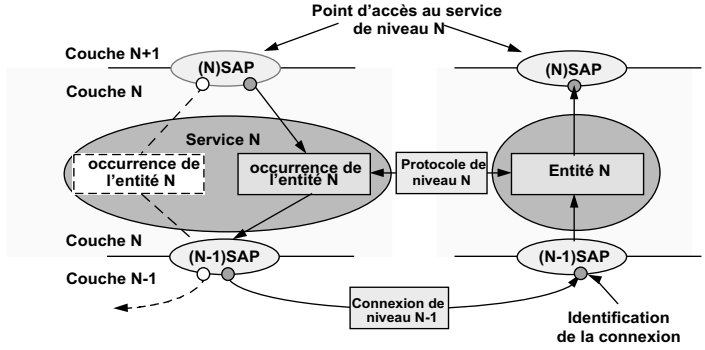


Figure 7.5 L'identification des services.

Les services de la couche (N) sont offerts par une entité de niveau N et accessibles *via* une interface désignée par un identificateur ou point d'accès au service (**SAP**, *Service Access Point*). Un SAP ne peut être rattaché qu'à une seule entité, mais une même couche peut mettre en œuvre plusieurs occurrences de l'entité de niveau (N).

Le dialogue OSI est un dialogue entre entités homologues distantes *via* une mise en relation ou connexion de niveau (N–1).

Les unités de données manipulées

Les données manipulées par une couche et envoyées à l'entité homologue constituent une unité de données (*Data Unit*). La couche de niveau (N+1), utilisatrice des services de niveau (N), adresse

à la couche (N), des unités de données de service notées (N)SDU[3] (*Service Data Unit*). Pour la couche (N), les données entrantes sont considérées comme utilisatrices du service (N).

La couche N ajoute aux données reçues (SDU) des informations de service nécessaires à la couche N homologue pour que celle-ci traite et délivre correctement les données à sa couche (N+1) distante. Ces informations de protocole constituent le (N)**PCI** (*Protocol Control Information*). Les données sont acheminées vers l'entité homologue *via* une connexion de niveau (N–1). La couche N distante recevant la (N)SDU extrait le (N)PCI, l'interprète et délivre les données (N)SDU à la couche (N+1) ; ces données deviennent alors la (N+1)PDU. La figure 7.6 illustre ce mécanisme.

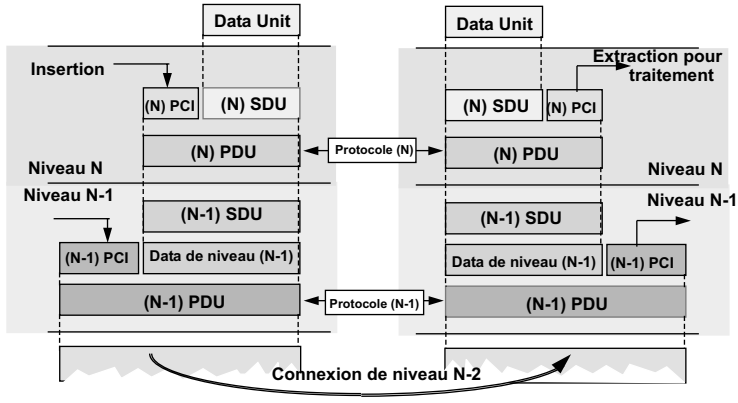


Figure 7.6 Le modèle général d'une couche.

Ainsi, chaque couche ajoute (ou extrait) un en-tête (*Header*), spécifique au protocole utilisé. Cet en-tête contient toutes les informations nécessaires au traitement distant de l'unité de données : l'identifiant de la connexion, l'adresse du destinataire, les compteurs de contrôle de l'échange...

Le contrôle de l'interface

Lors de l'invocation d'un service de niveau (N), le niveau (N+1) fournit un ensemble d'informations nécessaires au traitement correct de l'unité de données. Une partie de ces informations est utilisée pour construire le PCI, comme, par exemple les informations concernant l'adressage, le niveau de priorité demandé... L'autre est à l'usage exclusif de l'entité de niveau N, elle précise le traitement qui doit être opéré localement sur les données. Ces informations de contrôle de l'interface (**ICI**, *Interface Control Information*) sont annexées à la SDU pour former une unité de données de contrôle de l'interface (**IDU**, *Interface Data Unit*). L'ICI à usage exclusif de la couche N n'est pas transmis. La figure 7.7 illustre ce propos.

3. Les notations OSI utilisent, pour désigner les couches, les notations suivantes :
– (N) SDU désigne une SDU de niveau (N) générique ;
– N_SDU ou encore NSDU désigne une SDU d'un niveau particulier, ici le niveau 3 (*Network*), ces deux écritures seront indifféremment utilisées.

© Dunod – La photocopie non autorisée est un délit

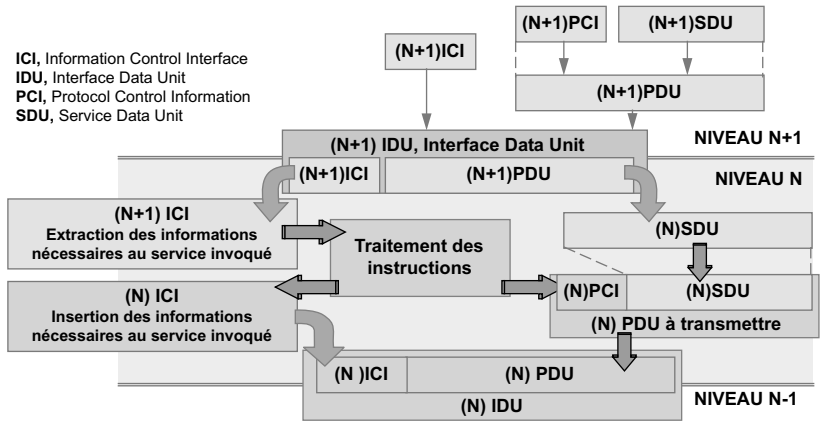


Figure 7.7 Le contrôle de l'interface.

Le protocole en mode point à point et de bout en bout

La communication entre deux systèmes peut être directe ou se réaliser à travers un ou plusieurs relais (sous-réseau réel de transport ou autre moyen d'interconnexion). Cette approche conduit à définir deux types de dialogue (figure 7.8) :

– Un dialogue entre les systèmes d'extrémité et le relais : dialogue en mode point à point.
– Un dialogue entre les systèmes d'extrémité : dialogue de bout en bout.

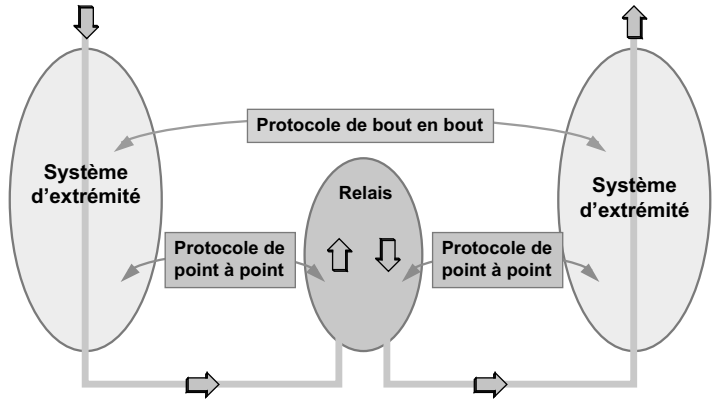


Figure 7.8 Le protocole en mode point à point ou de bout en bout.

Les protocoles de point à point assurent le transport de l'information dans le sous-réseau réel de transport, ils assurent notamment le contrôle du lien, le contrôle et éventuellement la reprise sur erreur, l'adressage et l'acheminement. Les protocoles en mode point à point peuvent être en mode orienté connexion ou en mode non connecté.

Les protocoles de bout en bout doivent essentiellement vérifier l'intégrité, au sens large, des informations remises aux applications et organiser le dialogue. Les protocoles de bout en bout sont généralement en mode orienté connexion.

7.3 L'ORGANISATION DU MODÈLE DE RÉFÉRENCE

7.3.1 Les concepts ayant conduit à la modélisation

Définition

Au sens du modèle OSI, modèle pour l'interconnexion des systèmes ouverts, on appelle système réel l'ensemble constitué d'un ou plusieurs ordinateurs, logiciels et périphériques associés capables d'effectuer des traitements informatiques et de s'échanger des informations (normes ISO IS7498, NF 27498). Un système est dit ouvert si les communications entre les divers constituants s'effectuent conformément au modèle de référence (OSI).

Les principes ayant guidé la détermination des couches

La nécessité d'identifier des fonctions élémentaires distinctes, mais participant au processus de communication, a conduit à étudier un modèle structuré en couches. La définition des différentes couches du modèle respecte les principes suivants :

– Ne pas créer plus de couches que nécessaire, pour que le travail de description et d'intégration reste simple, ce qui conduit à regrouper les fonctions similaires dans une même couche.
– Créer une couche chaque fois qu'une fonction peut être identifiée par un traitement ou une technologie particulière mise en jeu.
– Créer une couche là où un besoin d'abstraction de manipulation de données doit être distingué.

Une interface sera créée à la frontière de chaque couche. Les figures 7.9 et 7.10 illustrent le principe de la structuration du système. Chaque couche (N) fournit les services (N) aux entités (N+1) de la couche (N+1). Chaque couche échange des unités de données (*Data Unit*) avec la couche correspondante sur l'entité distante (homologue) à l'aide d'un ensemble de règles (protocole) en utilisant pour cela les services de la couche inférieure.

Couches hautes, couches basses

Deux fonctions essentielles peuvent être distinguées pour assurer l'interfonctionnement d'applications informatiques à travers un réseau (figure 7.9).

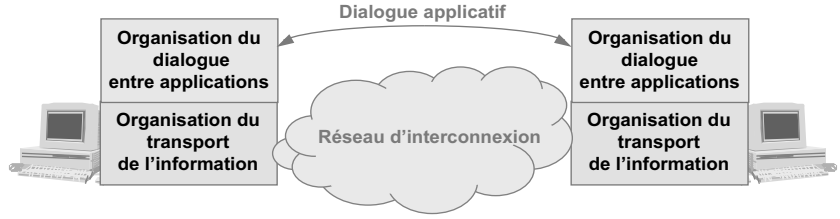


Figure 7.9 L'interfonctionnement des applications.

Il faut, d'une part garantir un transport fiable des informations à travers le réseau, et d'autre part organiser le dialogue entre les applications distantes (dialogue applicatif). Le modèle doit masquer à l'utilisateur la répartition physique des ressources et offrir les mêmes performances aux applications, que les ressources soient locales ou distantes.

© Dunod – La photocopie non autorisée est un délit

Cet aspect conduit à spécifier deux ensembles de couches aux fonctionnalités spécifiques (figure 7.10) :

– les **couches hautes** essentiellement chargées d'assurer l'interfonctionnement des processus applicatifs distants, ces couches sont dites orientées application ;
– les **couches basses** destinées à fournir aux couches hautes un service de transport fiable de données, déchargeant les couches hautes de la gestion de tous les mécanismes de localisation et de transfert d'information à travers un ou plusieurs systèmes relais, ces couches sont dites orientées transport (ou transfert).

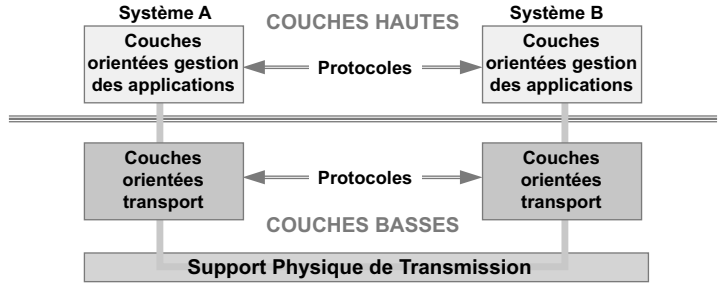


Figure 7.10 La spécification en deux ensembles de couches.

Les couches basses garantissent aux couches hautes que le transfert d'information se réalise correctement. Il est donc nécessaire que la dernière couche basse du système destinataire vérifie, avant de délivrer les données aux couches applicatives, que celles-ci sont correctes (contrôle de bout en bout). Les autres couches inférieures n'effectuent qu'un transfert de proche en proche entre systèmes. Les couches hautes n'assurent, globalement, que l'organisation des échanges et fournissent les mécanismes nécessaires à assurer l'interfonctionnement de une ou plusieurs applications distantes.

7.3.2 La description du modèle de référence

Définition des couches

Pour réaliser une communication à travers un ou plusieurs systèmes intermédiaires (relais), il faut (figure 7.11) :

– relier les systèmes par un lien physique (couche PHYSIQUE) ;
– contrôler qu'une liaison peut être correctement établie sur ce lien (couche LIAISON) ;
– assurer à travers le relais (réseau) l'acheminement des données et la délivrance au bon destinataire (couche RÉSEAU) ;
– contrôler, avant de délivrer les données à l'application que le transport s'est réalisé correctement de bout en bout (couche TRANSPORT) ;
– organiser le dialogue entre toutes les applications, en gérant des sessions d'échange (couche SESSION) ;
– traduire les données selon une syntaxe d'échange compréhensible par les deux entités d'application (couche PRÉSENTATION) ;

– fournir à l'application utilisateur tous les mécanismes nécessaires pour masquer à celle-ci les contraintes de transmission (couche APPLICATION).

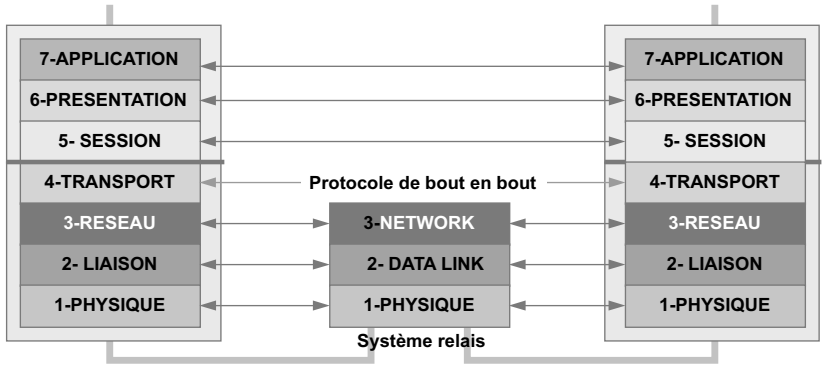


Figure 7.11 Le modèle de référence.

C'est ainsi, qu'après de nombreux débats, le modèle de référence a été défini en sept couches (compromis entre 6 et 8 !). Le modèle de référence (figure 7.11) ne définit pas seulement les fonctionnalités de chaque couche mais précise aussi la dénomination des unités de données manipulées par chacune d'elle (figure 7.13). La figure 7.12 détaille les fonctionnalités de chacune des couches composant le modèle.

COUCHES	FONCTIONS
NIVEAU 1 Couche Physique *Physical Layer*	La couche physique assure un transfert de bits sur le canal physique (support). À cet effet, elle définit les supports et les moyens d'y accéder : spécifications mécaniques (connecteur), spécifications électriques (niveau de tension), spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne. Elle détermine aussi les moyens d'adaptation (ETCD).
NIVEAU 2 Couche Liaison de données *Data Link Layer*	La couche liaison assure, sur la ligne, un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Les protocoles de niveau 2 permettent, en outre, de détecter et de corriger les erreurs inhérentes aux supports physiques.
NIVEAU 3 Couche Réseau *Network Layer*	La couche réseau assure, lors d'un transfert à travers un système relais, l'acheminement des données (paquets) à travers les différents nœuds d'un sous-réseau (routage). Les protocoles de niveau 3 fournissent les moyens d'assurer l'acheminement de l'appel, le routage, le contrôle de congestion, l'adaptation de la taille des blocs de données aux capacités du sous-réseau physique utilisé. Elle offre, en outre, un service de facturation de la prestation fournie par le sous-réseau de transport.
NIVEAU 4 Couche Transport *Transport Layer*	La couche transport est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout des informations (messages) entre les deux systèmes d'extrémité. La couche transport est la dernière couche de contrôle des informations, elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé.

Figure 7.12 Synthèse des fonctionnalités de chaque couche.

© Dunod – La photocopie non autorisée est un délit

COUCHES	FONCTIONS
NIVEAU 5 Couche Session *Session Layer*	La couche session gère l'échange de données (transaction) entre les applications distantes. La fonction essentielle de la couche session est la synchronisation des échanges et la définition de points de reprise.
NIVEAU 6 Couche Présentation *Presentation Layer*	Interface entre les couches qui assurent l'échange de données et celle qui les manipule, cette couche assure la mise en forme des données, les conversions de code nécessaires pour délivrer à la couche supérieure un message dans une syntaxe compréhensible par celle-ci. En outre, elle peut, éventuellement, réaliser des fonctions spéciales, comme la compression de données...
NIVEAU 7 Couche Application *Application Layer*	La couche application, la dernière du modèle de référence, fournit au programme utilisateur, l'application proprement dite, un ensemble de fonctions (entités d'application) permettant le déroulement correct des programmes communicants (transferts de fichiers, courrier électronique...).

Figure 7.12 Synthèse des fonctionnalités de chaque couche. (suite)

Les mécanismes élémentaires

➤ L'encapsulation

Chaque couche du modèle insère un en-tête de protocole PCI. La figure 7.13, où le symbole H*x* représente l'en-tête (*Header*) de niveau, illustre ces mécanismes.

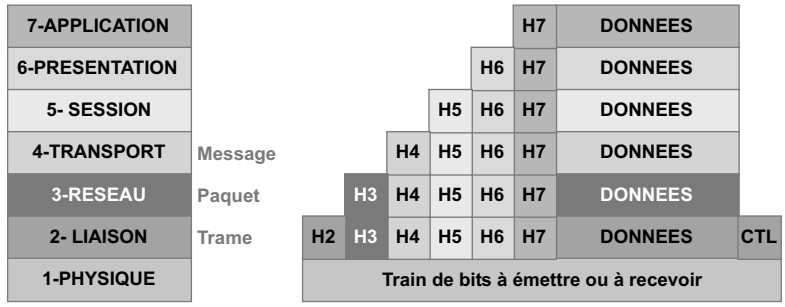


Figure 7.13 L'encapsulation des données dans le modèle OSI.

La couche liaison de données ajoute un champ supplémentaire qui contient les informations nécessaires au contrôle (CTL) de la transmission (**FCS**, *Frame Check Sequence*). Le mécanisme d'encapsulation est illustré par la figure 7.13.

➤ Primitives de service

Les services offerts par la couche (N) sont invoqués par la couche (N+1) à l'aide de primitives de service de niveau (N). Par exemple, en mode connecté (figure 7.14), quatre primitives sont utilisées pour offrir un service : demande (*Request*), indication (*Indication*), réponse (*Response*), confirmation (*Confirm*). En mode non connecté, seules les primitives demande (*Request*) et indication (*Indication*) sont exploitées.

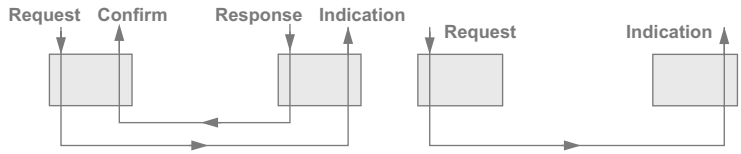


Figure 7.14 Les primitives de service.

Les mécanismes pouvant être mis en œuvre dans une couche

➤ L'adaptation de la taille des unités de données

Les unités de données, manipulées par les différentes couches ou par les systèmes intermédiaires, ne sont pas forcément de taille compatible avec les capacités de ces systèmes. Différents mécanismes d'adaptation peuvent alors être utilisés (figure 7.15).

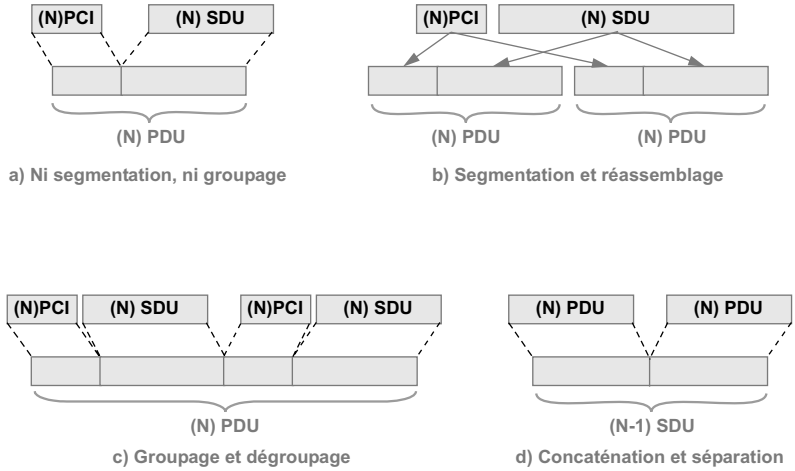


Figure 7.15 L'adaptation de la taille des unités de données.

La segmentation consiste à diviser une unité de données du service (N) en plusieurs unités de données de protocole (N). L'entité correspondante distante doit être capable d'assurer le réassemblage afin de reconstituer la SDU d'origine.

Le groupage réunit en une seule PDU de niveau (N) plusieurs unités de données de service. Chaque unité possède son propre en-tête.

La concaténation procède de la même manière, plusieurs PDU de niveau N sont associées pour former une seule SDU de niveau N–1.

➤ Le multiplexage et l'éclatement des connexions

Le multiplexage (figure 7.16) consiste pour une couche à prendre en charge plusieurs connexions de niveau (N) sur une seule connexion de niveau (N–1), alors que l'éclatement permet à la couche (N) d'utiliser plusieurs connexions (N–1).

© Dunod – La photocopie non autorisée est un délit

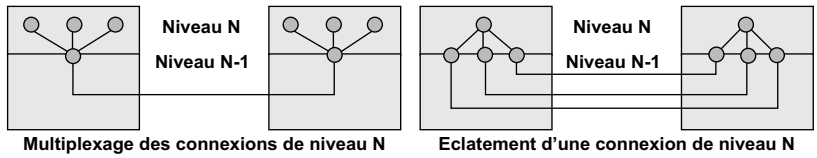


Figure 7.16 Le multiplexage et l'éclatement.

➤ Le contrôle de flux

Cette technique, déjà évoquée, assure une cadence de délivrance des données compatibles avec les capacités de traitement entre couches adjacentes (contrôle de flux à l'interface) ou entre couches homologues (contrôle de flux entre systèmes).

➤ Le maintien en séquence

Cette fonction garantit que les données remises à une couche (N) sont dans le même ordre que celles émises par la couche (N) distante. Le maintien en séquence n'est pas obligatoirement garanti par toutes les couches. La couche chargée de cette fonction doit être capable de mémoriser les données reçues hors séquence et les ordonner avant de les délivrer en séquence à la couche supérieure. La fenêtre de réception représente, en nombre d'unités de données, la capacité de mémorisation et de réordonnancement de la couche. En mode orienté connexion, le maintien en séquence est toujours garanti.

➤ L'accusé de réception

L'entité destinataire de niveau (N) rend compte à l'entité émettrice de niveau (N) de la réception correcte ou incorrecte d'une unité de protocole de niveau (N). La technique de l'accusé de réception n'est pas obligatoirement liée au mode connecté. Dans les réseaux locaux, le service dit « LLC3 » implémente un service en mode datagramme avec accusé de réception (l'accusé de réception indique que le message est arrivé et non qu'il a été traité).

➤ La réinitialisation

Les entités communicantes peuvent revenir à un état de référence, la non-perte de données et la non-duplication ne sont pas garanties.

➤ Les données exprès

Les données exprès[4] correspondent à la possibilité d'émettre de petites unités de données. Ces données ne sont pas acheminées plus rapidement par le réseau de transport, cependant elles échappent au contrôle de flux. Ces données sont délivrées, en priorité, par les entités destinatrices.

4. Attention, ISO institue essentiellement un mode connecté. Dans ces conditions, les données émises sur un lien arrivent dans l'ordre, il n'y a pas de données qui peuvent en « doubler » d'autres dans le réseau (données expresses), il s'agit ici de données délivrées à dessein (exprès) et qui seront traitées en priorité.

➤ La détection, la correction et la notification d'erreur

Les protocoles de niveau (N) peuvent utiliser des fonctions de détection d'erreur et mettre en œuvre des mécanismes de correction (reprise sur erreur). En cas d'échec de la reprise sur erreur, la couche (N) signale à la couche supérieure (N+1) une erreur non corrigée (notification d'erreur).

➤ La qualité de service

Certaines couches ont la faculté de négocier entre elles, une certaine qualité de service (**QoS**, *Quality of Service*). La qualité de service peut concerner les paramètres suivants :

– délai d'établissement de la connexion ;
– débit ;
– temps de transit et sa variation ou gigue ;
– taux d'erreur résiduelle ;
– coût...

La qualité de service est représentée, dans la demande de connexion, par deux listes, la liste des paramètres relatifs à la qualité demandée et celle relative à la qualité minimale de service acceptable. Si les valeurs minimales ne peuvent être offertes par l'un des sous-réseaux réels traversés ou par l'entité distante, la connexion est refusée.

7.4 L'ÉTUDE SUCCINCTE DES COUCHES

Nous limiterons cette étude aux fonctionnalités et particularismes essentiels de chacune des couches. Les protocoles et techniques en relation avec ces couches ont déjà fait l'objet d'étude ou le feront lors de l'étude des services qui les mettent en œuvre.

7.4.1 La couche physique

La couche physique (figure 7.17) fournit l'interface avec le support physique sur lequel elle transmet un train de bits en assurant, éventuellement, la transparence de binaire. Elle est chargée de la synchronisation entre les horloges source et destination. La couche physique ne distingue pas le mode connecté du mode sans connexion. Elle prend en charge les transmissions synchrones ou asynchrones en fonctionnement simplex, semi-duplex ou duplex que la liaison soit en mode point à point ou multipoint.

Les services fournis, à la couche liaison, sont :

– l'établissement et la libération de la connexion physique ;
– la transmission série et ou parallèle de « *n* » bits ;
– l'identification des extrémités de la connexion physique, qui peut être unique (liaison point à point) ou multiple (liaison multipoint) ;
– l'identification du circuit de données, cette identification pouvant être utilisée par les entités réseaux pour identifier une voie logique ;
– le maintien en séquence des bits émis ;
– l'horloge et la récupération d'horloge (synchronisation) ;
– la notification de dérangement.

© Dunod – La photocopie non autorisée est un délit

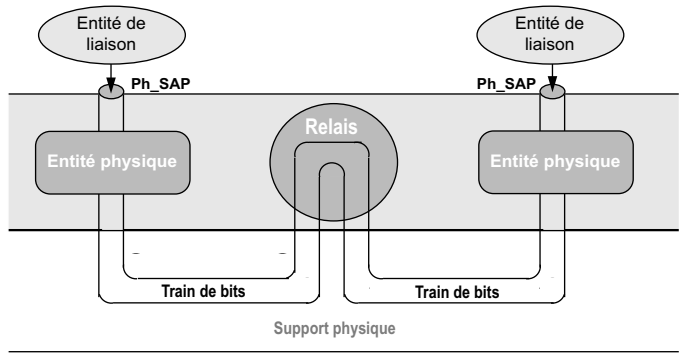


Figure 7.17 La couche physique.

La qualité de service fournie dépend essentiellement des supports utilisés, elle est caractérisée par le débit offert, le débit effectif, le taux d'erreur et la disponibilité.

Les normes couvertes par la couche physique comprennent principalement les normes relatives aux jonctions (V.24, V.35, X.21...) et aux ETCD (Modem, TNR – Terminaison numérique de réseau...).

7.4.2 La couche liaison de données

La couche liaison de données (figure 7.18) assure le contrôle logique de la liaison et le transfert de données entre entités de réseau sous forme de trame (DL_PDU). La couche liaison de données fournit un service de point à point, dit aussi en **cascade**, et éventuellement un mécanisme de détection et de correction d'erreur.

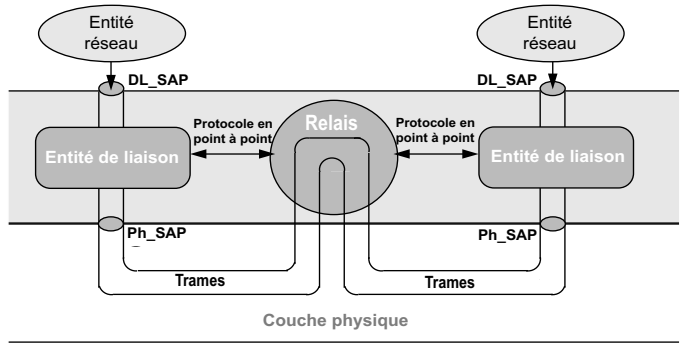


Figure 7.18 La couche liaison de données.

Les services fournis aux entités de réseau, accessibles au SAP dit **DLSAP** (*Data Link Service Access Point*), sont :

– l'établissement, le maintien et la libération de la connexion logique établie entre deux points d'accès au service de liaison de données ;
– éventuellement la fourniture d'identificateur d'extrémité ;

– la délimitation et le transfert des données (trames) en assurant :
  – le maintien en séquence,
  – la détection et la correction d'erreur,
  – la notification d'erreur non corrigée,
  – le contrôle de flux.

La qualité de service fournie s'exprime principalement par le taux d'erreurs résiduelles, ces erreurs pouvant provenir de données altérées, perdues, dupliquées ou du non-respect de l'ordonnancement des trames.

7.4.3 La couche réseau

Structure générale

La couche réseau (figure 7.19) assure un transfert de données entre deux systèmes d'extrémité à travers un ou plusieurs sous-réseaux physiques (systèmes relais). Elle fournit les fonctions de routage et garantit aux entités de transport un service réseau uniforme indépendamment des technologies utilisées dans les sous-réseaux physiques traversés. Deux fonctions essentielles en découlent :

– la localisation des systèmes (adressage),
– l'adaptation de la taille des unités de données (NPDU) aux capacités des différents sous-réseaux traversés.

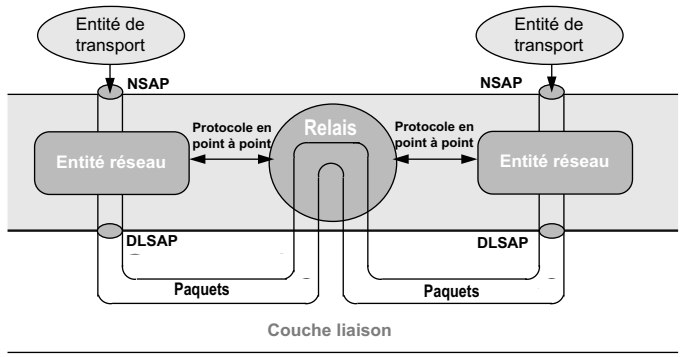


Figure 7.19 La couche réseau.

La localisation du système résout deux problèmes : l'adressage et l'acheminement (le routage). Le **NSAP** (*Network Service Access Point*) correspond à l'identification, sur les systèmes d'extrémité, de l'accès au service réseau (entités homologues) et non à la localisation du destinataire. Déduit de la NSAP adresse, le **SNPA** (*SubNetwork Point of Attachment*) est couramment appelé adresse du destinataire[5]. Le SNPA identifie le point où le système réel d'extrémité (ou l'unité

5. Dans la pratique cette distinction n'est pas faite, l'adresse NSAP et le point d'accès au réseau SNPA sont souvent confondus.

© Dunod – La photocopie non autorisée est un délit

d'interfonctionnement – relais –) est raccordé au sous-réseau réel (figure 7.20). Le terme de sous-réseau réel désigne le ou les sous-réseaux physiques de transfert, l'emploi du terme réseau est à réserver à la désignation de la couche réseau et des entités réseaux.

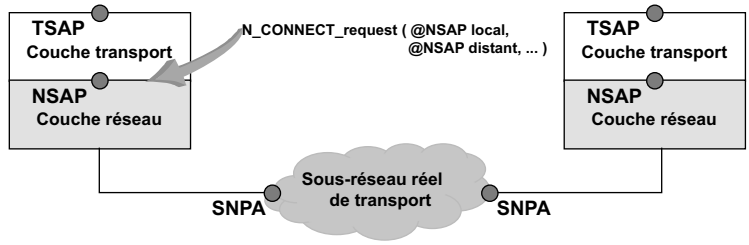


Figure 7.20 L'adressage dans la couche réseau.

L'adresse NSAP (figure 7.21) correspond à un espace d'adressage, appelé **adressage du réseau global**, subdivisé en domaines et contrôlé par une autorité d'adressage (voir chapitre 6, figure 6.16). Étudiée pour s'adapter à tous les types de réseaux, elle est déterminée à partir de la **TSAP** (*Transport Service Access Point*).

NSAP		
AFI *Autority and Format Identifier*	IDI *Initial Domain Identifier*	DSP *Domain Specific Part*
Identifie l'autorité d'adressage, le format et la syntaxe de l'adresse (chiffre de 0 à 99, ex : adressage X.121 AFI= 38).	Identifie le domaine auquel s'applique l'adresse (DSP) c'est, par exemple, le code pays.	Partie spécifique du domaine, c'est l'adresse proprement dite : le SNPA (N° Transpac, N° téléphone...).
IDP *Initial Domain Part*		

Figure 7.21 La structure de l'adressage réseau.

La traversée d'un ou plusieurs sous-réseaux nécessite l'adaptation du format et de la taille des données pour être conforme aux possibilités de chaque sous-réseau traversé. Cet impératif explique la complexité réelle de la couche réseau qui doit réaliser :

– éventuellement une conversion d'adresse ;
– l'adaptation de la taille des paquets de données ;
– l'adaptation des débits ;
– l'adaptation des modes de fonctionnement, c'est-à-dire le passage du mode connecté au mode non connecté ou inversement.

À cet effet, la couche réseau est subdivisée en trois sous-couches qui ne sont pas nécessairement toutes présentes. La couche la plus basse est chargée directement de l'accès physique au sous-réseau réel (**SNACP**, *SubNetwork ACcess Protocol*), la couche la plus haute assure les fonctions réseaux indépendamment du sous-réseau réel utilisé (**SNICP**, *SubNetwork Independant Convergence Protocol*), la couche intermédiaire est chargée d'une éventuelle adaptation (**SNDCP**, *SubNetwork Dependant Convergence Protocol*).

Pour réaliser ses objectifs la couche réseau réalise les fonctions suivantes :

– routage et service relais ;
– connexion de niveau réseau ;
– multiplexage des connexions ;
– segmentation et groupage ;
– détection d'erreur et reprise sur erreur ;
– maintien en séquence ;
– contrôle de flux ;
– transfert de données exprès ;
– réinitialisation.

Exemples d'enchaînement de primitives

➤ Établissement de connexion

L'initiative de l'établissement d'une connexion réseau appartient à la couche transport (figure 7.22). Celle-ci formule sa demande à l'aide de la primitive N_Connect.request dont les paramètres principaux sont les NSAP adresses source et destination et la qualité de service demandée (QoS). N'ayant pas de connexion au niveau liaison, la couche réseau mémorise cette requête et demande à la couche liaison d'établir une connexion de niveau 2 à l'aide de la primitive DL_Connect.request. La demande est traduite par une trame non numérotée SABM[6] ; la couche 2 distante, à réception de la trame SABM en réfère à la couche 3 (DL_Connect.ind) ; celle-ci ayant les ressources suffisantes pour accueillir une nouvelle connexion de niveau liaison accepte et le signifie à la couche 2 par la primitive DL_Connect.response.

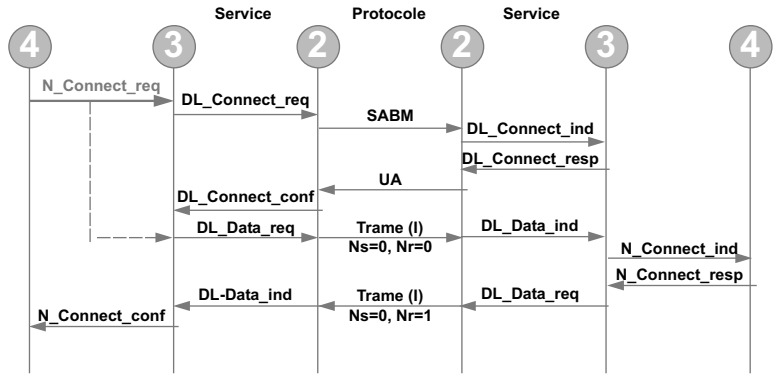


Figure 7.22 L'établissement d'une connexion réseau.

La couche liaison acquitte alors la demande de connexion par la trame (U) UA, à réception de l'UA, la couche 2 locale informe la couche 3 de cette acceptation (DL_Connect.confirm). Disposant d'une connexion de niveau 2, la couche réseau locale peut émettre la demande de connexion

6. Pour illustrer le mécanisme d'établissement de la connexion, nous utiliserons, pour le niveau liaison, les unités de données du protocole HDLC, seul protocole étudié jusqu'ici.

© Dunod – La photocopie non autorisée est un délit

réseau en attente (N_Connect.request), cette demande de connexion est transportée dans une unité de données de niveau 2 (DL_Data_.request)[7] traduite en une trame d'information. La couche 2 distante remet cette demande (DL_Data.indication) à la couche 3 distante. De même, celle-ci en réfère à la couche 4 (N_Connect.indication) qui l'autorise à accepter la connexion de niveau 3 (N_Connect.response)... Enfin, la connexion est établie (N_Connect.confirm).

➤ Échange de données

L'échange des données n'appelle aucun commentaire particulier, il est symbolisé figure 7.23.

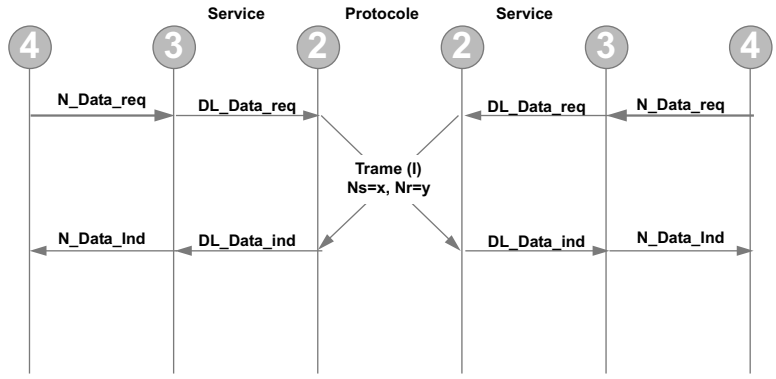


Figure 7.23 L'échange de données.

➤ Rupture de connexion

Le mécanisme de rupture de la connexion de niveau 3 est symétrique à celui de l'établissement. La connexion de niveau 3 est d'abord rompue, puis celle de niveau 2 (figure 7.24).

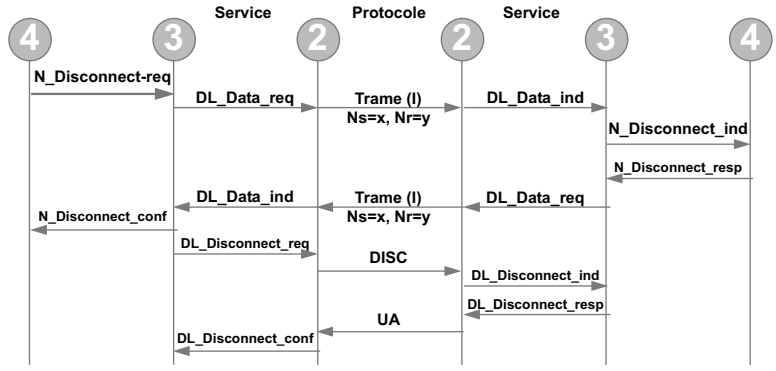


Figure 7.24 La rupture de connexion.

7. Selon le mode utilisé, il existe deux primitives de transfert de données. En mode connecté, les primitives se nomment DL_Data_.xxx, et en mode non connecté DL_Unidata.xxx. Pour faciliter la lecture du schéma, cette distinction a été volontairement omise.

7.4.4 La couche transport

Principes généraux

La couche transport (figure 7.25) garantit aux couches hautes un transfert fiable et transparent des données, en masquant, à celles-ci, les détails d'exécution de ce service. C'est-à-dire qu'elle fournit, aux entités de session, un service de transfert fiable de bout en bout quel que soit le sous-réseau utilisé disponible au point d'accès au service : le TSAP (*Transport Service Access Point*). La couche transport effectue, éventuellement, une remise en séquence des unités de données reçues, si ce service n'est pas garanti par les couches inférieures.

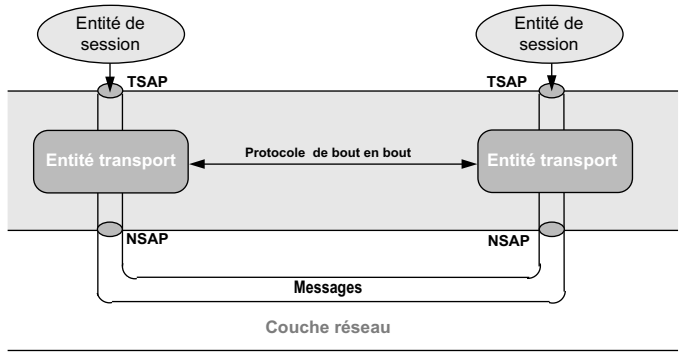


Figure 7.25 La couche transport.

La complexité du protocole de transport est directement liée à la qualité du service réseau utilisé. Les sous-réseaux sont classés en trois types (A, B et C) en fonction de deux grandeurs (figure 7.26) :

– le taux d'erreur signalée, les erreurs signalées sont des erreurs détectées par la couche réseau mais non corrigées par celle-ci ;
– le taux d'erreur résiduelle correspond aux erreurs non détectées et par conséquent non signalées.

Type Réseau	Taux d'erreur résiduelle	Taux d'erreur signalée	Qualité de service
A	Acceptable	Acceptable	Bonne
B	Acceptable	Inacceptable	Moyenne
C	Inacceptable	Inacceptable	Mauvaise

Figure 7.26 La classification des réseaux selon l'ISO.

Les différentes fonctions de la couche transport visent à améliorer la qualité du service offert par le sous-réseau sous-jacent. Les protocoles de transport sont répartis en 5 classes (classe 0 ou TP0, classe 1 ou TP1 ... classe 4 ou TP4). La classe 0 est la classe de base, elle offre un service minimum, les autres en sont issues par enrichissement successif (figure 7.27).

La figure 7.28 fournit la correspondance entre les différents types de réseau et la classe de transport préconisée.

© Dunod – La photocopie non autorisée est un délit

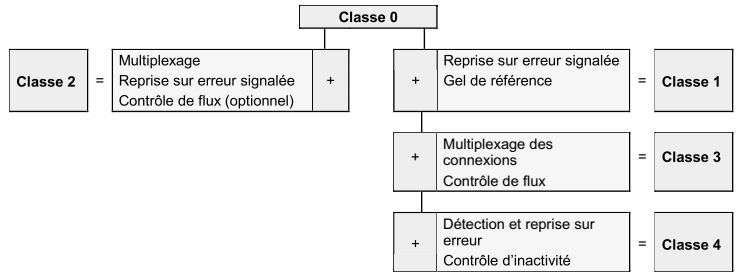


Figure 7.27 Les classes de transport.

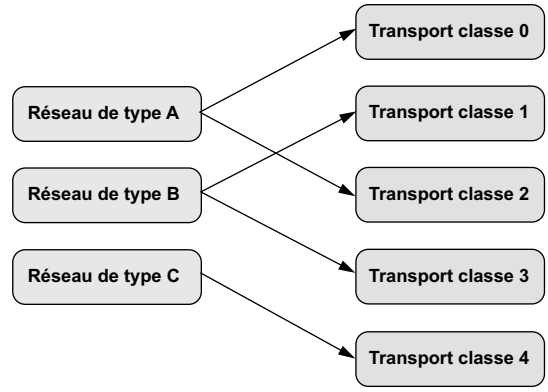


Figure 7.28 Correspondance type réseau et classe transport.

La classe de transport à employer dépend de la qualité de service offert par les sous-réseaux de transport utilisés. Lors d'une connexion, plusieurs sous-réseaux peuvent être traversés, les hôtes n'ont, en principe, que la connaissance de leur sous-réseau de rattachement. De ce fait, lors de la connexion de transport, la classe de transport employée est l'un des paramètres négociés. La demande de connexion de transport propose une classe préférentielle et, éventuellement, une classe de substitution acceptable. L'entité homologue accepte la classe préférentielle ou celle de substitution, sinon elle propose une classe inférieure de repli. L'appelant peut accepter cette classe de repli ou refuser la connexion.

Les mécanismes de la couche transport

Les mécanismes mis en œuvre par les protocoles de transport sont nombreux, quelques-uns sont spécifiques, ils sont détaillés ci-dessous :

- La **résolution de l'adresse de transport**, la localisation de l'entité distante, sur laquelle le système local doit se connecter, est déduite de l'adresse de transport destination (TSAP). Plusieurs cas sont envisageables :
  - le système local connaît la TSAP distante, il émet une demande de connexion à l'adresse de celle-ci ;
  - le système local ne connaît pas la TSAP distante, il peut, dans ce cas, par exemple, se connecter à un service d'annuaire local ou distant qui lui indiquera la TSAP désirée.

- Le **référencement des connexions** de transport, plusieurs connexions de transport peuvent aboutir à une même TSAP. Pour identifier les flux de données de provenances différentes, l'entité de transport attribue à chaque flux un identifiant, sur 2 octets, appelé **référence de transport** (référence source et référence destination). En mode connecté, seule la requête de connexion T_Connect.request transporte, dans la partie option de la TPDU, l'adresse de transport : TSAP. Dans les autres primitives, la connexion est identifiée par les références source et destination. En mode non connecté (**UD**, *User Datagramme*) et en classe 0 (pas de notion de multiplexage) l'adresse TSAP est toujours présente et le champ référence absent (UD) ou non renseigné (classe 0).
- Le **gel de référence**, lors de la libération d'une connexion, les références de celle-ci ne peuvent être réutilisées par une nouvelle connexion pendant un certain temps. Cette technique interdit qu'une nouvelle connexion ne soit établie avec les mêmes références et ne reçoive alors des données, appartenant à la connexion précédente retardées dans le sous-réseau de transport.
- La **libération implicite ou explicite**, la libération est dite implicite lorsque sa vie est liée à celle de la connexion réseau, elle est réalisée en même temps que celle-ci ; elle est dite explicite quand sa vie est indépendante de celle de la couche réseau.
- La **détection et la correction d'erreur**, (optionnel et en classe 4 uniquement), un total de contrôle est calculé tel que la somme modulo 255 des octets de la TPDU soit nulle.
- Le **contrôle d'inactivité**, (classe 4 uniquement), une horloge d'inactivité (*Timer*) est gérée par l'entité de transport, cette horloge est réinitialisée à chaque réception de TPDU. À l'échéance du timer, la connexion transport est libérée. Ce mécanisme pallie les libérations de connexion non signalées. Pour éviter, lors de longs silences, une rupture de connexion sur détection d'inactivité, les entités de transport peuvent acquitter les messages (ACK).
- La **segmentation**, lorsqu'une TSDU est plus grande que la taille des TPDU autorisée sur le réseau et déterminée à la connexion, celle-ci est segmentée.
- Le **contrôle de flux**, la couche transport utilise un mécanisme dit de contrôle de flux explicite. Le récepteur, en fonction de son état, accorde un crédit à l'émetteur. Le crédit indique, à l'émetteur, le nombre de TPDU que celui-ci est autorisé à émettre.
- **L'établissement de la connexion en trois temps** (*Three ways handshake*), si la demande de connexion est acceptée par le destinataire celui-ci émet, à destination de l'appelant, une TPDU CC (Connect.confirm). Si le service réseau est un service fiable, la connexion est alors établie et l'échange de données peut débuter (figure 7.29). Si le service réseau est non fiable, un incident quelconque peut survenir et la CC (TPDU Conect.confirm) peut ne jamais être reçue. Dans ces conditions, l'appelé attend des données qui ne lui parviendront jamais, le système est bloqué (*Deadlock*).
  Pour éviter cette situation, un *timer* d'inactivité libère la connexion. En classe 4, la connexion ne sera effectivement établie qu'à réception, par l'appelé, d'un accusé de réception de son acceptation (ACK), la validation est dite en trois phases (figure 7.29). La TPDU de demande de connexion (CR) peut transporter un message de 32 octets, ce message peut, par exemple, contenir un mot de passe.
- La **déconnexion**, le mécanisme de déconnexion est identique à celui de la connexion, il peut survenir à n'importe quel moment (déconnexion brutale ou non négociée). De ce fait, des données retardées dans le sous-réseau peuvent être perdues. L'éventuelle perte de données, due à une déconnexion brutale est, en fait, traitée par la couche session.

© Dunod – La photocopie non autorisée est un délit

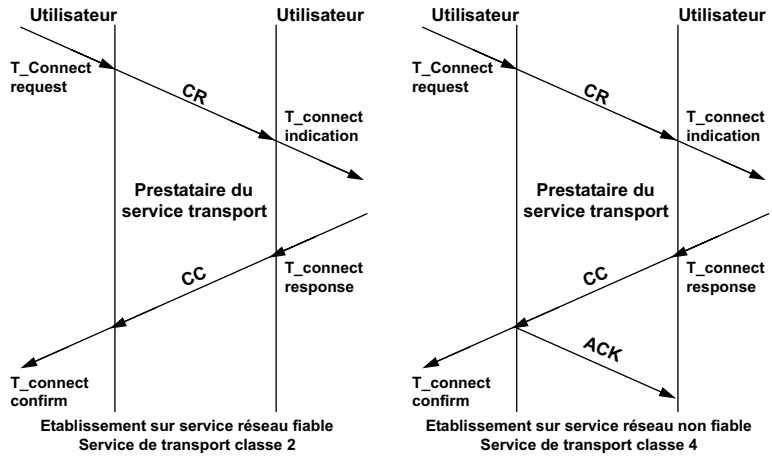


Figure 7.29 Établissement de la connexion de transport.

La figure 7.30 résume les principales fonctions mises en œuvre dans les différentes classes de transport.

Mécanismes mis en œuvre par les protocoles de transport.	Classes				
	0	1	2	3	4
Affectation à une connexion réseau	•	•	•	•	•
Établissement de connexion	•	•	•	•	•
Refus de connexion	•	•	•	•	•
Traitement des erreurs de protocole	•	•	•	•	•
Libération sur erreur	•		•		
Resynchronisation		•		•	•
Multiplexage et démultiplexage			•	•	•
Contrôle de flux (A avec, S sans) ***de bout en bout***	S	S	AS	A	A
Libération normale (I implicite, E explicite)	I	E	E	E	E
Numérotation des TPDU (S sans, N normale, E étendue)	S	N	NE	NE	NE
Gel de référence		•		•	•
Segmentation et réassemblage	•	•	•	•	•
Concaténation et séparation		•	•	•	•
Remise en séquence					•
Total de contrôle optionnel (***détection d'erreur de bout en bout***)					•
Retransmission après temporisation					•
Éclatement et recombinaison					•
Détection d'inactivité					•

Figure 7.30 Synthèse des différents mécanismes de la couche transport.

Le protocole de transport sans connexion

Le protocole de transport, en mode connecté, est lourd à mettre en œuvre, un additif à la norme (ISO 7498) spécifie un protocole en mode non connecté. Les fonctions assurées sont réduites : mise en correspondance de l'adresse de transport et de l'adresse réseau (NSAP), délimitation des blocs de données (TPDU), détection d'erreur et choix du service réseau le mieux adapté.

Si au service de transport en mode non connecté est associé un service réseau, lui aussi en mode non connecté, aucune garantie de remise ni de séquencement n'est assurée à la couche session. Les unités de données ne sont pas acquittées, un total de contrôle optionnel peut être utilisé.

7.4.5 La couche session

La couche session est l'interface entre le processus d'application et le service de transfert de données (connexion de transport). Elle assure au processus d'application[8] les moyens de contrôler le dialogue en organisant celui-ci et en autorisant les reprises (resynchronisation).

La gestion du dialogue et la synchronisation sont assurées par l'intermédiaire de quatre jetons :

- le jeton de données qui contrôle l'accès au transfert de données lors d'un échange à l'alternat ;
- le jeton de terminaison qui autorise le détenteur à demander une libération normale de la connexion de session ;
- le jeton de synchronisation mineure (**mi**) qui permet la pose d'un point de synchronisation mineure ;
- le jeton de synchronisation majeure (**MA**) et d'activité qui autorise la pose d'un point de synchronisation majeure ou qui délimite le début et la fin d'une activité.

Un jeton est disponible ou indisponible. S'il est indisponible, aucun utilisateur ne peut bénéficier des services qui lui sont associés. L'entité qui ne possède pas le jeton peut le demander (*Please Token*), celle qui le possède peut le lui concéder (*Give Token*) ou ignorer la demande. Dans le cadre d'un dialogue en *full duplex*, aucune entité n'a l'usage exclusif du jeton.

La structuration du dialogue est garantie par la pose de points de synchronisation. Un point de synchronisation permet d'identifier des instants significatifs de l'échange. Il est posé sous la responsabilité du processus d'application (services reflétés), son identification est à la charge de la couche session.

Une connexion de session est découpée en activités (figure 7.31). Une activité correspond à un transfert autonome de données, par exemple le transfert d'un fichier. Une session peut comporter une ou plusieurs activités, de même une activité peut être couverte par plusieurs sessions. Une activité est découpée en unités de dialogue, elles-mêmes séparées par des points de synchronisation majeure. La pose d'un point de synchronisation majeure suppose que toutes les données précédemment transmises sont correctes. Lorsqu'une activité est interrompue (coupure réseau) ou en cas d'erreur de transmission, il est possible de reprendre le transfert à partir d'un point de synchronisation (resynchronisation). À l'intérieur d'une unité de dialogue, il est toujours possible de revenir et de resynchroniser le dialogue sur un point de synchronisation mineure appartenant à l'unité de

8. Les services de la couche session sont dits réfléchis ; la couche présentation est transparente en ce qui concerne l'organisation du dialogue, celui-ci est directement contrôlé par la couche application (voir couche application § 7.4.7).

© Dunod – La photocopie non autorisée est un délit

dialogue en cours et ce, jusqu'au dernier point de synchronisation majeure posé. Le début et la fin d'une activité correspondent à des points de synchronisation majeure implicite.

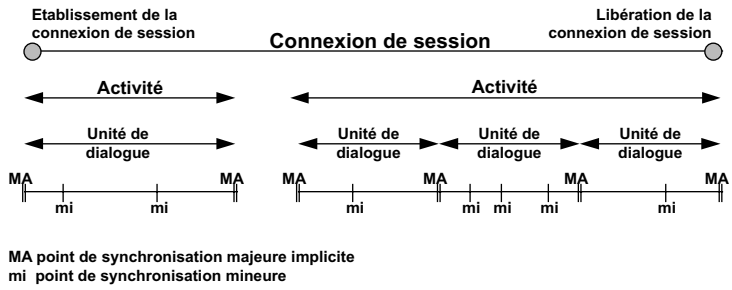


Figure 7.31 Activité, dialogue, points de synchronisation.

7.4.6 La couche présentation

Fonctionnalités

La couche présentation (figure 7.32) est la première couche non impliquée dans les mécanismes de transfert d'information. Son rôle essentiel consiste à garantir la signification des données transférées, indépendamment de la représentation interne de celles-ci, du codage utilisé (ASCII, EBCDIC...), de la longueur des mots machines (32, 64 bits...), de la représentation des valeurs négatives (complément à 1 ou à 2) dans les hôtes communicants.

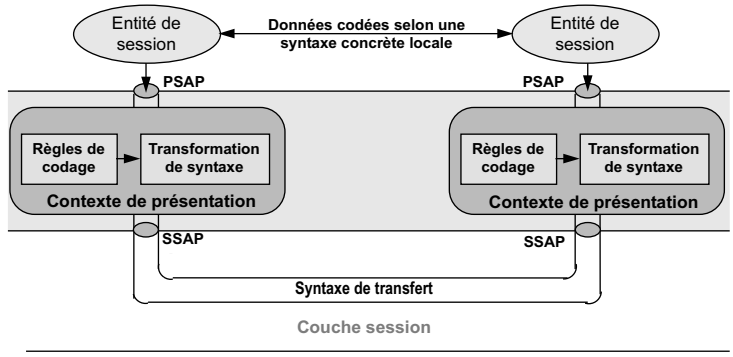


Figure 7.32 La couche présentation.

La couche présentation garantit à la couche application :

– l'accès aux services de la couche session, la plupart des primitives de service de présentation ne font que traverser la couche présentation, elles ont une correspondance directe avec les primitives de service de la couche session (services réfléchis) ; ainsi, par exemple, l'invocation, par la couche application, de la primitive de service P_TOKEN_PLEASE.request se limite à appeler la primitive S_TOKEN_PLEASE.request ;
– les services de cryptographie et de compression de données ;

– la négociation d'une syntaxe de transfert (contexte de présentation) lors de l'établissement de la connexion de présentation.

Notions de syntaxe concrète, abstraite et de transfert

Les données manipulées par l'application sont formatées selon une certaine structure dite **structure de données** (*Record* ou enregistrement). La signification des données dépend de l'application utilisateur, la valeur qui leur est assignée est liée à la représentation interne des nombres dans la machine. Ces données sont codées selon une syntaxe concrète locale directement fonction du contexte (processus applicatif utilisateur, machine cible...). Afin de garantir l'interprétation identique des données entre entités d'application distantes, celles-ci négocient une représentation commune des données, c'est la **syntaxe de transfert**.

La syntaxe de transfert (figure 7.33) est obtenue par transformation (codage) de la syntaxe concrète locale à l'aide de règles de codage, les données étant présentées selon une syntaxe indépendante du contexte, c'est la syntaxe abstraite[9].

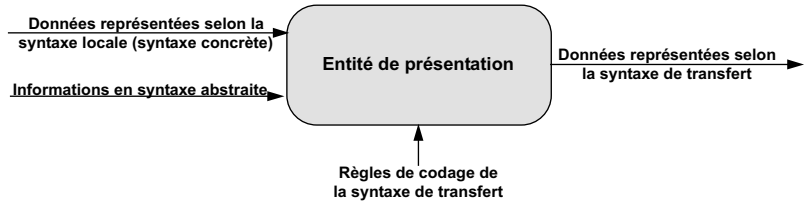


Figure 7.33 Principe d'élaboration d'une syntaxe de transfert.

L'ISO a défini une notation pour spécifier une syntaxe abstraite des données : la notation de syntaxe abstraite N°1 (**ASN-1** ou ISO 8824 *Abstract Syntax Notation 1*). ASN-1 fournit :

– une méthode pour décrire (syntaxe) les données échangées indépendamment des processeurs et systèmes d'exploitation ;
– un ensemble de types de données de base (types simples ou primitifs) pouvant être employés pour en construire d'autres (types construits) ;
– un ensemble de règles de construction de ces types et les opérateurs associés.

La figure 7.34 donne en exemple quelques types de données.

➤ Exemple

La structure représentative de l'identité d'un individu pourrait être codée :

```
Individu  ::= SEQUENCE {
          Nom             OCTET STRING,   -- 20
          prenom          OCTET STRING,   --20
          age             INTEGER,
          sexemasculin    BOOLEAN
          }
L'expression --20 est un commentaire qui indique la longueur de la chaîne.
```

9. On parle également de « langue pivot ».

© Dunod – La photocopie non autorisée est un délit

ID	Types Primitifs	Signification
2	INTEGER	Entier de taille arbitraire, utilisable pour définir des types énumérés.
1	BOOLEAN	Valeur alternative : False ou True.
3	BIT STRING	Liste de 0 ou de bits en binaire pur
4	OCTET STRING	Liste d'octets
5	NULL	Définit un objet sans type, n'est pas transmis.
6	OBJET IDENTIFIER	Permet d'identifier, par une chaîne de caractères, un objet dans un protocole.
	Types Constructeurs	
16	SEQUENCE	Autorise la construction de types complexes (similaire au *record* du langage Pascal).
16	SEQUENCE OF	Définit un tableau de valeurs d'un même type.
17	SET	Représente un ensemble non ordonné d'objets de type quelconque.
17	SET OF	Ensemble d'objets de même type.

Figure 7.34 Exemple de types de données.

À chaque type est associée une étiquette (ID) qui permet d'identifier la nature de la donnée transmise. La chaîne de caractères « BONJOUR » (ID 4, voir figure 7.34) sera transmise selon le codage de la figure 7.35, ce qui correspond à la syntaxe de transfert.

Type	Longueur	Valeur
4	7	BONJOUR
ou en hexadécimal		
4	7	42 4F 78 74 4F 85 82

Type (4) Chaîne de caractères — est représentative de la syntaxe abstraite ;
Valeur BONJOUR — est la valeur codée en ASCII, c'est la syntaxe concrète ;
Codage 04 07 42 4F 78 74 4F 85 82 — est la valeur transmise, c'est la syntaxe de transfert.

Figure 7.35 Exemple de syntaxes.

7.4.7 La couche application

Structure générale

La couche application est la dernière couche et la plus abstraite du modèle OSI, ses utilisateurs ne sont pas des entités d'une couche supérieure mais l'application utilisateur proprement dite (**AP**, *Application Process* ou **UAP,** *User Application Process*). Elle a pour objet de fournir tous les mécanismes nécessaires au fonctionnement des programmes utilisateurs situés sur des machines distinctes et interconnectées.

Ces mécanismes sont réunis en ensembles homogènes de fonctions rendant un service défini (**ASE**, *Application Service Element*). Un ASE est un service normalisé communiquant avec l'ASE homologue distant par un protocole normalisé[10]. Les différents services offerts par les ASE sont

10. Ce qui a fait dire à certains que la couche application était constituée d'un ensemble de sous-couches, cette vision est erronée.

accessibles à l'applicatif utilisateur *via* une interface (**UE**, *User Element*). Cette interface se présente comme un ensemble de librairies de procédures et de fonctions constituant des appels normalisés aux ASE.

Attention, un processus d'application constitue un tout homogène, la séparation entre l'application utilisateur et la couche application n'est que conceptuelle. Dans ces conditions, la structure générale de la couche application peut être représentée comme l'indique la figure 7.36.

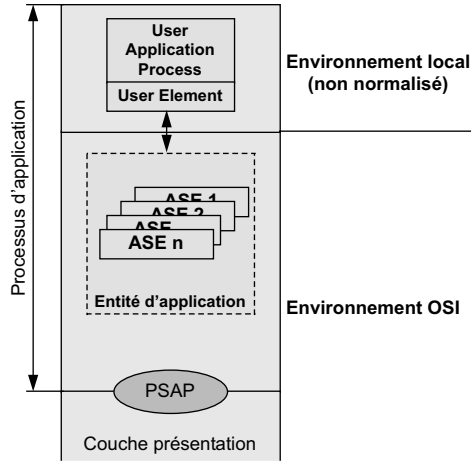


Figure 7.36 Structure générale de la couche application.

Les ASE

Les ASE peuvent offrir des services banalisés couramment utilisés par toutes les applications, ce sont les **ASE de base**. Lorsque les ASE sont dédiés à des tâches spécifiques ils sont dits **ASE fonctionnels**[11].

➤ Les ASE de base

ACSE (*Association Control Service Element*), ISO 8649 et 8650 CCITT X.217 et X.227, cet ASE appartenant à toute association gère la connexion (l'association), il assure l'établissement, le maintien, la libération ou l'abandon d'une association.

CCRSE (*Commitment, Concurency and Recovery Service Element,* engagement, concurrence et reprise), ISO 9804 et 9805, garantit l'intégrité des transactions, il est utilisé chaque fois que les applications exigent un certain niveau de sécurité, par exemple l'intégrité d'un système de bases de données réparties. CCRSE assure la cohérence globale des transactions en définissant une action atomique. Une action atomique comprend un nombre de tâches qui doivent toutes être réalisées ou pas du tout. En cas de défaillance, le système est rétabli dans son état d'origine. Il permet la mise en

11. La distinction ASE fonctionnels et ASE de base est préférable à celle d'éléments de service d'application spécifique (SASE, *Specific Application Service Element*) pour les ASE fonctionnels et d'éléments de service d'application commun (CASE, *Common Application Service Element*) pour les ASE de base.

© Dunod – La photocopie non autorisée est un délit

place des éléments protocolaires associés au protocole de validation à 2 phases utilisé pour rendre une opération atomique.

RTSE (*Reliable Transfer Service Element*), ISO 9066, CCITT X.218 et X.228, initialement prévu pour le transfert de documents dans la messagerie X.400, RTSE est devenu un service de base. Il offre un service fiable de transport de données en assurant les reprises en cas de défaillance d'un des systèmes d'extrémité.

ROSE (*Remote Operation Service Element*), ISO 9072, CCITT X.219 et X.229, cet ASE comprend un ensemble de fonctions supportant les opérations interactives. ROSE est notamment utilisé dans le modèle client/serveur.

➤ Les principaux ASE fonctionnels

MHS (*Message Handling System*, système de messagerie), ISO 10021, CCITT X.400/MOTIS, implémente un service de messagerie en mode non connecté. En cas d'absence du destinataire, le message est délivré dans sa boîte aux lettres. X.400 offre les services de création, envoi, réception et stockage de messages.

DS (*Directory Service*), ISO 9594, CCITT X.500, offre un service d'annuaire, c'est une base de données permettant la localisation géographique (adresse) des équipements adressables connectés au réseau. La norme prévoit un seul annuaire mondial, en fait, il s'agit de réaliser un ensemble d'annuaires locaux coopérants. Les éléments sont adressés selon une organisation hiérarchique ou en arbre (**DIT**, *Directory Information Tree*). X.500 assure la correspondance entre un nom mnémonique et une adresse physique.

FTAM (*File Transfer, Access and Management*), ISO 8571, assure les opérations d'accès, de transfert et de gestion de fichiers distants. FTAM travaille sur des fichiers virtuels ou documents, c'est le système d'exploitation qui manipule les fichiers physiques. Trois types génériques de fichiers sont décrits dans FTAM :

- Les fichiers non structurés, dans ce type de fichiers, les applications ne connaissent pas la structure de ceux-ci, seules les opérations de lecture et d'écriture portant sur l'intégralité du fichier sont admises.
- Les fichiers structurés, constitués d'une suite d'enregistrements éventuellement associés à une clé. Il est possible d'accéder à un enregistrement spécifique, séquentiellement ou à l'aide de la clé associée. Toutes les opérations sur les fichiers sont autorisées : lecture, écriture, modification suppression ou ajout d'enregistrement.
- Les fichiers hiérarchisés, modèle plus général, ce type de fichier peut être représenté par un arbre, à chaque nœud est associée une clé.

DTP (*Distributed Transaction Processing*), ISO 10026, est spécialement dédié à la gestion de transactions s'exécutant sur des terminaux répartis. DTP utilise la notion de transaction atomique afin de garantir l'intégrité des données (fichiers cohérents).

VT (*Virtual Terminal*), ISO 9040 et 9041, définit un terminal virtuel (nombre de lignes, nombre de caractères par ligne, attributs de caractère, fontes...). Il assure la correspondance entre les caractéristiques du terminal virtuel et le terminal du système physique réel. VT gère les différents types de terminaux :

- terminal en mode défilement ou rouleau ;
- terminal en mode page ;

– terminal en mode masque d'écran et données ;
– terminal graphique simple ou multifenêtre.

ODA (*Office Document Architecture*), ISO 8613, CCITT T.400, normalise une architecture de documents, et concerne le traitement de textes. ODA spécifie une structure générale de document comprenant :

– Le profil du document, ensemble d'informations caractérisant un document (titre, objet, date de création, dernière mise à jour, auteur...).
– La structure logique, qui structure le document en chapitres, sections, paragraphes, table des matières, références...
– La structure physique, qui décrit le document pour en assurer la reconstitution (fontes de caractère, nombre de colonnes...), elle est en correspondance directe avec la structure logique.

ODA reconnaît les textes en mode caractère (T.416), les dessins en mode point (T.417), les dessins en mode vectoriel (T.418). Le format d'échange des documents est défini par **ODIF** (*Office Document Interchange Format*).

JTM (*Job Transfer and Manipulation*) a pour objet la manipulation de documents (ensemble de fichiers dans le monde ISO). JTM distingue l'initiateur, processus ou utilisateur qui soumet le travail, la source ou système de gestion de fichiers, le puits ou destinataire des fichiers et l'exécuteur, la (ou les) machine(s), qui effectue les travaux.

RDA (*Remote Databade Access*) définit un modèle d'accès aux bases de données en proposant un modèle général : le modèle client/serveur.

7.4.8 Devenir du modèle OSI

Au début des années 80, le modèle OSI a suscité de grands espoirs. La plupart des constructeurs avaient entrepris des travaux de migration de leur architecture propriétaire vers l'architecture OSI. Mais devant la lenteur des travaux de normalisation, la complexité des solutions adoptées et la non-conformité aux exigences des nouvelles applications, le modèle de référence n'a jamais fait l'objet de véritables implémentations complètes. Cependant, le modèle OSI, en structurant les fonctions, décrit tous les concepts et les mécanismes nécessaires au développement d'une architecture de communication ; il demeure et restera une référence pour les autres architectures et un parfait modèle pédagogique.

Le modèle de référence et le temps réel

➤ Définitions

On a l'habitude de désigner par temps réel les applications où l'opérateur est en relation directe avec le système dont il attend une réponse. Ces applications doivent être appelées : applications interactives (réservation, consultation de bases de données...). Dans ce type d'application, il n'y a pas de contrainte réelle de temps. Il faut réserver la dénomination « temps réel » aux systèmes qui, non seulement, sont soumis à des contraintes temporelles sévères mais où les événements doivent être datés. Dans ces systèmes, l'information a une durée de vie limitée. Même si l'information est syntaxiquement exacte, sa signification peut être erronée ; c'est, par exemple, le cas de la transmission d'une information horaire, si celle-ci est précise au centième de seconde, la durée de validité

© Dunod – La photocopie non autorisée est un délit

de l'information transmise n'excède pas le centième de seconde. Il ne faut pas confondre non plus temps réel et transfert isochrone, un transfert isochrone est un transfert dont la cadence de réception des messages ne souffre pas de décalage temporel entre eux, le temps de transmission pouvant être indifférent.

Ces applications se rencontrent surtout dans les processus industriels (gestion d'un mobile, acquisition de données d'état...) et dans les systèmes d'arme (conduite de tir).

➤ L'incompatibilité temps réel et modèle OSI

Le modèle OSI définit des niveaux fonctionnels qui fournissent chacun un service spécifique. OSI résout les problèmes d'interconnexion d'équipements hétérogènes, mais ne prend pas en compte le critère temps.

Dans la pratique, le traitement des données correspond à une suite de procédures dont l'enchaînement peut être matérialisé, à la frontière de chaque couche, par une file d'attente. Cette approche est incompatible avec la prise en compte des contraintes temporelles imposées par le temps réel. Cette remarque est valable pour toutes les architectures en couches. La prise en compte des applications dites temps réel impose l'implémentation de mécanismes particuliers de contrôle des échanges.

Le modèle de référence et les hauts débits

La structure complexe du modèle de référence et les traitements qu'elle induit ne permettent pas aux protocoles conformes au modèle OSI d'évoluer vers des débits élevés. Les principaux handicaps proviennent essentiellement de la redondance des traitements d'une couche à l'autre, des mécanismes de reprises sur erreur et de la signalisation dans la bande qui conduit à des en-têtes variables (PCI) dont l'analyse pénalise les performances des différents relais.

C'est lors de la description de l'architecture du **RNIS-BE** (Réseau numérique à intégration de services bande étroite ou **ISDN**, *Integrated Service Data Network*) que le modèle de référence a montré ses insuffisances. En effet, ce dernier organise et contrôle l'interfonctionnement d'applications informatiques alors que le RNIS ne se préoccupe que du transport de bout en bout de données multimédias. Tandis que le modèle OSI suppose que les données de gestion et de contrôle sont transportées de la même façon que les données usagers (signalisation dans la bande), le RNIS transporte celles-ci de manière indépendante (signalisation par canal sémaphore).

Le modèle de l'IUT, défini pour RNIS-BE, a été repris pour le RNIS-LB (RNIS Large Bande). Ce modèle (recommandation I.321) comporte quatre couches dites couches de communication (figure 7.37) regroupant trois plans indépendants les uns des autres : le plan usager, le plan de commande et le plan de gestion.

Le plan usager (*User Plane*) a en charge le transfert des informations utilisateurs, le contrôle d'erreur et le contrôle de flux. Le plan de commande (*Control plane*) comporte tous les mécanismes de signalisation nécessaires à l'établissement, au maintien et à la libération de la connexion. Le plan de gestion (*Management plane*) assure la gestion des performances, la localisation des défaillances (*fault*), la détection des pannes et la mise en œuvre des mécanismes de protection du système (reconfiguration...) ; il utilise un flux de cellules spécifiques (**OAM *cells***, *Operation And Maintenance cells*). Contrairement aux données de gestion qui utilisent un canal spécifique (canal sémaphore), les cellules OAM sont multiplexées avec toutes les autres données transportées par le système.

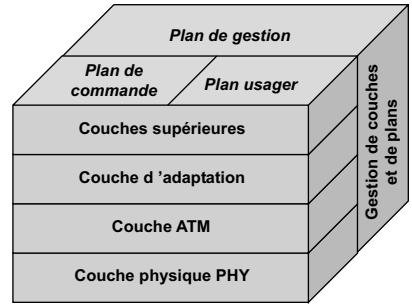


Figure 7.37 Le modèle de l'UIT.

Une autre particularité de ce modèle est d'avoir introduit une couche d'adaptation (**AAL**, *Adaptation ATM Layer*), interface entre le transport de données (couche ATM) et les applications. La couche AAL met en œuvre des mécanismes spécifiques à chaque type de données transportées autorisant ainsi, dans le réseau, le transport banalisé des données.

7.5 LES ARCHITECTURES CONSTRUCTEURS

7.5.1 L'architecture physique d'un système de téléinformatique

Les besoins croissants en terminaux connectés ont conduit les constructeurs à définir, bien avant l'avènement du modèle OSI, une architecture physique type autour de leur calculateur (*Mainframe*, hôte ou *Host*). Afin, de décharger l'hôte de la gestion des télécommunications, un ordinateur périphérique ou frontal de communication a pris en charge la gestion générale du réseau et des terminaux. De manière similaire et afin d'optimiser l'utilisation des liens, des équipements de concentration (contrôleur de grappe de terminaux) ont été utilisés (figure 7.38).

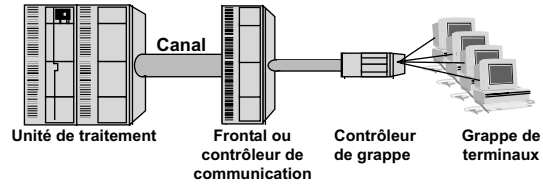


Figure 7.38 Structure d'un système informatique.

Le contrôleur de communication (frontal) gère l'ensemble des moyens logiciels et physiques (terminaux isolés, grappes de terminaux *via* des concentrateurs, liaisons privées ou publiques). La figure 7.38 illustre le concept d'architecture physique des systèmes propriétaires autour d'un *mainframe*.

7.5.2 L'origine des architectures constructeurs

La normalisation succède à un état de fait, aussi le modèle OSI n'est apparu que parce que l'interconnexion d'équipements hétérogènes était devenue complexe par la diversité des problèmes à

© Dunod – La photocopie non autorisée est un délit

résoudre. En effet, les constructeurs n'avaient pas attendu les travaux de l'ISO pour définir l'environnement d'interconnexion de leurs équipements. Ces environnements (ou architectures propriétaires) sont nés dans les années 1970 (IBM avec SNA en 1975, BULL avec DSA en 1979, DEC avec DNA).

La figure 7.39 représente les principales architectures propriétaires. Elles ont en commun une structuration en couches mais les approches peuvent être totalement différentes. Par exemple, OSI est orienté service alors que SNA est orienté fonction. Globalement, tous les services à offrir sont fournis dans les architectures propriétaires mais ils ne sont pas obligatoirement localisés dans une couche en correspondance directe avec le modèle OSI et peuvent, éventuellement, être éclatés en plusieurs couches ; c'est, par exemple, le cas de la session OSI qui recouvre approximativement la couche contrôle de flux et contrôle de transmission de l'architecture SNA.

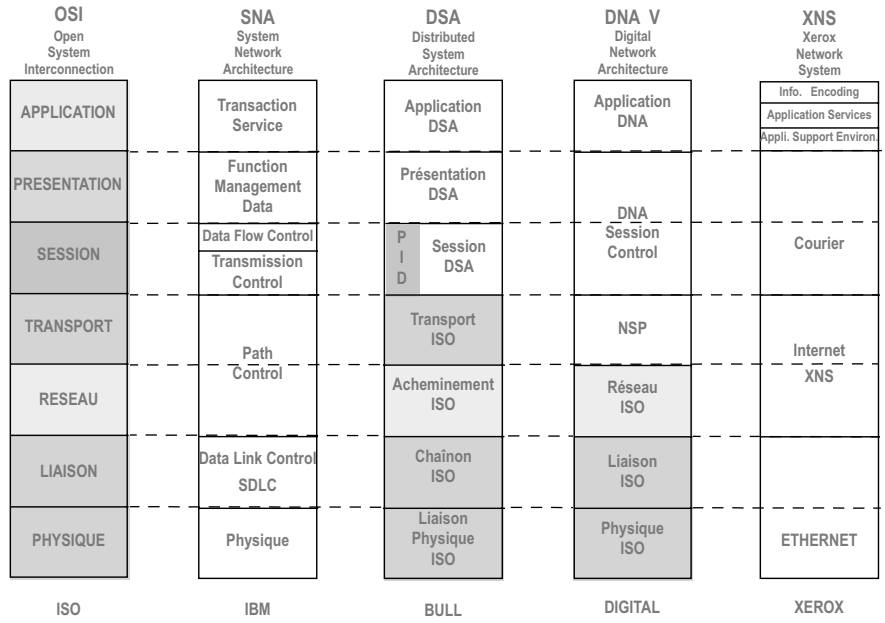


Figure 7.39 Les architectures propriétaires et OSI.

7.6 CONCLUSION

Une architecture propriétaire s'applique à un réseau physique spécifique et formalise les concepts fondamentaux qui ont conduit les constructeurs à tel ou tel choix. Aucune n'a pu s'imposer comme étant l'architecture de référence. Le modèle OSI, a certes formalisé les concepts, mais compte tenu de la complexité de ce modèle et donc des difficultés d'implémentation et d'évolution, il n'a donné lieu qu'à de timides développements. Le modèle de l'IUT s'est imposé pour les couches basses (signalisation hors bande). Quant à TCP/IP, objet du prochain chapitre, il est devenu aujourd'hui le modèle fédérateur.

EXERCICES

Exercice 7.1 Fonctions et couches OSI

Quelles sont les couches OSI chargées des opérations suivantes :

1. découpage du flot binaire transmis en trame ?
2. détermination du chemin à travers le réseau ?
3. fourniture de la synchronisation des échanges ?

Exercice 7.2 Adresse SAP d'une émission FM

Quelles sont les adresses SAP d'une émission de radio FM ?

Exercice 7.3 Encapsulation

Dans le modèle OSI, est-ce que ce sont les TPDU qui encapsulent les paquets ou le contraire ?

Exercice 7.4 Mode connecté et mode non connecté

Quel est, selon vous, le niveau OSI le plus approprié pour le mode de mise en relation (connecté ou non connecté), et pourquoi ?

Exercice 7.5 Terminal virtuel

Qu'apporte le protocole de terminal virtuel par rapport aux émulations et dans quels types d'application s'impose-t-il ?

Exercice 7.6 Contrôle de flux et transferts isochrones

Peut-on appliquer un mécanisme de contrôle de flux dans un système de communication multimédia (voix, données, vidéo) ? Justifiez votre réponse.

Exercice 7.7 Contrôle de flux et classe de transport 0

La classe 0 du protocole de transport OSI n'a pas de contrôle de flux, pourquoi ?

Exercice 7.8 Référencement d'une connexion de transport

Pourquoi a-t-on besoin d'identifier les références source et destination dans la partie fixe de la TPDU_CR sachant que les TSAP source et destination sont référencées dans la partie variable ?

© Dunod – La photocopie non autorisée est un délit

Exercice 7.9 Connexion de transport et connexion de session

Énumérez au moins trois similitudes et trois différences entre une connexion session et une connexion transport.

Exercice 7.10 Les types de variables d'ASN-1

1. Expliquez les différents types de variables ASN-1 pour illustrer les types :
   - BOOLEAN
   - BITSTRING
   - ISO646STRING
   - CHOICE
   - SEQUENCE.
2. Puis, définissez une variable de type SET pour illustrer l'utilisation des mots clés :
   - IMPLICIT
   - OPTIONAL
   - DEFAULT
   - NULL

Exercice 7.11 Couche transport

Rappelez et illustrez, avec un exemple simple de la vie courante, le rôle de la couche transport.

Chapitre **8**

Introduction à TCP/IP

8.1 GÉNÉRALITÉS

8.1.1 Origine

L'architecture TCP/IP a été développée, dans le milieu des années 70, par la **DARPA** (*Defense Advanced Research Projets Agency* – États-Unis) pour les besoins de communication et d'interfonctionnement des applications entre les systèmes informatiques de l'armée (**DoD**, *Department of Defense*). Pour cela, il fallait définir un format d'échange des données commun à tous les systèmes tout en préservant l'existant, c'est-à-dire sans modifier les réseaux réels. L'architecture à définir devant garantir une grande résistance à la défaillance de n'importe quel nœud du réseau, le mode datagramme s'imposait pour la couche réseau.

Pour conclure, TCP/IP, du nom de ses deux protocoles principaux (**TCP**, *Transmission Control Protocol* et **IP**, *Internet Protocol*), est un ensemble de protocoles permettant de résoudre les problèmes d'interconnexion en milieu hétérogène. À cet effet, TCP/IP décrit un réseau logique (réseau IP) au-dessus du ou des réseaux physiques réels, auxquels sont effectivement connectés les ordinateurs (figure 8.1).

Dans cette approche, les échanges entre applications sont réalisés selon le format défini par TCP/IP, alors que l'échange des données dans les sous-réseaux physiques réels se réalise selon le format propre à chaque sous-réseau.

L'intégration de TCP/IP à UNIX BSD 4, par l'université de Berkeley, en fit le standard de la communauté UNIX (1980). En 1983, TCP/IP a remplacé le protocole NCP (*Network Control Program*) dans ARPANET, ancêtre de l'Internet. Aujourd'hui, TCP/IP est le protocole standard de tous les réseaux, du LAN au WAN. De récentes adaptations autorisent les flux multimédias et, en particulier, les services voix sur IP (**ToIP**, *Telephony over TCP/IP*).

8.1.2 Principe architectural

Précédant le modèle OSI, TCP en diffère fortement, non seulement par le nombre de couches, mais aussi par l'approche. Le modèle OSI spécifie des services (approche formaliste), TCP/IP

des protocoles (approche pragmatique). Développé au-dessus d'un environnement existant, TCP/IP ne décrit, à l'origine, ni de couche physique ni de couche liaison de données. Les applications s'appuient directement sur le service de transport. Aussi l'architecture TCP/IP ne comprend que deux couches : la couche transport (TCP) et la couche inter-réseau (IP). La figure 8.2 compare les deux architectures.

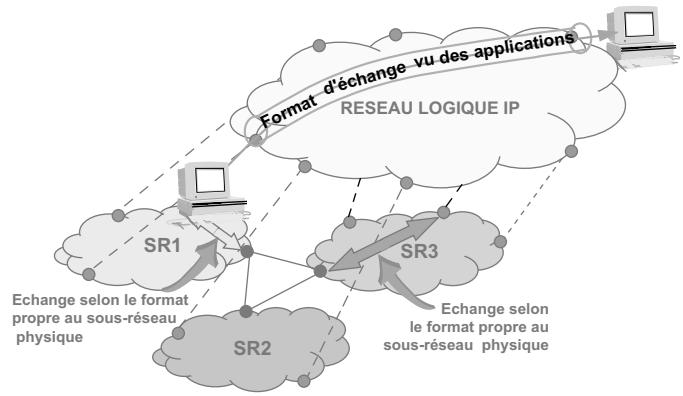


Figure 8.1 Le réseau logique IP et sous-réseaux physiques réels (SRx).

Il n'y a pas de couche application au sens OSI du terme, c'est-à-dire de couche présentant des « **API** » (*Application Programming Interface*) aux applications qui rendent transparents à ces dernières le ou les sous-réseaux réels de transport utilisés. Cependant, un mécanisme particulier, les *sockets*, assure une communication d'application à application en masquant les éléments réseaux.

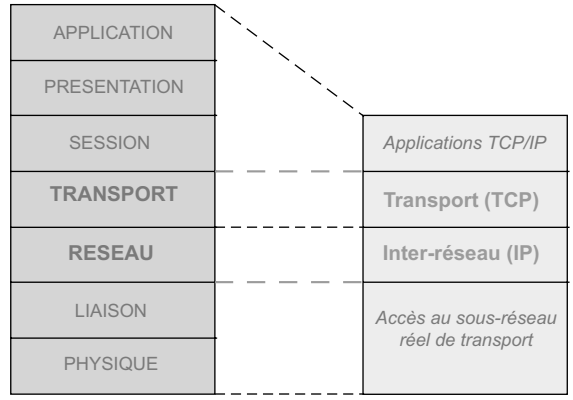


Figure 8.2 Le modèle OSI et l'architecture TCP/IP.

La couche transport fournit deux types de service : un service en mode connecté (TCP) comparable, en ce qui concerne les services rendus, à TP4 d'ISO et un service de transport allégé **UDP** (*User Datagram Protocol*) qui n'offre qu'un service de type *best effort* (datagramme).

La couche réseau[1] (*Internet Protocol*, IP) présente les mêmes fonctionnalités que la couche réseau d'ISO en mode non connecté (mode datagramme), et les services rendus sont comparables à ceux de la norme ISO 8473 (couramment appelé CLNP/CLNS, *Connectionless Network Protocol/Connectionless Network Services*).

8.1.3 La description générale de la pile et les applications TCP/IP

L'architecture TCP/IP comprend de nombreux programmes applicatifs, utilitaires et protocoles complémentaires (figure 8.3). À l'origine TCP/IP ne spécifiait aucun protocole de ligne, il s'appuyait sur les réseaux existants. L'utilisation massive de TCP/IP a fait apparaître le besoin de liaisons tout IP et donc la nécessité de disposer de protocoles de liaison spécifiques (SLIP, PPP). De même, TCP/IP a été adapté aux protocoles dits « haut débit » comme le Frame Relay[2] et l'ATM (*Asynchronous Transfer Mode*) qui constituent aujourd'hui le cœur de la plupart des réseaux privés et d'opérateurs.

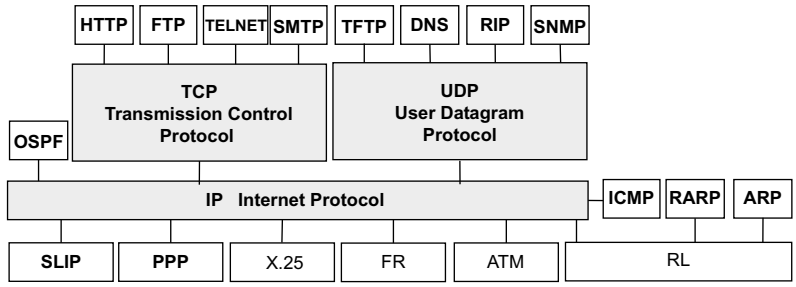


Figure 8.3 Les protocoles et les applications de TCP/IP.

Les principaux protocoles et applications de l'environnement TCP/IP sont les suivants :

- **ARP**, *Address Resolution Protocol*, met en correspondance une adresse logique IP avec une adresse physique **MAC** (*Medium Access Control*, adresse de l'interface dans les réseaux locaux) ;
- **DNS**, *Domain Name System*, est un système de bases de données réparties assurant la correspondance d'un nom symbolique et d'une adresse internet (adresse IP) ;
- **FTP**, *File Transfer Protocol*, est un système de manipulation de fichiers à distance (transfert, suppression, création...) ;
- **HTTP**, *HyperText Transport Protocol*, assure le transfert de fichiers hypertextes entre un serveur Web et un client Web ;
- **ICMP**, *Internet Control and error Message Protocol*, assure un dialogue IP/IP et permet notamment : la signalisation de la congestion, la synchronisation des horloges et l'estimation des temps de transit... Il est utilisé par l'utilitaire **Ping** qui permet de tester la présence d'une station sur le réseau.

1. Devant répondre à des impératifs militaires, le réseau devait présenter une très grande robustesse à la défaillance d'un nœud. Dans ces conditions, seul le mode non connecté était approprié.
2. Les protocoles Frame Relay (Relais de Trames) et ATM seront étudiés au chapitre 14.

© Dunod – La photocopie non autorisée est un délit

– **OSPF**, *Open Shortest Path First*, est un protocole de routage du type état des liens, il a succédé, dans le réseau Internet, au protocole RIP ;
– **PPP**, *Point to Point Protocol*, protocole d'encapsulation des datagrammes IP, il assure la délimitation des trames, identifie le protocole transporté et la détection d'erreurs.
– **RARP**, *Reverse Address Resolution Protocol*, permet l'attribution d'une adresse IP à une station ;
– **RIP,** *Routing Information Protocol*, est le premier protocole de routage (vecteur distance) utilisé dans Internet ;
– **SLIP**, *Serial Line Interface Protocol*, protocole d'encapsulation des paquets IP, ce protocole n'assure que la délimitation des trames ;
– **SMTP**, *Simple Mail Transfer Protocol*, offre un service de courrier électronique ;
– **SNMP,** *Simple Network Management Protocol*, est devenu le standard des protocoles d'administration de réseau ;
– **TELNET**, *TELetypewriter NETwork protocol* (ARPA) ou *TERminaL NETwork protocol*, système de terminal virtuel, permet l'ouverture de sessions avec des applications distantes ;
– **TFTP**, *Trivial FTP*, est une version allégée du protocole FTP.

8.1.4 Les mécanismes de base de TCP/IP

Le mode de mise en relation

Désirant alléger au maximum la couche inter-réseau, les concepteurs de TCP/IP n'ont spécifié qu'une couche réseau en mode non connecté (mode datagramme). Ce mode de mise en relation optimise l'utilisation des ressources réseaux mais ne permet pas d'assurer ni un contrôle d'erreur, ni un contrôle de flux. Au niveau du réseau, ces tâches peuvent être assurées par le ou les sous-réseaux réels de transport. Cependant, compte tenu qu'IP ignore la qualité de service offerte par ces sous-réseaux, la couche TCP pallie les insuffisances de la couche inter-réseau (*Internet Protocol*) en assurant le contrôle d'erreur, le contrôle de flux et de congestion. Cette approche, illustrée par la figure 8.4, reporte sur les systèmes d'extrémité les tâches normalement dévolues à la couche réseau et en particulier le contrôle de congestion.

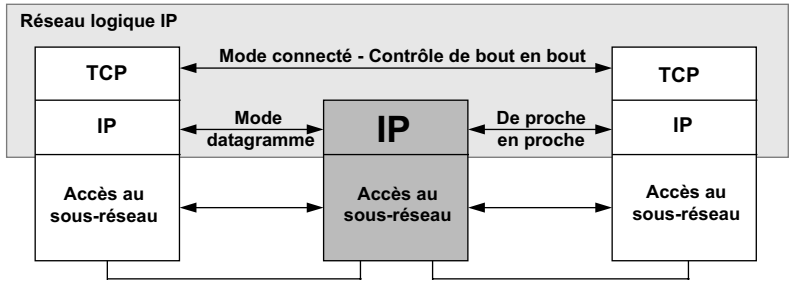


Figure 8.4 Le réseau logique IP et les modes de mise en relation.

L'encapsulation des données

L'encapsulation consiste à transporter les données d'une couche dans une unité de données de la couche inférieure. Un en-tête contient les informations nécessaires à l'entité homologue distante pour extraire et traiter les données. Dans le modèle TCP/IP, les données de l'application constituent des messages, ceux-ci sont transportés dans des segments TCP qui seront émis sur le réseau sous forme de datagrammes IP. L'unité de transport élémentaire est la trame qui constitue au niveau physique un train de bits (figure 8.5).

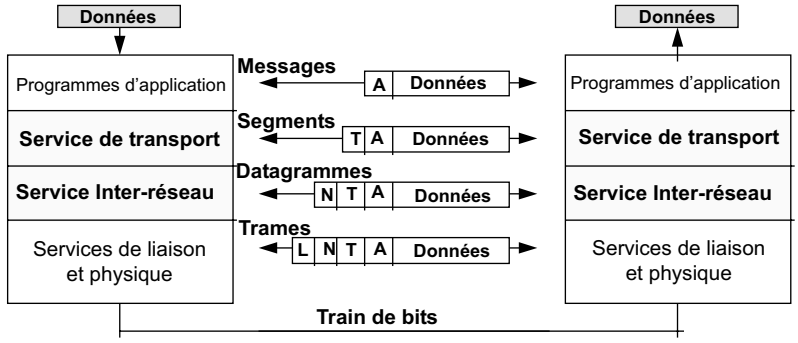


Figure 8.5 L'encapsulation des données dans TCP/IP.

Contrairement au modèle OSI, TCP/IP utilise un format unique d'en-tête de taille fixe. Cette approche, en nécessitant des en-têtes relativement importants, pénalise le débit (*overhead* protocolaire), mais optimise le traitement des blocs de données dans les systèmes intermédiaires. La terminologie utilisée pour désigner les différents blocs de données diffère quelque peu de celle du modèle de référence de l'ISO.

L'identification des protocoles

À l'instar du modèle OSI avec la notion de **SAP** (*Service Access Point*), un adressage de couche organise le dialogue vertical. Chaque unité protocolaire de TCP/IP identifie le protocole ou l'application supérieure. L'**EtherType** des trames « Ethernet[3] » identifie le protocole du niveau réseau. L'identifiant de **Protocol** dans le datagramme IP désigne le protocole de transport utilisé et la notion de **Port** dans le segment TCP détermine l'instance locale de l'application. La figure 8.6 illustre ce principe et donne quelques exemples d'identifiants normalisés.

La taille du segment de données échangé

Chaque réseau, en fonction de ses caractéristiques spécifiques, admet des unités de données de taille plus ou moins grande (**MTU**, *Maximum Transfer Unit*). Pour certains réseaux, cette taille est normalisée. C'est le cas, par exemple, pour les réseaux de type Ethernet où la MTU est fixée à 1 500 octets. Dans les réseaux étendus (WAN), la taille est déterminée par l'opérateur en fonction des caractéristiques de ses éléments actifs (*buffers*...). Un datagramme peut, pour atteindre

3. Ethernet est le nom de marque déposé par Xerox d'un type de réseau local ; ce terme désigne par abus de langage tous les réseaux locaux utilisant le protocole d'accès CSMA/CD.

© Dunod – La photocopie non autorisée est un délit

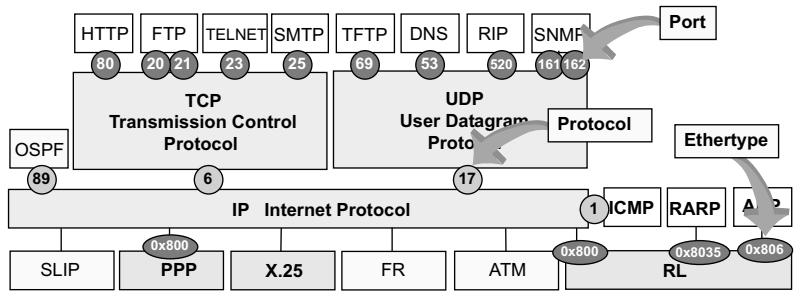


Figure 8.6 L'identification des protocoles dans TCP/IP.

sa destination, traverser plusieurs réseaux dont les MTU diffèrent. Si le datagramme à transférer a une taille supérieure à la MTU du réseau, le routeur d'accès devra le rejeter ou le fractionner (segmenter) pour le rendre compatible avec les capacités de transport du réseau (figure 8.7).

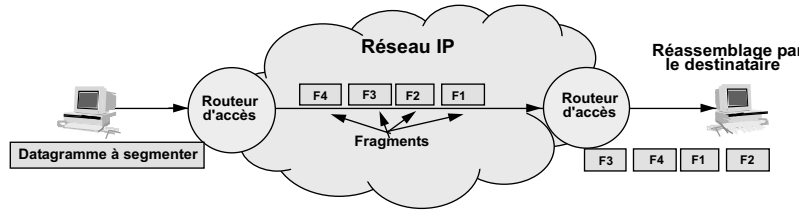


Figure 8.7 Principe de la segmentation sous IP.

Le routage de chaque fragment étant indépendant du précédent et du suivant, aucun nœud n'a la certitude de recevoir tous les fragments ; dans ces conditions, seul le destinataire a la capacité de réassembler les différents fragments.

Ainsi, en mode datagramme la perte d'un seul fragment implique une retransmission complète du segment TCP d'origine. Afin d'éviter la reprise d'un segment complet, on cherche à définir une taille de segment correspondant à la taille maximale que peut supporter le réseau. En principe, tous les réseaux IP doivent assurer une MTU minimale de 576 octets. En conséquence, les passerelles inter-réseaux doivent être capables de traiter des segments de 576 octets sans avoir à les fragmenter. Néanmoins, cette taille n'est pas nécessairement compatible avec celle admissible par tous les sous-réseaux physiques traversés. Dans ces conditions, la couche IP fragmentera le bloc de données (datagramme IP), chaque fragment constituant un nouveau datagramme IP acheminé indépendamment des autres.

Lors de l'établissement de la connexion de transport, une option de TCP permet l'annonce, et non la négociation, de la taille maximale de segment que le système d'extrémité peut admettre (**MSS**, *Maximum Segment Size*). La figure 8.8 illustre la relation entre MSS et MTU pour une valeur de MTU par défaut de 576 octets. Cette MTU garantit une charge utile minimale de 512 octets aux données de l'application.

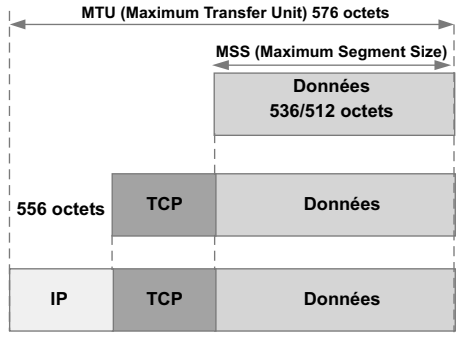


Figure 8.8 Relation entre MTU et MSS (valeur implicite).

8.1.5 Les instances de normalisation

Plusieurs organismes contribuent à la cohérence des développements des protocoles liés à TCP/IP. Ce sont principalement l'**IAB** (*Internet Activities Board*) qui assure les relations avec les autres organismes de normalisation et définit la politique d'évolution à long terme. L'**IETF** (*Internet Engineering Task Force*) se préoccupe des évolutions à court et moyen terme. Enfin, l'**IANA** (*Internet Assigned Number Authority*) gère l'attribution d'adresses IP. Des organismes régionaux agissent par délégation de l'IANA, c'est par exemple le **RIPE** (Réseaux IP européens) représenté en France, depuis le 1er janvier 1998, par l'**AFNIC** (Association française pour le nommage internet en coopération). Les standards ou normes TCP/IP sont publiés sous forme de **RFC** (*Request For Comments*). La RFC 1602 décrit le processus d'élaboration (*The Internet Standards Process*) d'une RFC.

8.2 L'ADRESSAGE DANS LE RÉSEAU LOGIQUE

8.2.1 Principe de l'adressage IP

Chaque machine (*Host*), raccordée au réseau logique IP, est, indépendamment de l'adressage physique utilisé dans le sous-réseau réel (figure 8.9), identifiée par un identifiant logique ou une adresse IP. Le réseau logique IP masque le réseau physique. Pour assurer l'acheminement des données dans le réseau physique, il est nécessaire de définir des mécanismes de mise en relation de l'adresse logique, seule connue des applications, avec l'adresse physique correspondante (résolution d'adresses).

Les techniques utilisées pour réaliser la mise en correspondance des adresses diffèrent selon que le réseau supporte ou non la diffusion (réseaux **NBMA**, *Non Broadcast Multiple Access*). Notamment dans les réseaux en mode connecté, l'administrateur réseau peut être conduit à renseigner manuellement les passerelles[4] inter-réseaux (table statique, figure 8.10).

4. Le terme passerelle sera fréquemment utilisé en lieu et place du terme routeur. En effet, en principe un routeur achemine des données dans un même espace d'adressage, or le nœud d'accès entre le réseau logique et le réseau physique réalise certes le routage du niveau IP, mais aussi met en correspondance l'adressage IP avec celui du réseau physique utilisé. Il ne s'agit donc pas d'un routeur au sens strict mais plutôt d'une passerelle inter-réseau.

© Dunod – La photocopie non autorisée est un délit

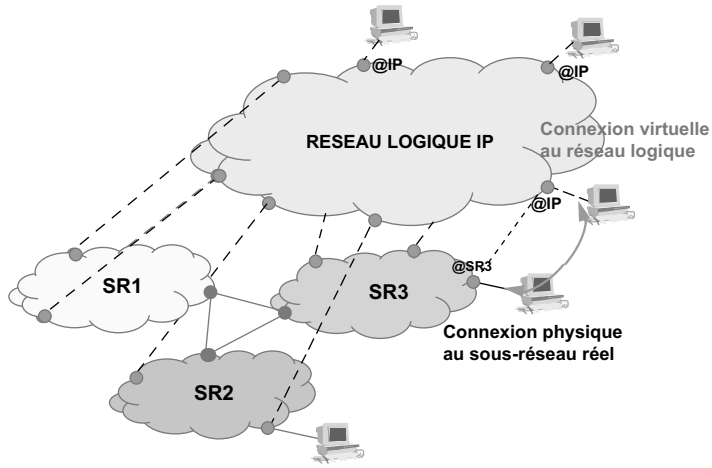


Figure 8.9 Nécessité d'une résolution d'adresses.

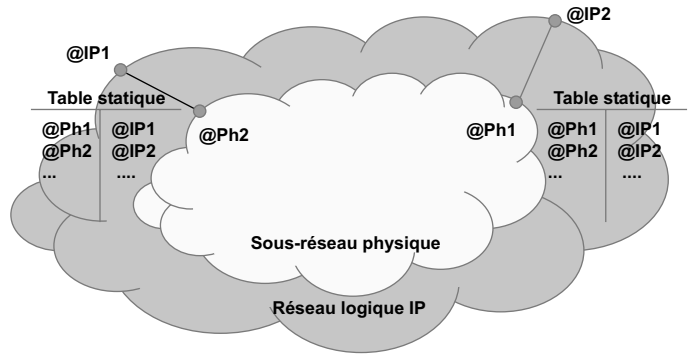


Figure 8.10 La résolution d'adresses dans les réseaux sans diffusion.

Dans les réseaux où la diffusion est réalisable, la machine source diffuse un message du type *broadcast* (diffusion à tous) pour s'enquérir de l'adresse physique du destinataire. Seul, le destinataire qui reconnaît son adresse IP répond en indiquant quelle est son adresse physique. L'émetteur mémorise cette correspondance pour une utilisation ultérieure (cache ARP, *Address Resolution Protocol*). Ce mécanisme est illustré figure 8.11. Certains protocoles en mode connecté mettent en œuvre des mécanismes de résolution d'adresses en émulant sur un réseau en mode connecté un réseau de diffusion ou en utilisant un serveur d'adresses.

Enfin, le protocole IP doit assurer le routage dans le réseau logique IP. À cet effet, il doit pouvoir identifier le réseau logique IP (**Net_ID**) et, dans ce réseau, la machine cible (**Host_ID**). L'adressage logique IP ne comporte que ces deux informations (figure 8.12).



Figure 8.11 La résolution d'adresses dans les réseaux à diffusion.

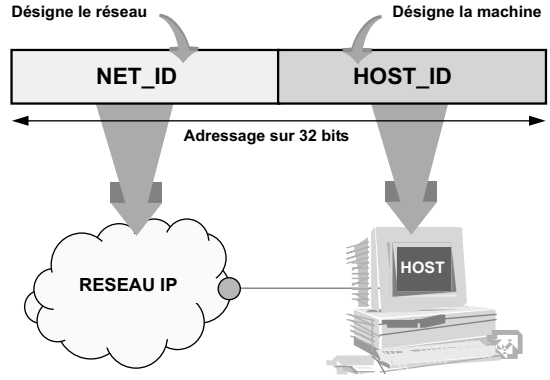


Figure 8.12 L'adressage dans le réseau logique IP.

8.2.2 Les techniques d'adressage dans un réseau IP

Les classes d'adressage

À chaque interface d'un système, connecté à un réseau IP, est assignée une adresse IP ou numéro IP. Cependant, l'adressage IP est un adressage à plat, il n'est pas possible, à partir de l'adresse IP, de déterminer la localisation géographique du réseau logique IP[5].

Limitée à 4 octets (32 bits), on représente l'adresse IPv4 par quatre valeurs décimales séparées par un point, la notation est dite décimale pointée (*Dotted-decimal notation*). Afin d'assurer une meilleure utilisation de l'espace d'adressage et d'adapter celui-ci à la taille et au besoin de chaque organisation, il a été introduit une modularité dans la répartition des octets entre l'identifiant réseau (Net_ID) et l'identifiant machine (Host_ID). Ainsi, cinq classes d'adresse (figure 8.13) ont été définies. Les premiers bits du champ adresse réseau (ID réseau ou Net_ID) permettent de distinguer la classe d'adressage.

Les adresses de classe A s'étendent de 1.0.0.1 à 126.255.255.254. Elles permettent d'adresser 126 réseaux[6] ($2^7 - 2$) et plus de 16 millions de machines[7] ($2^{24} - 2$, soit 16 777 214).

5. L'adressage IP a été redéfini dans IPv6. Cependant, les systèmes clients d'extrémité continueront encore longtemps d'utiliser IPv4 ; c'est pour cette raison qu'IPv4 continue d'avoir une place prépondérante dans cet ouvrage.
6. Les valeurs 0 et 127 sont réservées.
7. Les valeurs du champ Host_ID 0 et 255 ont une signification spécifique.

© Dunod – La photocopie non autorisée est un délit

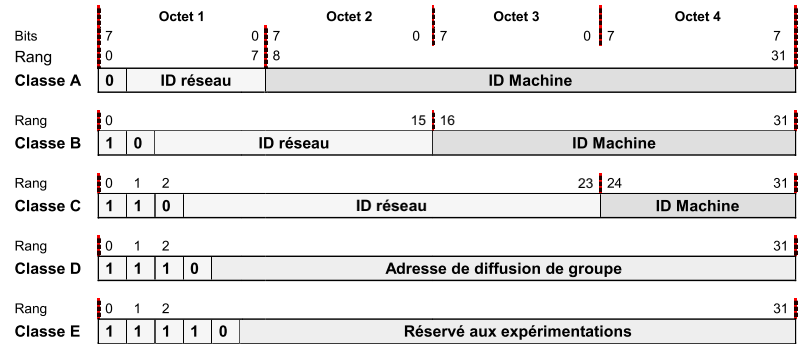


Figure 8.13 Les classes d'adresse IP.

Les adresses de classe B vont de 128.0.0.1 à 191.255.255.254, ce qui correspond à plus de 16 384 réseaux de 65 533 machines. Cette classe est la plus utilisée et les adresses sont aujourd'hui pratiquement épuisées.

La classe C couvre les adresses 192.0.0.1 à 223.255.255.254, elle adresse plus de deux millions de réseaux (2 097 152) de 254 machines.

Les adresses de la classe D sont utilisées pour la diffusion (*Multicast*) vers les machines d'un même groupe. Elles vont de 224.0.0.0 à 239.255.255.255. Ce groupe peut être un ensemble de machines, mais aussi un ensemble de routeurs (diffusion des tables de routage). Tous les systèmes ne supportent pas les adresses de *multicast*.

Enfin, les adresses de la classe E sont réservées aux expérimentations.

Les adresses spéciales

Toutes machines d'un réseau IP est identifié par le couple <Net_ID><Host_ID>. Certaines valeurs de ces champs ont une signification particulière. C'est ainsi que l'adresse <Net_ID> <0>, où tous les bits du champ Host_ID sont à zéro, désigne le réseau lui-même[8].

Certaines machines n'ont pas la possibilité de mémoriser une adresse IP. Lors du lancement de cette machine, le système émet une requête pour se voir attribuer une adresse IP (Protocole **RARP**, *Reverse Address Resolution Protocol*). Durant cette phase d'initialisation, la machine utilise l'adresse 0.0.0.0. Cette adresse ne peut donc pas être affectée à une machine particulière. Dans les routeurs, l'adresse 0.0.0.0 désigne la route par défaut (route à prendre si aucune autre route ne correspond à l'adresse destination).

La machine elle-même ou machine locale peut être auto-adressée avec une adresse de la forme 127. *x*. *x*. *x* ; cette adresse dite de boucle locale (*loopback* ou encore *localhost*) est utilisée lors de tests de la machine ou de programmes applicatifs. Tout datagramme émis à destination d'une adresse 127. *x. x .x* est directement recopié du tampon d'émission vers le tampon de réception, il

8. En fait, cette adresse correspond à l'adresse de *broadcast* du système UNIX BSD version 4.2. Son emploi, comme adresse *unicast*, est possible mais est à déconseiller. Il est préférable d'en réserver l'utilisation à la désignation du réseau. Dans cet ouvrage, nous nous conformerons à cet usage.

n'est jamais émis sur le réseau, ce qui protège ce dernier d'éventuels dysfonctionnements du nouvel applicatif en développement ou en test (figure 8.14).



Figure 8.14 L'adresse de boucle locale.

Lorsqu'une machine veut diffuser un message, elle peut, si le message ne s'adresse qu'à un ensemble de machines particulières, utiliser une adresse de *multicast* dite aussi de diffusion restreinte ou réduite. Si le message doit être adressé à toutes les machines, elle utilisera alors une adresse dite de diffusion générale. On distingue deux types d'adresses de diffusion générale :

– L'adresse 255.255.255.255 utilisée pour envoyer un message à toutes les machines du même segment de réseau. La diffusion est limitée aux seules machines de ce segment, le datagramme n'est pas relayé sur d'autres réseaux. L'adresse 255.255.255.255 est dite adresse de **diffusion générale** ou **limitée.**

– Si une machine veut s'adresser à toutes les machines d'un autre réseau, elle utilisera une adresse du type[9] <Net_ID><1>, tous les bits à 1 du champ Host_ID identifient toutes les machines du réseau <Net_ID><0>. Ce message de diffusion est relayé de réseau en réseau pour atteindre le réseau destinataire. L'adresse est dite de **diffusion dirigée**. Ce principe est illustré figure 8.15.

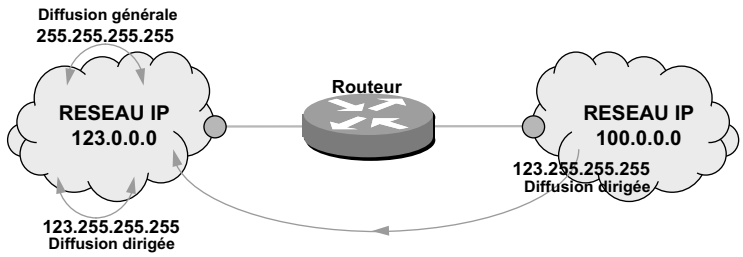


Figure 8.15 Les différentes adresses de diffusion.

Ainsi :

– l'adresse 123.0.0.0 désigne le réseau d'identifiant 123 ;

– l'adresse 123.0.0.18 désigne la machine 18 du réseau 123

9. Pour simplifier et généraliser l'écriture des adresses, nous adopterons la convention d'écriture suivante : <0>, tous les bits du champ concernés sont à zéro ; <1>, tous les bits du champ concerné sont à 1.

© Dunod – La photocopie non autorisée est un délit

– l'adresse 123.255.255.255 est l'adresse de diffusion dirigée à utiliser pour envoyer un message à toutes les machines du réseau 123 ;
– l'adresse 255.255.255.255 est l'adresse de diffusion limitée aux seules machines du même segment de réseau que la machine source.

Les adresses publiques et les adresses privées

Pour permettre l'interconnexion des réseaux, il faut garantir l'unicité des adresses. C'est l'une des attributions de l'IANA qui attribue à chaque réseau un identifiant unique. Cependant, tous les réseaux n'ont pas nécessairement un besoin d'interconnexion *via* un réseau public, dans ce cas le respect de l'unicité d'adresse au plan mondial n'est pas nécessaire. Certaines entreprises (organisations) disposent de leur propre réseau (réseau privé) et n'ont aucun besoin d'interconnexion vers l'extérieur, il est alors possible d'utiliser n'importe quelle adresse IP. Les adresses utilisées dans ce cas sont dites illégales. Par opposition, une adresse attribuée par l'IANA est dite publique ou légale.

Afin de prévenir, dans les réseaux privés, une éventuelle utilisation anarchique des adresses, il a été envisagé de réserver des plages d'adresses à ces réseaux. Ces adresses ne sont pas routables sur le réseau Internet. Elles sont réservées à un usage privé (RFC 1918). De ce fait, elles sont dites adresses privées alors que par opposition les autres sont dites publiques. La figure 8.16 fournit la liste de ces adresses.

Classe	Début de la plage	Fin de la plage	Nombre de réseaux
A	10.0.0.0		1
B	172.16.0.0	172.31.0.0	16
C	192.168.0.0	192.168.255.0	256

Figure 8.16 Les adresses privées (RFC 1918).

Que faire si un réseau utilisant des adresses de type privé a soudainement des besoins d'accès à un réseau public ? Deux solutions sont envisageables :

– renuméroter toutes les stations avec des adresses publiques, non envisageable dans un grand réseau ;
– réaliser une conversion d'adresses (**NAT**, *Network Address Translator*), c'est-à-dire mettre en œuvre un mécanisme qui établit une correspondance entre une adresse privée et une adresse publique.

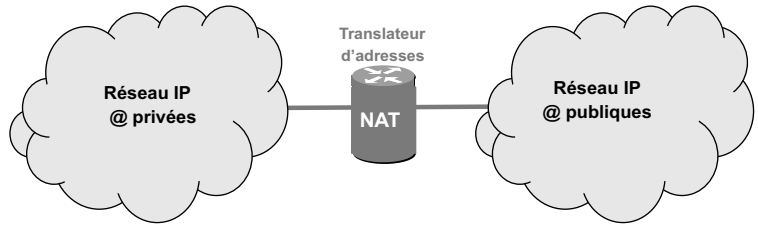


Figure 8.17 Le NAT est l'interface entre un réseau privé et un réseau public.

Pour des raisons évidentes de commodité, seule la seconde solution est généralement adoptée. La passerelle d'accès au réseau public réalisera la translation d'adresses (figure 8.17). La traduction peut être statique, dans ce cas la table de correspondance est renseignée par l'administrateur du réseau, à une adresse privée on fait correspondre une adresse publique. Cette approche limite les possibilités de connexion vers l'extérieur. La traduction peut aussi être dynamique, la mise en correspondance adresse privée/adresse publique est établie au moment du besoin d'interconnexion de la machine du réseau privé. Les adresses publiques peuvent alors être partagées par l'ensemble des machines du réseau privé. La traduction dynamique permet de n'utiliser qu'un nombre restreint d'adresses publiques voire une seule pour *N* machines.

Notion de sous-réseau : le subnetting

➤ Nécessité de définir des sous-réseaux

Supposons une organisation dont les moyens informatiques sont répartis sur deux sites, A et B (figure 8.18). Les tables de résolution d'adresses des passerelles d'accès au réseau physique doivent contenir une entrée pour chaque machine du site distant, alors que le point d'accès au sous-réseau physique réel est le même et que, par conséquent, l'adresse physique est identique (figure 8.18, site A). Pour alléger cette table et faciliter le routage, on pourrait imaginer doter chaque réseau de site (sous-réseau) d'un identifiant réseau <Net_ID>. Cette approche, non seulement n'est pas rigoureusement conforme à l'approche IP qui consiste à ne créer qu'un seul réseau logique IP par organisation, mais de plus elle est consommatrice d'adresses. Il est préférable de n'attribuer qu'un seul identifiant de réseau (un seul réseau logique IP par organisation) et de remplacer l'énumération d'adresses IP par un identifiant de site (figure 8.18, site B), il n'aura plus alors qu'une seule entrée pour toutes les machines attachées à un même réseau physique A.

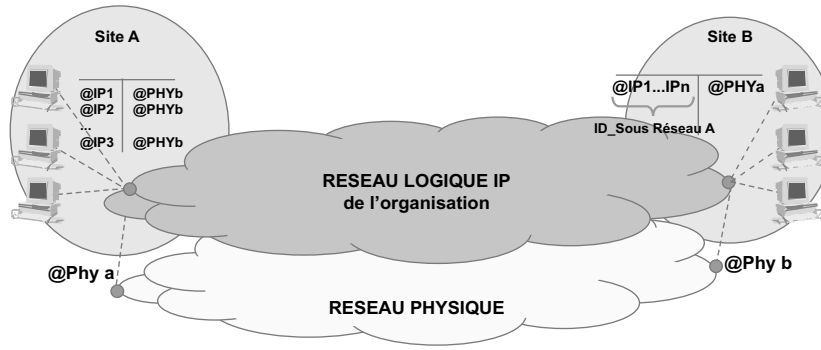


Figure 8.18 Notion de sous-réseaux logiques.

En pratiquant ainsi, tout nœud du réseau logique est parfaitement différencié et localisé par un unique identifiant du réseau logique <Net_ID>, un identifiant du site local ou de sous-réseau appelé <SubNet_ID> et enfin un numéro du nœud ou *host* (figure 8.19). La structure originelle de l'adressage IP ne prend pas en compte cette structure d'adresse. Aussi, compte tenu que généralement tous les bits du champ <Host_ID> ne sont pas utilisés pour numéroter les machines, il suffit donc d'en prélever quelques-uns pour identifier le sous-réseau. La taille du champ <SubNet_ID> sera déterminée en fonction du nombre de sous-réseaux à distinguer.

© Dunod – La photocopie non autorisée est un délit

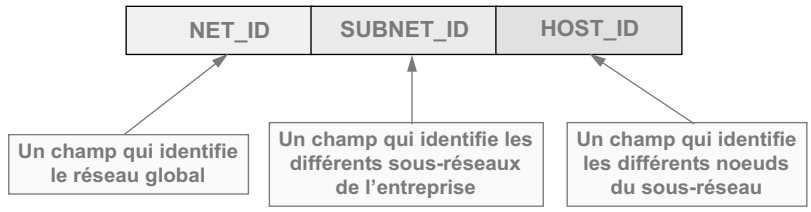


Figure 8.19 La technique du subnetting décompose l'adresse IP en trois champs.

En principe, l'acheminement est réalisé à partir du champ <Net_ID> dont la taille, dépendant de la classe d'adressage, est connue de chaque routeur. L'utilisation d'un identifiant supplémentaire de longueur variable nécessite d'indiquer à chaque nœud du réseau les bits de l'adresse IP à prendre en compte pour définir l'acheminement dans le réseau. Cette information est fournie, à chaque nœud adressé, sous forme d'un champ de bits à 1 appelé **masque de sous-réseau** (figure 8.20).

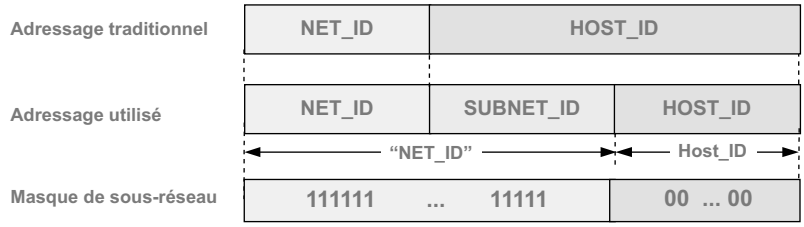


Figure 8.20 Principe du masque de sous-réseau.

Il existe deux méthodes d'écriture des masques de sous-réseaux, qui sont équivalentes :

– réseau : 10.0.0.0, masque de sous-réseau 255.255.240.0 ;
– ou plus simplement 10.0.0.0/20, le préfixe 20 indique la longueur en bits du masque de sous-réseau (longueur du préfixe réseau ou simplement préfixe).

➤ Utilisation du masque de sous-réseau

Lorsqu'une station émet un datagramme à destination d'une autre station, la couche IP locale vérifie, à l'aide du masque de sous-réseau, si le datagramme appartient au même sous-réseau que celui de l'émetteur. Si le datagramme est destiné à une station située sur un sous-réseau distant, le datagramme est envoyé à la passerelle par défaut, à charge pour celle-ci d'adresser le datagramme vers le bon sous-réseau. Ainsi, une station d'un réseau logique IP doit connaître (figure 8.21) :

– son adresse IP ;
– le masque de sous-réseau ;
– l'adresse de la passerelle locale (routeur).

Pour déterminer si la machine cible est localisée sur le même sous-réseau, la machine source réalise un « ET » logique entre les bits de l'adresse source et ceux du masque de sous-réseau, elle procède de même avec l'adresse destination. Si le résultat donne une valeur identique, les deux machines sont sur le même sous-réseau, sinon le datagramme est adressé à la passerelle par défaut (figure 8.22), charge à elle de trouver le sous-réseau destinataire.

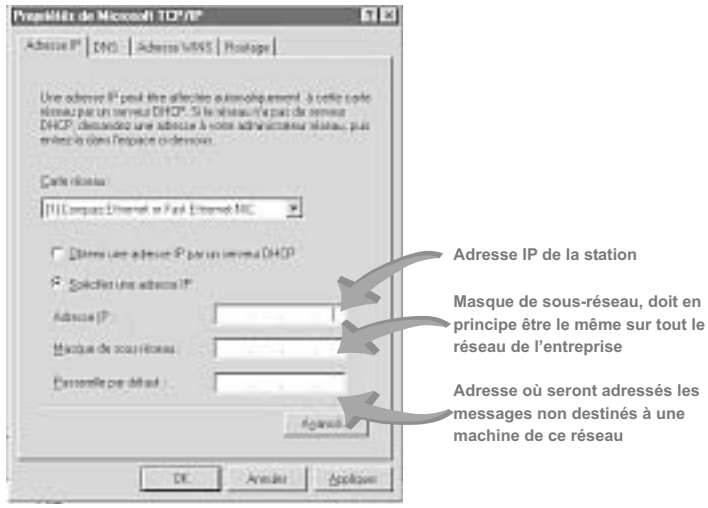


Figure 8.21 Les informations de configuration d'une machine.

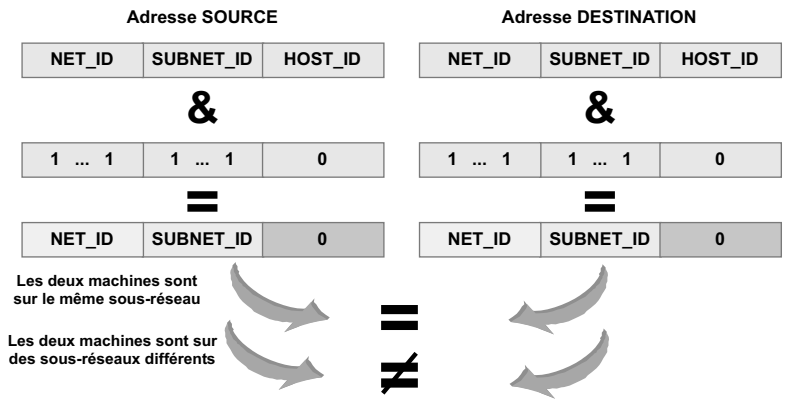


Figure 8.22 Détermination du sous-réseau cible à l'aide du masque de sous-réseau.

➤ Détermination du masque de sous-réseau

Broadcast de sous-réseau

Deux types de *broadcast* ont déjà été définis :

– 255.255.255.255 adresse toutes les machines du réseau sur lequel il a été émis. Ce *broadcast* ne franchit pas les passerelles (diffusion limitée).

– <Net_ID>.<1>, tous les bits du champ <Host_ID> à 1, désigne toutes les machines du réseau <Net_ID>. Ce *broadcast*, dit *broadcast* dirigé, est acheminé par les passerelles, sauf configuration spécifique de celles-ci.

Pour prendre en compte les sous-réseaux, il convient d'en ajouter un troisième :

– <Net_ID>.<SubNet_ID>.<1>, tous les bits du champ <Host_ID> à 1, adresse toutes les machines du sous-réseau <SubNet_ID>.

© Dunod – La photocopie non autorisée est un délit

L'unicité du masque sur un même réseau

Même si la RFC 1009 autorise, pour un même réseau, l'utilisation de masques de sous-réseaux multiples, cette pratique est à déconseiller. En effet, elle peut introduire des confusions dans l'interprétation des adresses et par conséquent dans l'acheminement. Soit, par exemple, le réseau 10.0.0.0 et le numéro IP 10.1.1.255 :

– si le masque de sous-réseau est 255.255.0.0, cette adresse représente la machine <1.255> du sous-réseau 1.
– mais si le masque de sous-réseau est 255.255.255.0, il s'agit alors de l'adresse de *broadcast* dirigé du sous-réseau 10.1.1.0.

De même, supposons le réseau de figure 8.23, lorsque l'*host* <1.8> du sous-réseau 10.1.0.0/16 veut adresser l'*host* <5> du sous-réseau 10.1.1.0/24, la machine <1.8> considère que son correspondant est situé sur le même sous-réseau qu'elle. Ceci est aussi vrai dans l'autre sens.

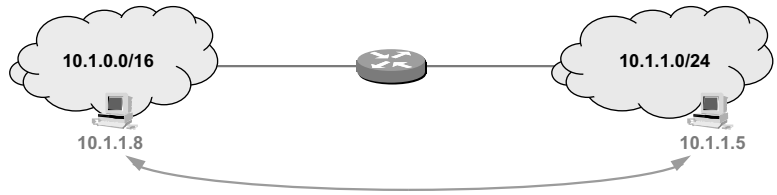


Figure 8.23 Les masques de sous-réseaux multiples et les problèmes d'acheminement.

Espace de numérotation d'un masque de n *bits*

Prenons un réseau d'adressage 10.0.0.0/20, le numéro :

– 10.3.0.0 représente-il le réseau <10.3> ou le premier sous-réseau <0> de numéro 10.3.0 ?
– 10.3.255.255 est-il un *broadcast* dirigé vers l'ensemble des machines du réseau <10.3 > ou un *broadcast* dirigé, mais limité au seul sous-réseau 10.3.240.0 ?

Dans ces conditions l'utilisation des valeurs tout à <0> et tout <1> du champ <SubNet_ID> est déconseillée. La capacité de numérotation (C_n) d'un masque de sous-réseau de n bits est de :

$$C_n = 2^n - 2$$

La première conséquence est que pour distinguer deux sous-réseaux, il faut au moins 2 bits (figure 8.24).

Valeur	Ordre du S/R
00	Interdit
01	1er S/R
10	2e S/R
11	Interdit

Figure 8.24 La capacité de numérotation de 2 bits.

Ainsi, les critères à prendre en considération pour la détermination d'un masque de sous-réseau sont :

– l'espace de numérotation des *hosts*, c'est-à-dire le nombre de machines à numéroter et l'évolution probable de ce nombre (nombre de bits du champ <Host_ID>) ;
– l'espace de numérotation des sous-réseaux, c'est-à-dire le nombre de sous-réseaux à distinguer et l'évolution probable de ce nombre (nombre de bits du champ <SubNet_ID>) ;
– la lisibilité, c'est-à-dire permettre par simple lecture d'identifier facilement le sous-réseau concerné.

Les masques de longueur variable (VLSM) de la RFC 1009

Si l'utilisation de masques de longueur variable de la RFC 1009 (**VLSM**, *Variable Length Subnet Mask*) est à déconseiller, l'utilisation d'adresses hiérarchiques permet d'ajuster la taille du masque aux besoins réels de l'entreprise et d'alléger les tables de routage en autorisant l'agrégation de routes. Cette approche n'est applicable que sur un réseau lui-même hiérarchique, c'est-à-dire que l'adresse doit avoir une signification topologique. La figure 8.25 illustre le principe de l'adressage hiérarchique. Dans cette représentation, une adresse d'un niveau dont le masque est de 16 bits correspond soit à un réseau $2^{16} - 2$ machines ou à 254 sous-réseaux dont le masque serait de 24 bits.

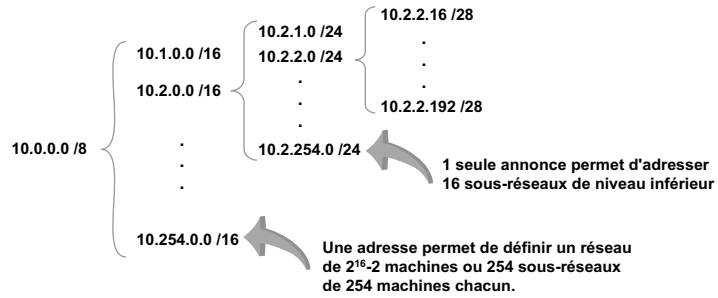


Figure 8.25 Principe du découpage hiérarchique de l'espace d'adressage.

L'adressage hiérarchique nécessite un réseau à routage statique ou l'utilisation d'un protocole de routage assurant le transport des masques de sous-réseaux comme RIPv2 ou OSPF. Si le routage dynamique est utilisé, les routeurs doivent mettre en œuvre un algorithme de recherche spécifique (recherche du préfixe le plus long) afin de déterminer la route à prendre.

L'adressage géographique ou CIDR

Une adresse IP désigne une organisation, elle ne permet pas d'en déterminer la localisation, c'est un adressage à plat. Dans ces conditions, chaque routeur du réseau Internet doit tenir à jour la liste de toutes les adresses attribuées (Net_ID) et la route à suivre. Cet encombrement des tables de routage pénalise les performances ; il a conduit, lors de la recherche de solutions pour pallier la prévisible pénurie d'adresses, à mettre en œuvre un mécanisme d'affectation géographique des adresses de classe C non attribuées.

D'autre part, il a été décidé de n'attribuer qu'exceptionnellement les adresses de classes B restantes et d'attribuer en lieu et place des adresses contiguës de classe C en leur faisant correspondre

© Dunod – La photocopie non autorisée est un délit

une seule entrée dans les tables de routage. La figure 8.26 indique les plages d'adresses géographiques[10] (RFC 2050).

Plage d'adresses	Zone d'affectation
192-193	Divers (adresses déjà attribuées)
194-195	Europe (65 536 réseaux)
196-197	Divers
198-199	Amérique du Nord
200-201	Amérique centrale et du Sud
202-203	Pacifique
204-205	Divers
206-207	Divers

Figure 8.26 L'allocation géographique des adresses de classe C.

Ainsi, pour l'Europe, les adresses 194 et 195 ont les sept premiers bits identiques. Il suffit donc d'indiquer aux routeurs que le champ <Net_ID> à prendre en compte est de 7 bits et non de considérer ces adresses comme des adresses de classes C. Une seule entrée suffit alors dans la table de routage. Le nombre de bits servant à coder la partie commune, ou préfixe d'adresse, est représenté à la fin de l'écriture de l'adresse comme suit : 194.0.0.0/7, ainsi cette adresse indique tous les sous-réseaux européens. Cette technique, issue de celle du masque de sous-réseau, porte le nom de *supernetting* ou routage interdomaine sans tenir compte de la classe d'adressage (**CIDR**, *Classless InterDomain Routing*).

Le CIDR améliore l'allocation des adresses et supprime l'usage des classes A, B et C en généralisant l'utilisant du préfixe (*classless*). L'utilisation du CIDR implique l'utilisation d'un protocole de routage transportant les préfixes étendus ; la mise en œuvre d'un algorithme de correspondance la plus longue et la distribution des adresses doit avoir une signification topologique. Dans ces conditions, le CIDR s'apparente au VLSM, cependant, l'un s'applique au domaine public, l'autre au domaine privé.

8.3 LE ROUTAGE DANS LE RÉSEAU IP

8.3.1 L'adressage d'interface

Supposons le réseau simplifié de la figure 8.27, peu importe le protocole mis en œuvre sur le lien reliant les passerelles d'accès (routeurs IP). Comment la couche IP peut-elle déterminer l'interface de sortie par rapport à une adresse IP destination alors que la couche IP ignore la technologie sous-jacente ?

En application du principe d'indépendance des couches, le point d'accès au réseau physique ne peut être connu de la couche IP que par une adresse IP. Les liaisons entre les différentes passerelles sont considérées, vu d'IP, comme constituant un réseau ; de ce fait chaque extrémité d'une

10. Les allocations d'adresses IPv4 peuvent être consultées à l'URL :
http://www.iana.org/assignments/ipv4-address-space

liaison possède une adresse IP. Dans ces conditions, l'algorithme d'acheminement recherche sur quel réseau (de liaisons) est situé le saut suivant (*Next hop*). Cette technique d'identification de l'interface d'accès au réseau physique est dite adressage d'interface ou **adressage de LS** (Liaison spécialisée). Cette méthode garantit l'indépendance des couches. En effet, le routage se réalise d'adresse IP destination à adresse IP d'interface.

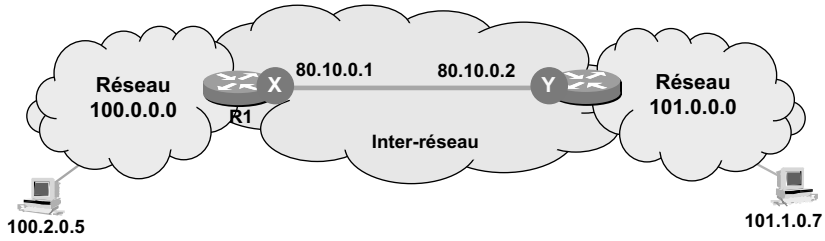


Figure 8.27 L'adressage du réseau physique.

Les liens inter-routeurs forment ainsi le réseau logique IP. Une adresse IP est attribuée à chaque extrémité. Pour comprendre le mécanisme de routage, la figure 8.28 fournit un exemple de configuration d'un routeur[11]. Notons que la route à prendre est désignée par l'adresse distante du lien (*Next hop*), ce qui correspond à l'adresse du point à atteindre sur le réseau de liens.

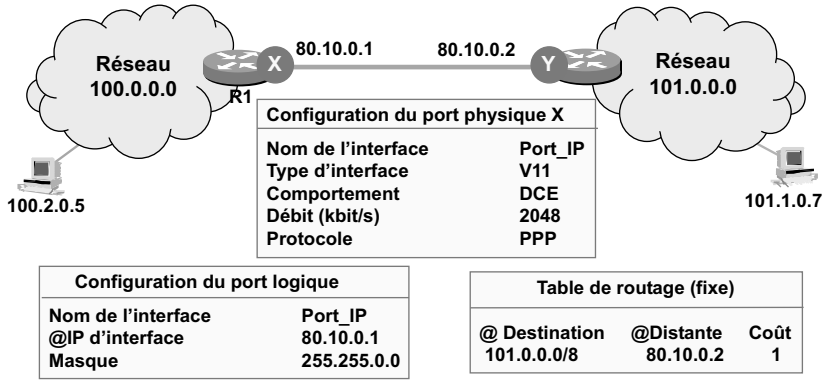


Figure 8.28 Exemple de configuration d'un routeur IP.

8.3.2 Le concept d'interface non numérotée

L'attribution d'adresses d'interface est consommatrice d'adresses, aussi la RFC 1812 a-t-elle autorisé le routage sur interface dite non numérotée (*Unnumbered IP*). Un exemple de configuration simplifiée est donné par la figure 8.29. Cette approche viole la règle d'indépendance des couches. Aussi, la RFC 1812 précise que les deux passerelles connectées par une ligne point à point non numérotée ne sont pas à considérer comme deux routeurs mais comme deux demi-routeurs constituant un seul routeur virtuel (figure 8.29).

11. Le mode de configuration d'un routeur est spécifique à chaque constructeur. Aussi, les exemples ci-après ne constituent qu'une illustration particulière.

© Dunod – La photocopie non autorisée est un délit

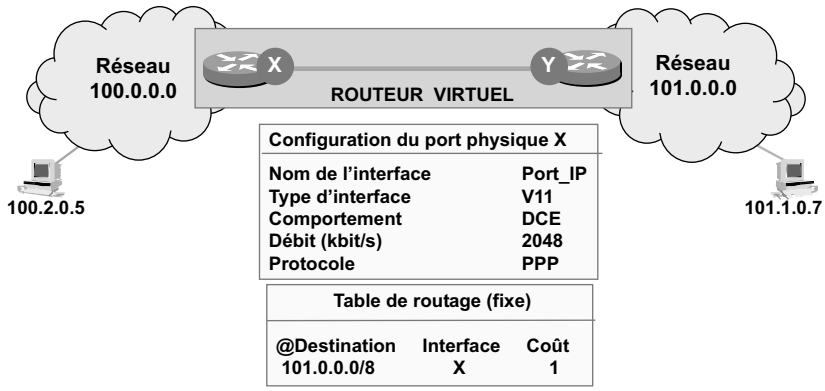


Figure 8.29 Le routage de la RFC 1812.

Les limitations de l'adressage, dues essentiellement à la structure à plat de l'adressage IP, conjuguées au succès d'Internet ont contribué à la pénurie d'adresses. Plusieurs solutions ont été imaginées pour pallier la pénurie. Celle retenue, IPv6, porte l'espace d'adressage de 32 à 128 bits.

8.4 L'ADRESSAGE DANS IPv6

8.4.1 Généralités

IPng (*Next generation*) ou IPv6 répond au besoin d'évolution de la communauté Internet et comble les faiblesses d'IPv4. La plus connue concerne l'espace d'adressage, IPv4 met en place un adressage à plat (Net_ID) ce qui a conduit à l'explosion des tables de routage (certains routeurs Internet ont plusieurs dizaines de milliers d'entrées dans leur table de routage). Le CIDR a partiellement résolu ce problème en faisant disparaître la notion de classe d'adresses, en autorisant l'agrégation d'adresses de réseaux contigus en un seul préfixe réseau et en organisant une affectation géographique des adresses. La seconde faiblesse concerne la pénurie d'adresses, l'utilisation d'un adressage privé associé à la translation d'adresses (NAT) résout partiellement ce problème mais pénalise fortement les performances. Aussi, l'adressage dans IPv6 a-t-il été porté à 128 bits, ce qui correspond à plusieurs milliers d'adresses au m^2 de surface terrestre.

Dans un système de réseaux interconnectés, seul un adressage hiérarchique permet l'allégement des tables de routage, chaque routeur ne traitant que la partie de l'adresse correspondant à son domaine. Cependant, dans une communauté aussi vaste que celle d'Internet, l'adressage hiérarchique devient vite sans signification, aussi entre l'adressage à plat non significatif d'IPv4 et l'adressage hiérarchique, tel que celui d'X.121, un compromis a été réalisé. L'adressage IPv6 comporte quatre champs (figure 8.30).

Le premier, sur 48 bits, est une agrégation hiérarchique de préfixes décrivant la connectivité du site, ce champ est désigné sous le terme topologie publique (identifiant des prestataires). Le second, sur 16 bits, décrit la topologie locale du site, enfin le dernier, sur 64 bits, identifie de manière unique au monde une interface. Cet adressage est dénommé adressage agrégé ou *Aggregatable Global Unicast Address Format*.

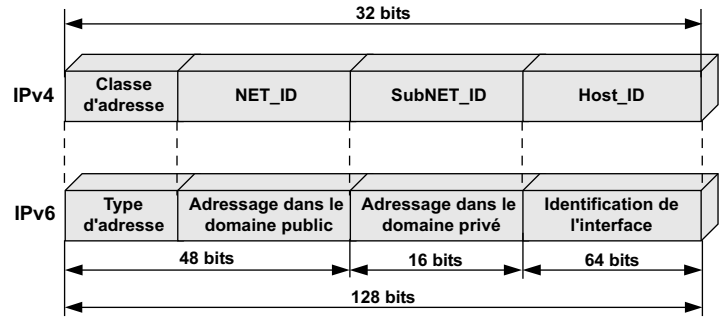


Figure 8.30 L'adressage IPv4 et IPv6.

8.4.2 La notation et le type d'adresse

Une notation hexadécimale, sur 16 bits séparés par deux points « : », remplace la notation décimale pointée d'IPv4. L'adresse passe de 32 à 128 bits, huit mots de 16 bits. Ainsi, une adresse IPv6 s'écrit :

FE0C:DA98:0:0:0:0:5645:376E

La notation peut être simplifiée en remplaçant une succession de 0 par « :: », l'abréviation « :: » ne pouvant être utilisée qu'une seule fois. Ainsi, l'adresse précédente devient :

FE0C:DA98::5645:376E

IPv6 adopte une notation similaire à celle du CIDR, le champ préfixe étant désigné par un nombre représentant la longueur en bits du préfixe, l'écriture est donc de la forme : @IPv6/ longueur du préfixe en bits, soit par exemple :

FE0C:DA98/32
FE0C:DA98:0:0/64
FE0C:DA98::/64

Très pénalisante en terme de performance réseau, la notion de *broadcast* disparaît. Elle est remplacée par une généralisation des adresses *multicast*. IPv6 distingue trois types d'adresse :

- les adresses ***unicast*** : une adresse *unicast* désigne une interface, elle peut être utilisée pour identifier un groupe d'interfaces lorsque ces interfaces constituent une agrégation de liens et doivent être vues comme une seule interface ;
- les adresses ***multicast*** (FF00::/8) : ces adresses désignent un ensemble d'interfaces dont la localisation n'est pas nécessairement sur le même réseau physique. Un datagramme adressé à une adresse *multicast* est acheminé à toutes les interfaces du groupe ;
- les adresses ***anycast*** : ces adresses introduites par IPv6 correspondent à une restriction des adresses de *multicast*. Elles désignent un ensemble d'interfaces partageant un même préfixe réseau. Cependant, lorsqu'un datagramme est adressé à une adresse *anycast*, il n'est délivré qu'à une seule interface du groupe, celle dont la métrique, au sens routage du terme, est la plus proche du nœud source.

© Dunod – La photocopie non autorisée est un délit

8.4.3 Le plan d'adressage

L'identifiant d'interface

L'indentifiant d'interface dans IPv6 correspond à la notion d'Host_ID d'IPv4. Afin de faciliter les opérations d'autoconfiguration et de disposer d'un identifiant unique au niveau mondial, l'identifiant correspond à une nouvelle proposition d'extension de l'adressage IEEE sur 64 bits. Ce nouvel identifiant d'interface sur 64 bits (*EUI-64*, *End-User Interface*) garantit l'unicité d'adresse. Pour les interfaces non dotées de cet identifiant, celui-ci peut être déduit de l'adresse MAC IEEE de 48 bits (figure 8.31).

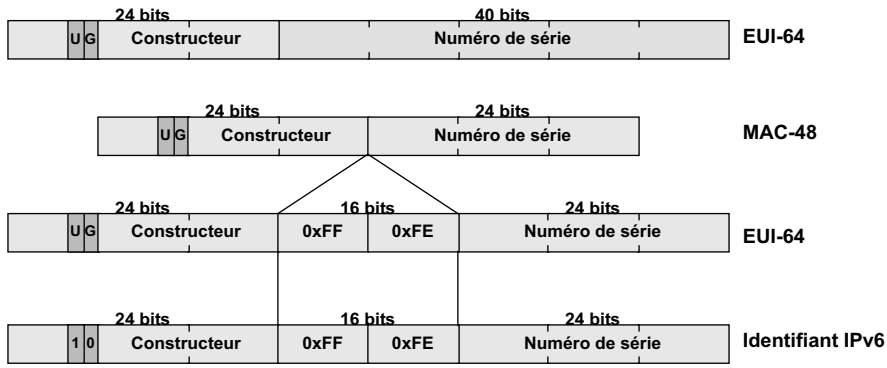


Figure 8.31 La construction de l'identifiant IPv6 à partir de l'adresse MAC.

Lorsqu'une interface n'est dotée d'aucun identifiant, l'administrateur local peut lui attribuer un identifiant, le bit U[12] est alors positionné à 0.

Les adresses spécifiques

Comme dans IPv4 certaines adresses ont une signification particulière :

- L'adresse dite indéterminée (*Unspecified address*), correspondant à l'adresse 0.0.0.0 d'IPv4, elle désigne une interface en cours d'initialisation. Cette adresse 0:0:0:0:0:0:0:0 ou :: ne doit jamais être attribuée à une interface.
- L'adresse de bouclage (*Loopback address*) correspond à l'adresse 127.0.0.1 d'IPv4, elle vaut 0:0:0:0:0:0:0:1 ou encore ::1.

Les adresses dites de site local

Les adresses de site local (FEC0::/10) correspondent aux adresses privées d'IPv4 (RFC 1918, adresses de type 10.0.0.0). À l'instar d'IPv4, ces adresses ont une portée limitée au réseau privé, elles ne peuvent être utilisées pour se connecter à Internet (figure 8.32). Le champ **SLA_id** (*Site Level Aggregator*) correspondant au champ Subnet_ID d'IPv4 permet à l'administrateur local de hiérarchiser son réseau.

12. La signification du bit U est inversée par rapport à celle du bit U/L utilisée dans l'adressage MAC-48.

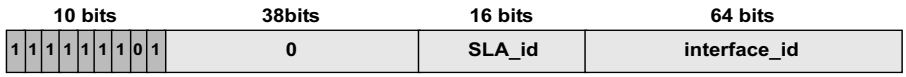


Figure 8.32 L'adressage de site local (adressage privé).

Le plan d'adressage agrégé

L'adressage agrégé se présente comme étant un compromis entre un adressage hiérarchique strict et un adressage à plat. Il instaure une hiérarchie vis-à-vis des fournisseurs d'accès. Le premier niveau de hiérarchisation (**TLA_id**, *Top Level Aggregator*) sur 13 bits correspond à l'identification du fournisseur d'accès de transit à Internet. Le champ suivant sur 24 bits (**NLA_id**, *Next Level Aggregator*) est un champ d'agrégation dont le découpage est défini par l'autorité désignée dans le champ précédent. La dernière partie champ du NLA désigne le site local connecté au fournisseur d'accès. Le dernier champ d'agrégation (**SLA_id**, *Site Level Aggregator*) sur 16 bits permet au gestionnaire du site de hiérarchiser son plan d'adressage. Devant la difficulté de dimensionner les champs TLA et NLA, un champ de 8 bits a été prévu pour permettre le débordement à droite (TLA) ou à gauche (NLA) des champs TLA et NLA. La figure 8.33 représente ce type d'adresse.

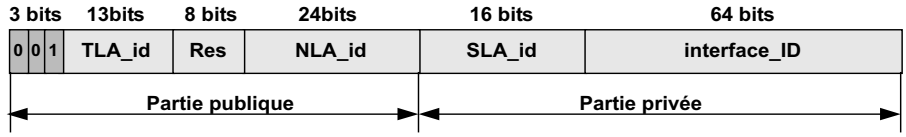


Figure 8.33 L'adressage agrégé.

L'adressage multicast

Afin d'éviter l'usage intempestif de *broadcast* qui pénalise les performances, IPv6 a généralisé la notion de *multicast* en définissant différents niveaux de diffusion. Une adresse *multicast* désigne un ensemble de nœuds, elle est dite aussi adresse sur abonnement. L'adresse *multicast* comporte quatre champs (figure 8.34), le premier identifie une adresse de *multicast* (préfixe FF00::/8). Le second, le champ flags, est un champ de bits (4 bits) dont seul le dernier est défini, il s'agit du bit T. Ce bit, lorsqu'il est à « 0 », indique que l'adresse est permanente. Le champ suivant indique le niveau de diffusion (*scope*). Les différentes valeurs de ce champ sont :

– 0, réservé ;
– 1, nœud local ;
– 2, lien local ;
– 5, site local ;
– 8, l'organisation locale ;
– E, global.

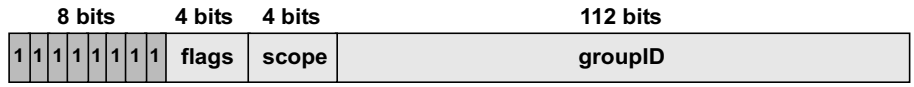


Figure 8.34 L'adressage multicast.

© Dunod – La photocopie non autorisée est un délit

Certaines adresses *multicast* ont été prédéfinies, ce sont notamment les adresses de diffusion des protocoles de routage. Chaque protocole de routage possède sa propre adresse.

L'adressage d'anycast

Concrètement, une adresse *anycast* résulte de la concaténation d'un préfixe désignant le sous-réseau adressé et d'un suffixe nul (figure 8.35). En principe, actuellement une adresse *anycast* ne peut être attribuée qu'à une passerelle.

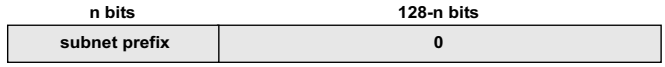


Figure 8.35 L'adressage d'anycast.

8.4.4 L'adressage de transition d'IPv4 vers IPv6

La migration d'IPv4 vers IPv6 ne peut être réalisée que progressivement. Durant un temps assez important, les deux versions de protocoles devront cohabiter. Aussi, deux solutions ont été envisagées pour permettre d'utiliser les adresses IPv4 dans le domaine IPv6. La première (figure 8.36) dite IPv4 mappée est une représentation interne des adresses afin de permettre à des programmes IPv6 de fonctionner sur un réseau IPv4, la communication se faisant d'une machine IPv4 à IPv4.

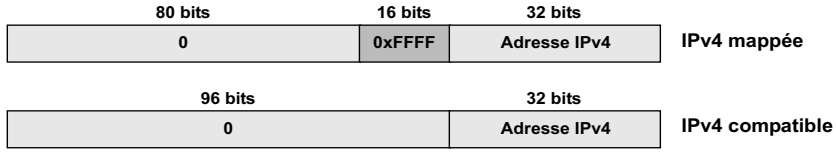


Figure 8.36 L'adressage IPv4/IPv6.

La seconde dite IPv4 compatible, permet à deux machines IPv6 de communiquer à travers un réseau IPv4 (tunnel IPv4). Le datagramme IPv6 d'adresse « ::a.b.c.d » est encapsulé dans un datagramme IPv4 d'adresse « a.b.c.d » (figure 8.36).

8.5 CONCLUSION

Défini pour répondre à un besoin précis, TCP/IP n'a été conçu que pour satisfaire les besoins de l'armée américaine, de ce fait il a bénéficié d'une approche très pragmatique. Si cette approche en limite les possibilités, elle autorise aussi les évolutions. Aujourd'hui TCP/IP, bien que conçu pour des applications en mode texte, a su s'adapter pour répondre aux transferts de flux multimédia.

EXERCICES

Exercice 8.1 Masque de sous-réseau

Une entreprise à succursales multiples utilise l'adresse IP 196.179.110.0. Pour une gestion plus fine de ses sous-réseaux, le responsable informatique désire pouvoir affecter une adresse IP propre à chaque sous-réseau des dix succursales.

1. De quelle classe d'adressage s'agit-il ?
2. Donnez et expliquez la valeur du masque de sous-réseau correspondant à ce besoin.
3. Combien de machines chaque sous-réseau pourra-t-il comporter et pourquoi ?
4. Définissez l'adresse de *broadcast* du sous-réseau 3 (expliquez) ?

Exercice 8.2 Masque de sous-réseau et dysfonctionnement

Certains utilisateurs du réseau local d'une entreprise, utilisant une application au-dessus de UDP, se plaignent de ne pas pouvoir communiquer avec tous les autres utilisateurs alors que ceux-ci le peuvent avec eux. Le responsable bureautique local vous demande d'expertiser son réseau. Pour lui, le fait qu'une station puisse émettre des messages vers une autre et que cette dernière ne puisse répondre le laisse perplexe.

Vous constatez que toutes les stations sont sur le même segment Ethernet et que celui-ci ne comporte aucun routeur et qu'aucune station n'est configurée pour remplir ce rôle.

Vous relevez les configurations suivantes :

- Station A @ 150.150.1.28 masque 255.255.255.0
- Station B @ 150.150.1.57 masque 255.255.0.0
- Station C @ 150.150.2.28 masque 255.255.255.0
- Station D @ 150.150.2.57 masque 255.255.0.0

Vous établissez la matrice de communication suivante.

Complétez la figure 8.37 par oui lorsque la communication est possible et par non dans le cas contraire.

Source Destination	150.150.1.28 (255.255.255.0)	150.150.1.57 (255.255.0.0)	150.150.2.28 (255.255.255.0)	150.150.2.57 (255.255.0.0)
150.150.1.28				
150.150.1.57				
150.150.2.28				
150.150.2.57				

Figure 8.37 La matrice de communication.

© Dunod – La photocopie non autorisée est un délit

Exercice 8.3 Masque de sous-réseau variable

Une entreprise dispose d'une seule adresse de classe C 194.28.32.0 pour identifier ses trois sous-réseaux. Sachant que deux des réseaux comportent 25 machines et le troisième 52 machines, établissez le plan d'adressage (masque de sous-réseau) de cette entreprise. Deux solutions sont envisageables, lesquelles ?

Chapitre **9**

L'architecture TCP/IP et le niveau liaison

9.1 GÉNÉRALITÉS

Le protocole IP a pour objectif de masquer, aux applications, les sous-réseaux réels physiques. Ces sous-réseaux fournissent donc à IP un service assimilable à celui offert par le niveau 2 de l'architecture OSI. Cette approche évidemment non conforme au modèle de référence décline les services de niveau 2 en trois catégories dont la finalité reste la même, mettre en relation deux entités IP (figure 9.1) :

– un service de niveau 2 basé sur des réseaux sans diffusion (réseaux X.25, Frame Relay ou ATM) ;
– un service de niveau 2 offert par les réseaux locaux ;
– enfin, un service de niveau 2 s'appuyant sur des liaisons spécialisées en mode point à point entre équipements IP d'un réseau dit alors réseau IP (protocole de liaison comme **SLIP**, *Serial Link Internet Protocol*, et **PPP**, *Point to Point Protocol*).

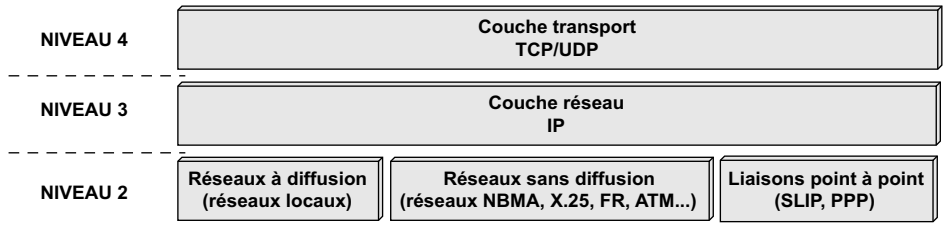


Figure 9.1 IP et les services de niveaux 2.

9.2 LES PROTOCOLES DE LIAISON (POINT À POINT)

9.2.1 Généralités

Bien que défini à l'origine pour s'appuyer sur des réseaux physiques existants, très vite la nécessité de réaliser des réseaux tout IP a conduit au développement de protocoles de niveau 2. En effet, IP n'assurant pas un service de délimitation des données, les datagrammes IP ne peuvent être émis directement sur une liaison série. La délimitation des données reste le rôle de base des protocoles de liaison (figure 9.2).

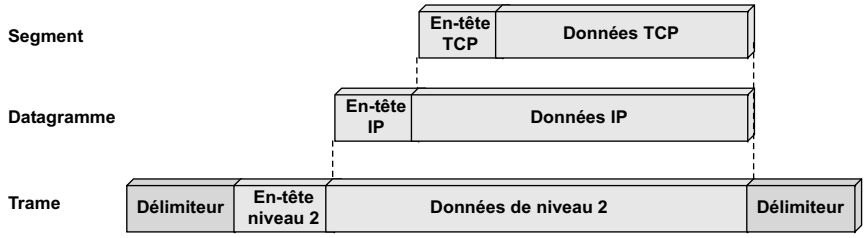


Figure 9.2 La délimitation des blocs de données.

Deux protocoles de liaison ont été spécifiés : **SLIP** (*Serial Line IP*) et **PPP** (*Point-to-Point Protocol*), le premier n'est utilisé que dans des liaisons point à point locales, car il suppose une ligne fiable, le second est mis en œuvre sur des liaisons point à point pour réaliser des réseaux tout IP et sur les liaisons d'accès aux réseaux WAN.

9.2.2 SLIP, *Serial Line Internet Protocol* (RFC 1055)

SLIP est un protocole asynchrone orienté bloc. Très simple, il n'effectue que la délimitation de trames. En fait, SLIP se contente d'émettre les données (datagramme) et signale au récepteur la fin du message par l'émission d'un caractère de délimitation (END, 0xC0). N'indiquant que la fin d'un datagramme, SLIP est susceptible d'introduire une confusion entre le bruit de ligne et les données effectives. Afin d'assurer une bonne délimitation du datagramme, la plupart des implémentations précèdent l'émission de données du caractère « END ».

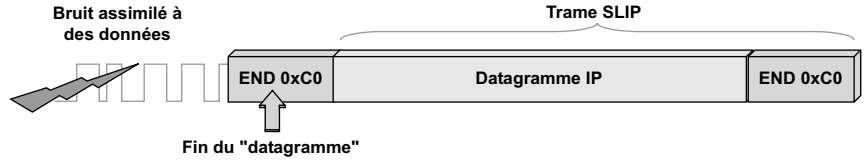


Figure 9.3 Le format de la trame SLIP.

Dans la figure 9.3, le bruit de ligne est assimilé à des données par le récepteur. L'émission d'un caractère END, avant l'émission du datagramme IP, marque la fin du « datagramme bruit ». Le datagramme réel est donc bien délimité. Le « datagramme bruit » sera éliminé par le contrôle d'erreur des couches supérieures. Si aucun caractère de délimitation n'avait précédé le datagramme réel, l'ensemble bruit et données du datagramme aurait constitué un bloc erroné et par conséquent aurait été rejeté par les couches supérieures. De ce fait, en l'absence de délimiteur de début, le bruit peut empêcher toute transmission valide.

Le caractère END (192D ou 0xC0) est donc utilisé comme délimiteur de début et de fin. Un caractère END dans le champ de données ne doit pas être interprété comme un délimiteur mais bien comme un octet de donnée. SLIP assure la transparence en remplaçant le caractère END par la séquence ESC_SLIP[1], ESC_END soit 0xDB, 0xDC. Le caractère d'échappement (ESC_SLIP) est lui-même protégé par l'insertion de la séquence ESC_SLIP, ESC_ESC soit les valeurs 0xDB, 0xDD. La figure 9.4 illustre ce mécanisme.

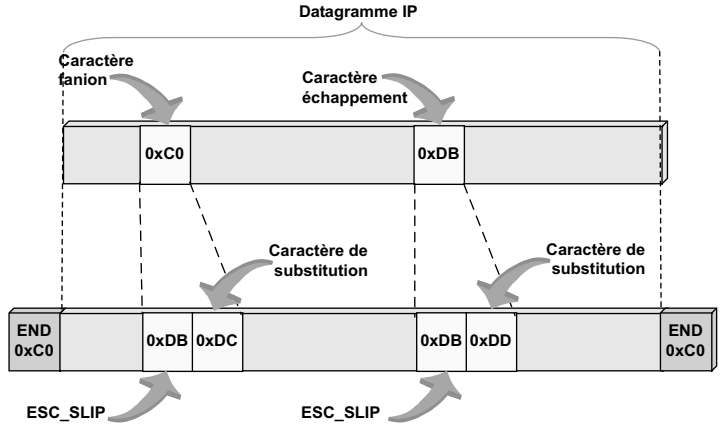


Figure 9.4 Le mécanisme de la transparence dans SLIP.

Les liaisons de type Terminal/Calculateur constituent l'utilisation la plus fréquente de SLIP. Ces liaisons sont généralement à bas débit et les applications mises en œuvre de type interactif (Telnet, RLogin) ; compte tenu du débit et du volume des données protocolaires par rapport aux données utiles (rapport 1/40 en Telnet), SLIP est peu efficace. Aussi, une version dite **CSLIP** (*Compressed SLIP*) a-t-elle été définie. CSLIP (RFC 1144) met en œuvre une technique de compression d'en-tête dite Jacobson du nom de son auteur, cette compression réduit les données protocolaires à 3 ou 5 octets. La compression Jacobson est fondée sur le constat que les données d'en-tête ne varient que peu entre deux datagrammes consécutifs, l'en-tête du datagramme ne contient alors que des informations sur la différence entre l'en-tête précédent et la présente avant compression.

9.2.3 PPP, *Point to Point Protocol* (RFC 1548 et 1661, 1662)

Généralités

Si SLIP doit son succès à sa simplicité, il souffre de nombreuses insuffisances qui en limitent l'emploi :

– SLIP réalise une encapsulation simple, il ne comporte aucune information sur le protocole transporté. De ce fait, il ne peut, sur une même liaison, assurer le transport que d'un seul protocole (IP). Si cette lacune est sans importance sur une liaison Terminal/Calculateur, elle devient une contrainte forte sur une liaison d'interconnexion de systèmes où plusieurs protocoles peuvent être utilisés simultanément.

1. Le caractère d'échappement utilisé par le protocole SLIP est différent du caractère d'échappement du code ASCII. Pour le distinguer, nous le noterons ESC_SLIP, de même celui utilisé par le protocole PPP sera noté ESC_PPP.

© Dunod – La photocopie non autorisée est un délit

– SLIP ne met en œuvre aucun mécanisme de contrôle d'erreur et de séquencement, il suppose que la liaison est fiable. Ce qui est généralement le cas sur des liaisons de faible longueur (Terminal/Calculateur), mais non sur des liaisons d'accès à un WAN ou entre éléments actifs d'un réseau WAN.
– SLIP suppose une liaison permanente et sûre, il ne prévoit aucun mécanisme d'authentification, alors que lors de connexions dites *Dial-Up* (connexions temporaires), il est généralement nécessaire d'assurer l'authentification de la partie appelante et de lui affecter temporairement une adresse IP.

PPP, protocole de liaison point à point, apporte une solution à ces différents problèmes. Il définit un format d'encapsulation dérivé d'HDLC et comporte un ensemble de protocoles pour :

– le transport de données (PPP proprement dit) ;
– la négociation des paramètres de liaison (**LCP**, *Link Control Protocol*) ;
– l'authentification (**PAP**, *PPP Authentification Protocol* et **CHAP**, *Challenge Handshake Authentification Protocol*) ;
– l'obtention des paramètres de configuration de niveau 3 par une famille de protocoles de contrôle de réseau (**NCP**, *Network Control Protocol*).

L'encapsulation PPP

➤ Le format de base

L'encapsulation PPP est une encapsulation à 2 niveaux. Le niveau inférieur, souvent désigné « encapsulation HDLC » est similaire au format de la trame HDLC. Cependant, la présence de tous les champs n'étant pas toujours nécessaire, une négociation préalable entre les entités communicantes autorise un format allégé. L'encapsulation de deuxième niveau permet de distinguer le transport de données applicatives de celles des protocoles complémentaires composant PPP. La figure 9.5 représente le format d'encapsulation générique de PPP.

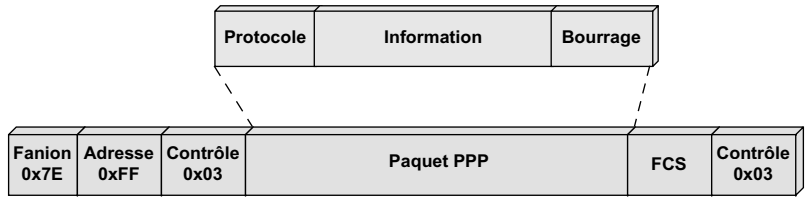


Figure 9.5 Le format générique de la trame PPP.

Hors le champ de donnée qui encapsule le datagramme IP, les différents champs de la trame PPP sont (figure 9.5) :

– Le champ **Adresse,** inutile sur une liaison point à point, sa valeur est constante et fixée à 0xFF.
– Le champ **Contrôle** qui a la même signification qu'en HDLC. Si la liaison est fiable, aucun contrôle de séquencement n'est utile (fenêtrage), PPP utilise une trame HDLC « UI » (Trame d'information non numérotée), le champ Commande vaut alors 0x03. Dans ce cas, les champs adresse et contrôle sont inutiles, ils peuvent être omis dans les trames émises (négociation LCP à la connexion).

– Le champ **Protocole**, sur deux octets, qui identifie le protocole de niveau supérieur. Il peut, lors de la connexion, être négocié à un octet. La figure 9.6 fournit quelques exemples de valeurs du champ Protocole.
– Enfin, le champ **FCS** (*Frame Check Sequence*) qui permet la détection d'erreur, son mode de calcul est identique à celui de HDLC.

Valeurs	Protocoles
0x0021	IP
0x002B	IPX
0x002D	TCP/IP (en-têtes compressés, Van Jaco bson)
0x002F	TCP/IP (en-têtes non compressés)
0x800F	IPv6
	Protocoles complémentaires de PPP
0xC021	LCP (Link Control Protocol)
0xC023	PAP (Password Authentification Protocol)
0xC223	CHAP (Challenge Handshake Protocol)

Figure 9.6 Les exemples de valeurs du champ Protocole de PPP.

L'une des particularités de PPP est d'avoir été dès l'origine imaginé pour fonctionner aussi bien sur une liaison asynchrone[2] que sur une liaison synchrone.

Lorsque le protocole est utilisé sur une liaison synchrone, la transparence au fanion est assurée de manière similaire à HDLC (insertion d'un bit à 0 tous les 5 bits à 1, technique dite du *bit stuffing*). S'il est utilisé sur une liaison asynchrone, la transparence au fanion (0x7E) est réalisée de manière similaire à celle du protocole SLIP. C'est-à-dire (figure 9.7) que le fanion, présent dans le champ de données, est remplacé par la séquence : ESC_PPP, ESC_FLAG soit les valeurs 0x7D, 0x5E. De même, le caractère d'échappement (ESC_PPP, 0x7D) est remplacé par la séquence : ESC_PPP, ESC_ESC soit 0x7D, 0x5D.

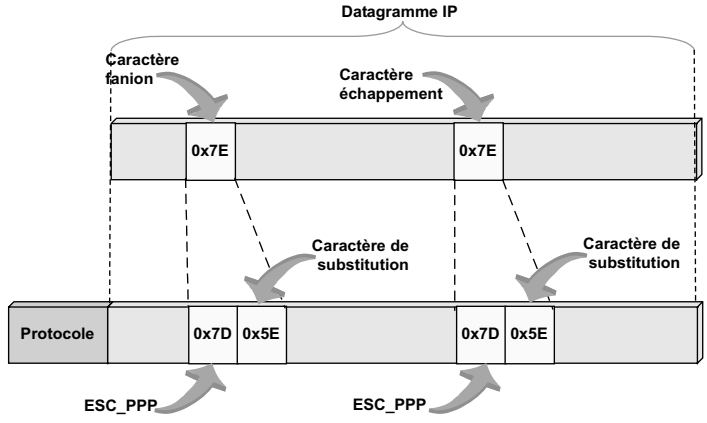


Figure 9.7 Le mécanisme de la transparence dans SLIP.

2. Les micro-ordinateurs sont équipés d'origine d'une interface asynchrone.

© Dunod – La photocopie non autorisée est un délit

Certains modems utilisent les 32 premiers caractères du code ASCII comme caractères de commande pour éviter que ces caractères ne soient considérés par les modems comme une commande, ils seront, à l'instar du mécanisme de transparence aux fanions, remplacés par des séquences de caractères spécifiques. Les caractères dont la transparence doit être assurée sont indiqués à la connexion lors de l'exécution du protocole LCP (table **ACCM**, *Asynchronous Control Character Map*). La transparence de ces caractères est obtenue par la séquence ESC_PPP, ESC_Commande où la valeur de ESC_Commande est la valeur ASCII de la commande avec le sixième bit complémenté (inversé). La figure 9.8 illustre ce mécanisme, elle fournit les valeurs des caractères masqués et la table ACCM correspondant.

Commande	Rang ASCII	Valeur ASCII Hex	Binaire	
ETX	4	0x03	0000	0011
ETX masqué		0x23	0010	0011
ACK	7	0x06	0000	0110
ACK masqué		0x26	0010	0110

Table ACCM correspondant au masquage des caractères de rang 4 et 7 :

0000 0000 0000 0000 0000 0000 0100 1000 soit 0x00000048

Figure 9.8 Le mécanisme de masquage de caractères PPP.

Par défaut, en mode asynchrone la table ACCM vaut 0xFFFFFFFF et en mode synchrone 0x00000000.

L'établissement d'une session PPP (figure 9.9) se déroule en trois phases, établissement du niveau liaison, authentification des extrémités (facultatif) et enfin négociation des paramètres du protocole réseau.

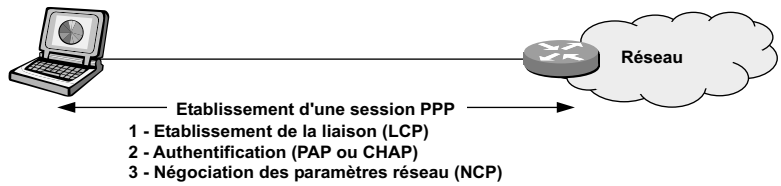


Figure 9.9 Établissement d'une session PPP.

LCP, Link Control Protocol

Lors de l'initialisation d'un transfert, chaque extrémité de la connexion entreprend une procédure de négociation des paramètres de l'échange par l'intermédiaire du protocole **LCP** (*Link Control Protocol*). La figure 9.10 illustre le format de la trame LCP transportée dans la trame PPP.

Le protocole LCP est identifié dans la trame PPP par le code **Protocole_ID** = « 0xC021 » (figure 9.10), le champ **Code** précise le type de trame (figure 9.11), le champ **Identification** permet d'associer une requête à une réponse tandis que le champ **Longueur** permet de distinguer les données d'un éventuel bourrage. Les options LCP sont codées : **type** d'option, **longueur** du champ valeur et **valeur** des données de l'option (figure 9.13).

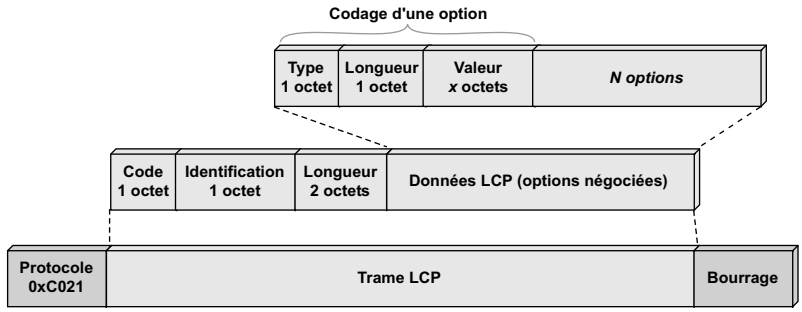


Figure 9.10 La trame LCP.

Type de trame	Code	Utilisation
Configure_Request	1	Trame de négociation, le champ données comprend la liste des options proposées lorsque la valeur désirée est différente de la valeur par défaut.
Configure_Ack	2	Trame d'acceptation des options proposées par la trame Configure_Request.
Configure_Nack	3	Trame d'acceptation des options négociées, mais pas des valeurs indiquées. L'émetteur doit proposer de nouvelles valeurs.
Configure_Reject	4	Trame de refus des options, le champ données indique les valeurs des options non négociables. L'émetteur reformule une requête de configuration avec les valeurs indiquées dans la trame de rejet.
Terminate_Request	5	Cette trame met fin à une connexion.
Terminate_Ack	6	Acquittement d'une fin de connexion.
Code_Reject	7	Trame utilisée pour indiquer à l'émetteur que le récepteur ignore une option, ceci signifie que les deux extrémités utilisent une version différente de PPP.
Protocol_Reject	8	Trame de gestion, indiquant que la valeur du champ Protocole de la trame PPP est inconnue.

Figure 9.11 Exemple de trames LCP.

La figure 9.12 illustre les différentes phases d'un échange. Dès que la liaison est établie, chaque entité négocie à son tour ses propres options, la liaison n'est pas nécessairement symétrique. L'échange débute par la trame Configure_Request, le champ données contient les modifications à apporter aux valeurs par défaut (négociation des options). Si ces valeurs sont acceptées par le récepteur, celui-ci répond par la trame Configure_Ack. Si les valeurs ne conviennent pas au récepteur, celui-ci peut demander à la source de lui proposer d'autres valeurs (Configure_Nack) ou lui indiquer que les valeurs ne sont pas négociables (Configure_Reject).

La figure 9.13 présente quelques options négociables par LCP. Le champ données de la trame LCP contient autant de triplet « Type option, longueur du champ Valeur, Valeur proposée » que d'options négociées. La longueur totale du champ données est fournie par le champ longueur de la trame LCP.

La MTU (*Maximum Transfer Unit*) définit la capacité d'emport du niveau 2. Pour tenir compte de la taille du champ Protocole, il est nécessaire de définir une valeur de charge utile vue du niveau réseau : le **MRU** ou *Maximum Receipt Unit*, taille maximale du segment admis en réception, valeur par défaut 1 500 octets. La figure 9.14 illustre la relation entre MTU et MRU.

© Dunod – La photocopie non autorisée est un délit

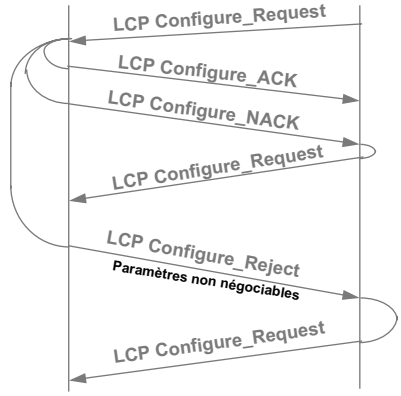


Figure 9.12 Les phases d'initialisation de PPP.

Code Option	Fonction	Longueur	Signification
1	MRU	4	**MRU**, *Maximum Receipt Unit* ; valeur par défaut 1 500 octets.
2	ACCM	6	**ACCM**, *Asynchronous Control Character Map* ; table de 4 octets ;
3	Authentification	6	Indique sur 2 octets le protocole de sécurisation utilisé (valeur du champ protocole de PPP) soit 0xC023 pour PAP et 0xC223 pour CHAP.
5	Nombre magique	6	Déterminée aléatoirement par chaque extrémité, cette valeur sur 4 octets permet d'identifier l'origine du message et de détecter les boucles (réception par une entité de ce qu'elle a émis).
7	Compression	2	Codage du champ Protocole de PPP sur un octet.
8	Compression	2	Suppression des champs Adresse et Commande de la trame PPP.
13	Rappel automatique	$\geqslant 3$	Option de sécurité, cette option non seulement permet l'identification de l'appelant par son rappel mais aussi la prise en compte du coût des communications par le serveur appelé initialement.

Figure 9.13 Les exemples d'options LCP.

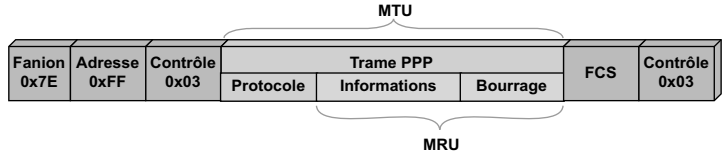


Figure 9.14 La relation e ntre MTU et MRU.

La sécurisation des échanges

Le protocole PPP est utilisé en point à point sur des liaisons permanentes, mais aussi sur des liens temporaires comme, par exemple, une connexion à Internet *via* le réseau téléphonique. De ce fait, l'entité appelée doit pouvoir identifier et authentifier l'appelant avant d'accepter une connexion, c'est le rôle des deux protocoles de sécurisation de PPP qui sont PAP et CHAP.

➤ Le protocole PAP, *PPP Authentification Protocol*

Le protocole PAP échange en clair sur le réseau l'identifiant et le mot de passe de l'appelant. L'échange n'a pour objet que de valider la connexion, ce n'est pas une phase dite de « login » sur un serveur ou une application distante. Éventuellement cette phase pourra être exigée par le processus distant appelé. La figure 9.15 illustre cet échange.

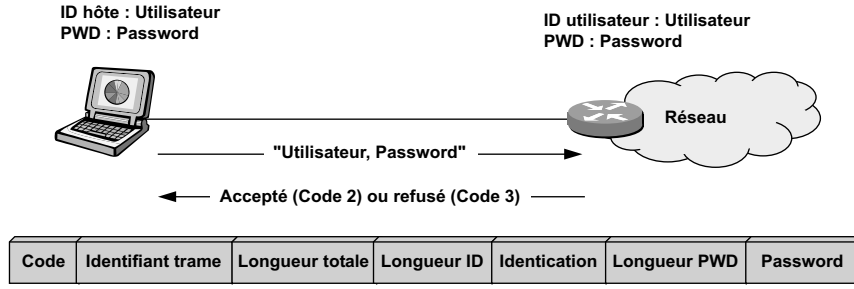


Figure 9.15 L'échange d'identification sous PAP et le format de la trame.

PAP met en œuvre trois types de trame (figure 9.14) identifiés par le champ Code :

– 1, Authentification_Request ;
– 2, Authentification_Ack ;
– 3, Authentification_Nack.

Le champ identifiant trame permet d'associer une requête à sa réponse. Les champs suivants contiennent l'identifiant et le mot de passe de l'extrémité qui s'authentifie. Ces champs, de longueur variable, sont précédés d'une information de longueur. En cas d'échec l'authentification est renouvelée, après *n* échecs l'établissement de la liaison est refusé.

➤ Le protocole CHAP, *Challenge Handshake Authentification Protocol*

PAP n'est pas un protocole d'authentification fiable. Les mots de passe ne sont échangés qu'une seule fois en début de session et circulent en clair sur le réseau. CHAP est utilisé dès la connexion pour authentifier celle-ci, puis périodiquement pour s'assurer qu'il n'y a pas eu substitution de correspondant. Le protocole CHAP est un protocole en trois temps (figure 9.16). Après l'établissement du lien, l'appelé envoie un message de test à l'appelant (*Challenge*). Ce dernier chiffre le contenu du message de test et le renvoie. L'expéditeur compare la réponse avec sa propre valeur. Si le résultat coïncide, l'authentification est acceptée, dans le cas inverse la liaison est rompue.

Plusieurs fonctions d'authentification pouvant être mis en œuvre, l'algorithme de chiffrement est précisé lors de la négociation LCP. La trame de négociation LCP est illustrée en figure 9.17. Le champ « Type » contient la valeur 3 (négociation du protocole d'authentification), Le champ Longueur contient la valeur 5, le champ « Protocole » indique que l'authentification demandée est CHAP (valeur 0xC223), enfin l'algorithme indiqué ici est le MD5 (valeur 5).

© Dunod – La photocopie non autorisée est un délit

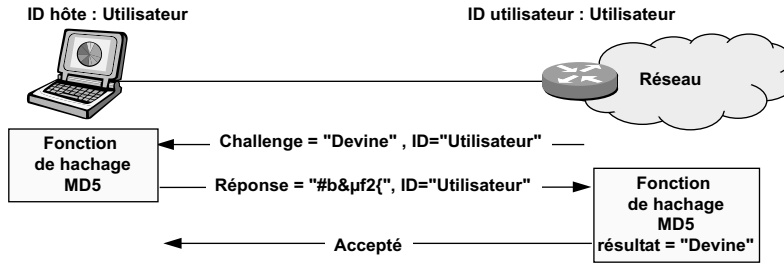


Figure 9.16 Principe de l'authentification en trois temps.

Code option Type = 3	Longueur L = 5	Protocole = 0xC223 (CHAP)	Algorithme = 5 (MD5)

Figure 9.17 Le format de la négociation de l'option CHAP.

CHAP utilise deux formats de paquets, l'un correspond à l'échange des données du challenge, le second à l'indication du résultat de celui-ci. La figure 9.18 illustre le format de ces paquets. Le champ **Code** indique le type de message CHAP (1, *Challenge* ; 2, *Response* – Réponse – ; 3, *Success* – Succès – ; 4, *Failure* – Échec –). Le champ **Identification** permet d'associer un message challenge à la réponse correspondante. Cette valeur est différente pour chaque challenge réalisé. Le champ **Longueur** indique la longueur totale du champ données. La taille du challenge ou de la réponse est fournie par le champ **Taille**. Le champ **Valeur** contient, suivant le type de message le challenge ou la réponse. Le champ **Nom** identifie les correspondants. Dans les messages *success* ou *failure*, le champ **Message** peut contenir une chaîne ASCII prédéfinie.

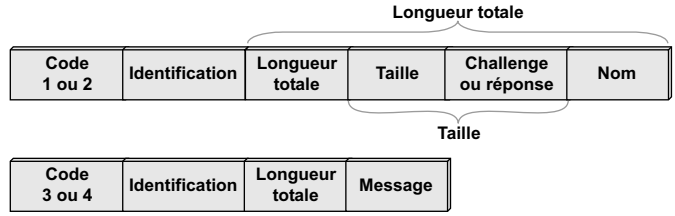


Figure 9.18 Le format des paquets CHAP.

Afin que l'accès aux données enregistrées soit limité, le dialogue CHAP doit être un dialogue d'extrémité, c'est-à-dire entre client et serveur.

Le protocole NCP, Network Control Protocol

➤ Généralités

Le protocole NCP est utilisé pour définir les paramètres du niveau réseau. PPP pouvant être interfacé à divers protocoles de niveau 3, NCP est constitué d'un ensemble de protocoles spécifiques à chaque protocole de niveau 3 :

– IPCP (IP *Configuration Protocol*) pour IP (RFC 1332) ;
– IPXCP (*IPX Configuration Protocol*) pour IPX (RFC 1552) ;
– ATCP (*AppleTalk Control Protocol*, RFC 1378)...

Le protocole IPCP est encapsulé dans une trame PPP (protocole=0x8021), il utilise le même format de trames que celui de LCP, type de trame 1 à 7 (figure 9.10). Le codage du champ Option dépend de l'option invoquée :

– 1, négociation des adresses IP (obsolète) ;
– 2, protocole de compression ;
– 3, négociation de l'adresse IP de l'équipement terminal.

➤ Le protocole de compression

Les en-têtes IP et TCP occupent une part non négligeable des données émises (40 octets, hors option). À l'instar de CSLIP, il peut donc être intéressant, lors de l'envoi de petits paquets, de procéder à une réduction de volume des en-têtes, c'est ce que propose la compression Van Jacobson (RFC 1144). Partant du principe que, sur une même connexion TCP, peu de données d'en-tête changent d'un datagramme à l'autre, la compression Van Jacobson ne transmet que la différence entre deux en-têtes successifs, réduisant ainsi l'en-tête à quelques octets. Chaque extrémité du lien doit, si elle le désire invoquer cette option.

➤ La négociation d'adresse IP de l'équipement terminal

Cette option de configuration fournit les moyens de négocier une adresse IP. Le lien local peut informer le distant de l'adresse IP qu'il souhaite utiliser. Le distant peut accepter ou refuser en fournissant alors au local une adresse IP valide. De même, le local peut directement demander une adresse IP à l'hôte distant. La figure 9.19 illustre le scénario complet d'une connexion PPP.

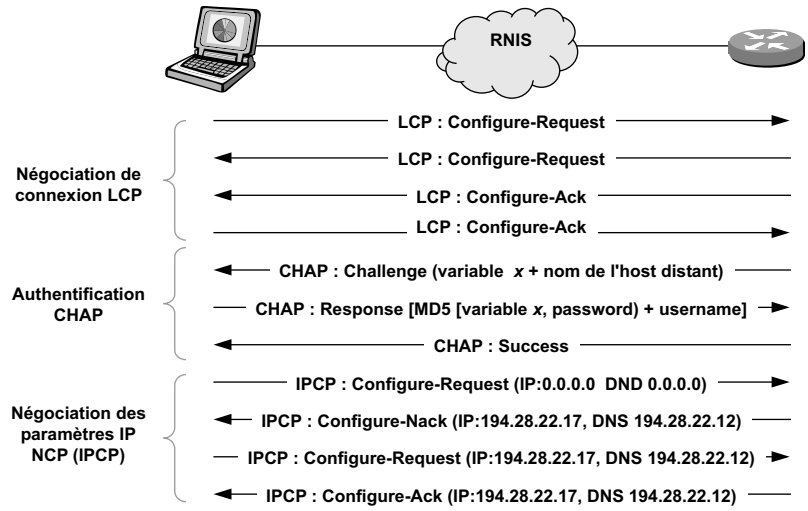


Figure 9.19 Les phases d'établissement d'une connexion PPP.

L'entité qui demande l'attribution d'une adresse IP émet sa requête avec le champ Adresse IP à zéro.

© Dunod – La photocopie non autorisée est un délit

MLPPP

L'accès à un réseau distant peut utiliser une ligne unique (**SLP**, *Simple Link Protocol*) ou agréger plusieurs lignes à bas débit pour obtenir une liaison haut débit. Ce procédé similaire au multiplexage inverse nécessite une adaptation du protocole de liaison. Le protocole multiligne (**MLP**, *Multi Link Protocol*, RFC 1990) fragmente le datagramme IP, transmet les différents fragments sur plusieurs lignes et assure le réassemblage. MLPPP peut aussi être utilisé pour répartir la charge sur plusieurs liens, il est transparent pour le protocole de niveau réseau[3]. Le principe de MLPPP est illustré figure 9.20.

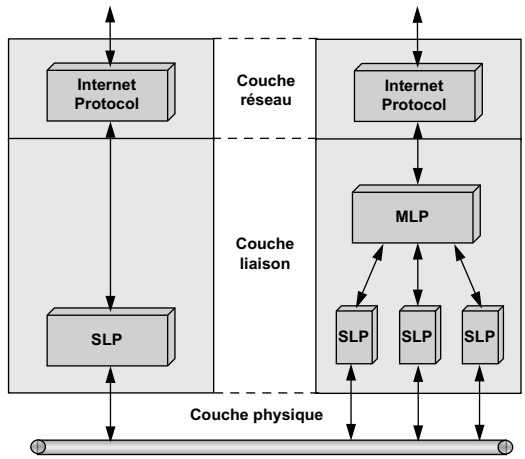


Figure 9.20 Principe général des liaisons SLP et MLP.

Le niveau MLP agit en multiplexeur et démultiplexeur des données. La capacité de réassemblage **MRRU** (*Max Receive Reconstructed Unit*) est négociée par LCP (type d'option 17). Le format des unités de données MLPPP est illustré en figure 9.21.

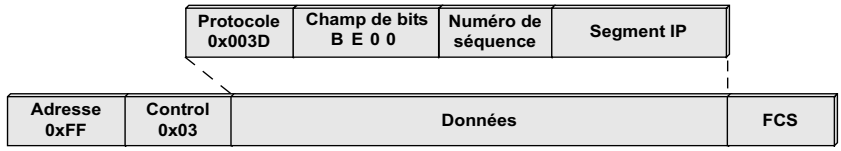


Figure 9.21 Le format de la trame MLPPP.

Le champ Protocole de la trame PPP de la figure 9.21 identifie MLPPP (0x003D). Le champ suivant sur 4 bits ou 8 bits, selon la taille du champ Numéro de séquence, gèrent sur la liaison la fragmentation. Le bit B (*Beginning*) est positionné à 1 dans le premier fragment, de même le bit E (*Ending*) vaut 1 dans le dernier fragment. Si un datagramme n'a fait l'objet d'aucune fragmentation, les bits B et E sont tous les deux à 1. Le champ Numéro de séquence de 12 bits (4 bits du quartet de poids faible de l'octet précédent + 8) ou 24 bits indique la position du fragment dans le datagramme d'origine.

3. Il ne faut pas confondre, l'accès multiligne qui utilise simultanément plusieurs voies physiques pour accéder au réseau avec l'accès multivoie des réseaux en mode connecté qui, sur une même liaison physique, autorise plusieurs communications simultanées (multiplexage des circuits virtuels).

Les tunnels PPP

Initialement conçu pour être utilisé sur des liens point à point, PPP est rapidement devenu le protocole d'accès à un réseau et notamment au réseau des réseaux, c'est-à-dire à Internet. Avec l'arrivée des connexions à haut débit (***x*DSL**, *x Digital Subscriber Line*[4]), les fournisseurs d'accès ont dû s'équiper d'équipements capables de gérer ces nouvelles connexions. Les **BAS** (*Broadband Access Server*) assurent cette fonction. La connexion entre l'usager et le point d'accès au réseau de l'opérateur (**PoP**, *Point of Presence*) est réalisée, selon le type d'accès, par une adaptation du protocole PPP. L'accès peut alors être réalisé *via* un circuit virtuel ATM (*Asynchronous Transfer Mode*) entre l'abonné et le BAS : PPPoA (PPP over ATM, RFC 2364).

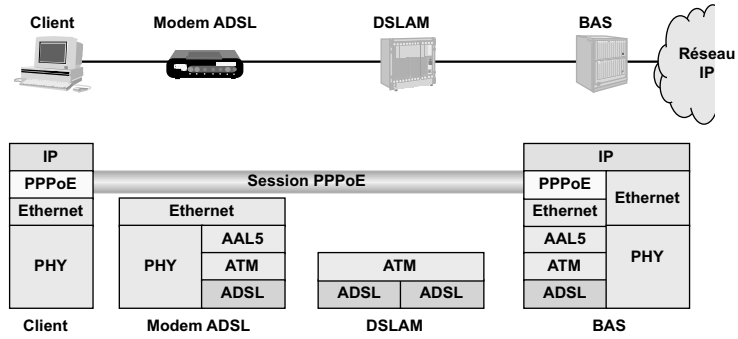


Figure 9.22 Principe d'un accès haut débit à Internet.

Ce mode d'accès a été amélioré en établissant entre le poste client final et le BAS un lien de type Ethernet (PPPoE, PPP *over* Ethernet, RFC 2516). Dans ce mode de fonctionnement (figure 9.22), les données IP sont encapsulées dans une trame PPP, elle-même encapsulée dans une trame Ethernet puis dans des cellules ATM (AAL5). Ce mode de fonctionnement simule un pont entre le réseau Internet et le client, il autorise l'utilisation d'une pile protocolaire IP standard et surtout permet de raccorder plusieurs terminaux sur une même connexion.

© Dunod – La photocopie non autorisée est un délit

4. x, indique le type de technique DSL mise en œuvre.

EXERCICE

Exercice 9.1 Table ACCM (*Asynchronous Control Character Map*)

Lorsque le protocole PPP (*Point to Point Protocol*) est utilisé sur une liaison synchrone, la transparence au fanion est assurée de manière similaire à HDLC (*bit stuffing*). S'il est utilisé sur une liaison asynchrone la transparence au fanion (0x7E) est réalisée de manière similaire à celle du protocole SLIP. C'est-à-dire que le **fanion** présent dans le champ de données est remplacé par la séquence : ESC_PPP, ESC_FLAG (0x7D, 0x5E). Le caractère d'échappement (ESC_PPP ou 0x7D) est lui-même remplacé par la séquence : ESC_PPP, ESC_ESC (0x7D, 0x5D).

De même, certains modems utilisent les 32 premiers caractères du code ASCII (figure 9.23) comme caractères de commande. Afin d'éviter que ces caractères, présents dans le champ de données, ne soient considérés par les modems comme une commande (transparence), ils seront aussi remplacés par des séquences de caractères spécifiques. Les caractères dont la transparence doit être assurée sont annoncés lors de la connexion par le protocole LCP (table **ACCM**, *Asynchronous Control Character Map*). La table ACCM est un champ de 32 bits dans lequel le bit de même rang que le caractère à masquer est à 1 : si le 12e caractère de la table ASCII doit être masqué, le 12e bit de la table ACCM est à 1. La transparence de ces caractères est obtenue par la séquence ESC_PPP, ESC_Commande où la valeur de ESC_Commande est la valeur ASCII de la commande avec le sixième bit complémenté (inversé).

Caractères nationaux

Jeu de commandes

BITS				b_7	0	0	0	0	1	1	1	1
				b_6	0	0	1	1	0	0	1	1
				b_5	0	1	0	1	0	1	0	1
b_4	b_3	b_2	b_1		0	1	2	3	4	5	6	7
0	0	0	0	0	NUL	DLE	SP	0	à	P		p
0	0	0	1	1	SOH	DC1	!	1	A	Q	a	q
0	0	1	0	2	STX	DC2	"	2	B	R	b	r
0	0	1	1	3	ETX	DC3	£	3	C	S	c	s
0	1	0	0	4	EOT	DC4	$	4	D	T	d	t
0	1	0	1	5	ENQ	NAK	%	5	E	U	e	u
0	1	1	0	6	ACK	SYN	'	6	F	V	f	v
0	1	1	1	7	BEL	ETB	(	7	G	W	g	w
1	0	0	0	8	BS	CAN	)	8	H	X	h	x
1	0	0	1	9	HT	EM	.	9	I	Y	i	y
1	0	1	0	A	LF	SUB		:	J	Z	j	z
1	0	1	1	B	VT	ESC	,	;	K		k	é
1	1	0	0	C	FF	ES		<	L	ç	l	ù
1	1	0	1	D	CR	GS		¨	M	§	m	è
1	1	1	0	E	SO	RS		>	N	^	n	¨
1	1	1	1	F	SI	US	/	?	O	–	o	DEL

Figure 9.23 La table ASCII.

1. Quelle est la séquence de bits émise, si celle à émettre en mode synchrone est :

   « 00111111111111111100111100011111011111110111110 » ?

2. En mode asynchrone, quelle est la séquence de caractères émise, si celle à émettre est :

   « 0x3F, 0x12, 0x5E, 0x7E, 0x7E, 0xE7, 0x7F, 0x7D, 0x7E, 0x5E, 0x30, 0x04 » ?

3. Sachant que cette séquence est émise sans contrôle de parité, combien de temps bit seront nécessaires à son émission (ou combien de bits seront émis au total, y compris éventuellement des bits de service) ?
4. Quelle est la valeur de la table ACCM si les 32 premiers caractères doivent être masqués (valeur par défaut pour une transmission asynchrone) ?
5. De même, quelle est la valeur de la table ACCM si aucun caractère ne doit être masqué (valeur par défaut pour une transmission synchrone) ?
6. Si le modem interprète comme des commandes les caractères « STX, ETX, ACK ».

   a) Quelle est la signification de ces caractères ?
   b) Quels sont leur rang dans la table ASCII et leur valeur (en binaire et hexadécimal) ?
   c) Quelle est la valeur de la table ACCM (donnez la valeur en une suite binaire de 32 bits et en hexadécimal) qui sera annoncée lors de l'exécution de LCP ?
   d) Sachant qu'une partie des données à transmettre est représentée ci-dessous (en hexadécimal), quelle est, pour assurer la transparence, la séquence qui sera transmise ?
   « ...C8 F4 AB 7E A3 C0 FA 02 C9 F3 05 C9 7D 03 04 7E 0F F1 06 E4 F1 34 5F... »

Chapitre **10**

Le protocole IP et les utilitaires réseaux

10.1 GÉNÉRALITÉS

Rappelons que le protocole IP a pour objectif de masquer aux applications les réseaux physiques traversés (figure 10.1). N'ayant pas la responsabilité de l'acheminement dans ces réseaux, IP est un protocole réseau allégé. En mode datagramme, IP n'entretient aucune variable d'état, il n'effectue que les tâches élémentaires d'adaptation de la taille des unités de données aux capacités d'emport du réseau physique traversé (MTU, *Maximum Transfert Unit*), la désignation des machines d'extrémité (adresse IP) et l'acheminement dans le réseau logique. Ainsi, IP ne réalise aucun contrôle d'erreur. C'est éventuellement au réseau physique emprunté d'assurer l'intégrité des données, le contrôle de flux et de congestion.

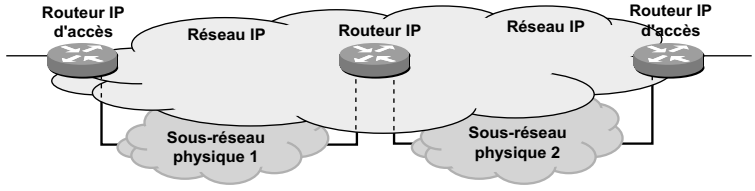


Figure 10.1 Le réseau IP (Internet Protocol).

10.2 LA STRUCTURE DU DATAGRAMME IP

Un datagramme IP (figure 10.2) peut contenir (champ données) un segment TCP, un message ICMP, ARP, RARP ou encore OSPF. Les différents champs de l'en-tête IP sont alignés sur des mots de 32 bits, si aucune option n'est invoquée cet en-tête comporte 20 octets (cinq mots de 32 bits). Les bits sont représentés dans l'ordre d'émission sur le support (bits de poids fort devant, dit aussi *big endian*).

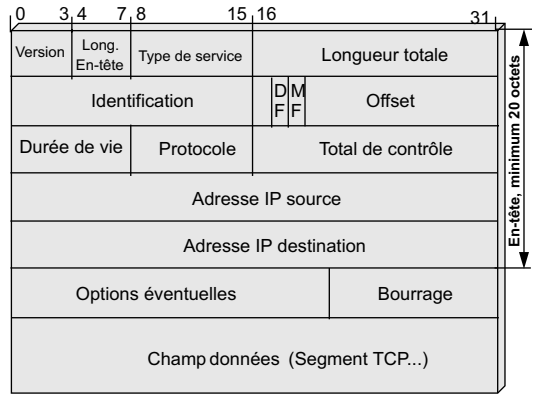


Figure 10.2 La structure du datagramme IP.

Le numéro de version sur 4 bits (**VER**) permet d'identifier la version d'IP en cours et par conséquent le format du datagramme. La présence de cette information autorise la cohabitation de plusieurs versions de protocole dans les systèmes intermédiaires, ce qui est indispensable lors de la mise à jour d'une version du protocole IP. La version courante est la version 4, cependant la version 6 (IPv6) est en cours de déploiement dans l'Internet.

Le champ longueur d'en-tête sur 4 bits (**IHL**, *Internet Head Lenght*) indique, en multiple de mots de 32 bits, la longueur de l'en-tête. Lorsqu'aucune option n'est invoquée, la valeur courante, est cinq (20 octets).

Le champ type de service[1] sur 8 bits (**TOS,** *Type Of Service*) spécifie, à la passerelle inter-réseau, le type d'acheminement attendu. Le RFC 791 a défini huit niveaux de priorité et quatre critères d'acheminement (figure 10.3), mais la plupart des systèmes intermédiaires n'ont pas la possibilité de traiter ces données.

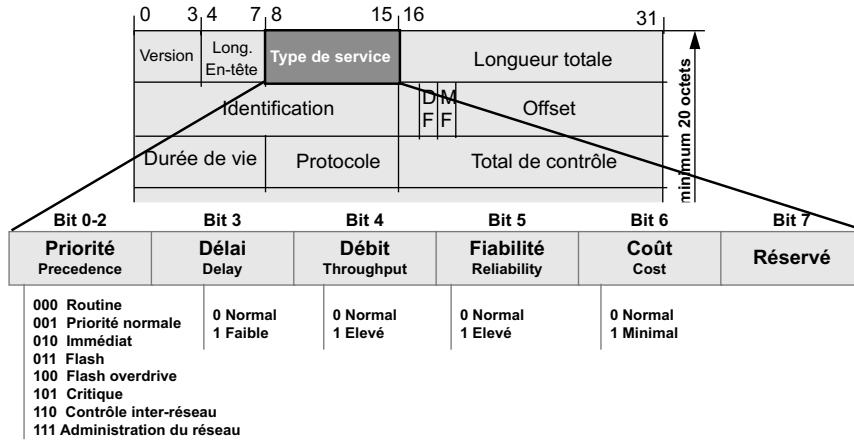


Figure 10.3 L'interprétation du champ TOS.

1. Les différentes notions introduites ici seront détaillées dans l'étude de la qualité de service dans les réseaux (chapitre 19).

Définies alors que les flux dans le réseau étaient tous de même nature (texte), les priorités du champ TOS sont inadaptées au transport des flux multimédias. Le RFC 1812 (IP *Precedence*) a modifié l'interprétation du champ TOS, en redéfinissant les trois premiers bits (figure 10.4).

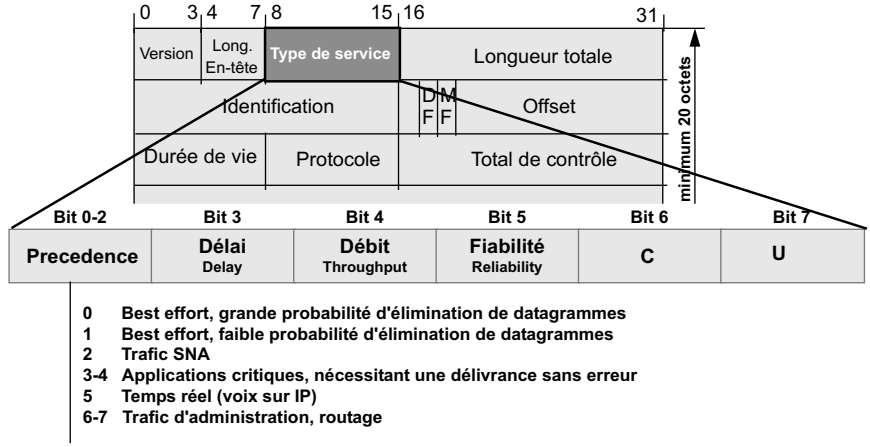


Figure 10.4 IP Precedence et type de trafic associé.

Cette nouvelle interprétation a été jugée insatisfaisante pour garantir aux différents flux IP une certaine qualité de service et un acheminement qui la respecte. Il est apparu nécessaire de différencier plus finement les flux pour, en cas de congestion dans le réseau, mettre en œuvre une politique d'acheminement et d'élimination des datagrammes en relation directe avec la qualité de service exigée par le flux IP. Le RFC 2474 (*Differentiated Services* ou *DiffServ*) introduit la notion de classes de service et définit, pour chaque classe, différentes politiques d'élimination des datagrammes. Le champ **DS** (*DiffServ*) remplace le champ TOS (figure 10.5).

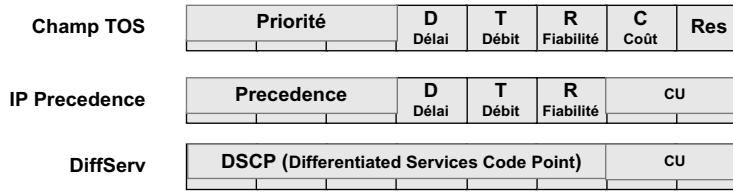


Figure 10.5 Comparaison des différentes interprétations du champ TOS.

Le champ DS comporte deux sous-champs, DSCP et CU. Le sous-champ **DSCP** (*Differentiated Service Code Point*), sur 6 bits, autorise 64 classes de trafic réparties en trois grandes familles :

– *Expedited Forwarding* (EF, RFC 2598), défini spécifiquement pour les applications temps réel, minimise le temps de latence dans le réseau. Le réseau prend en compte des contraintes fortes en terme de délai, de gigue (*jitter*) et de perte (Service dénommé *Premium Service*).

– *Assured Forwardind* (AF, RFC 2597) ou *Olympic Service* comprend quatre classes, elles-mêmes subdivisées. À chaque classe correspond une priorité différente avec une garantie de bande passante. Des mécanismes spécifiques permettent l'élimination de datagrammes en cas

© Dunod – La photocopie non autorisée est un délit

de congestion. Ces différentes classes sont généralement désignées sous les termes de : services Platinium, Gold, Silver ou Bronze.

– *Best effort*, aucun traitement spécifique n'est réalisé. Les datagrammes sont transmis pour le mieux.

Le sous-champ **CU** (*Currently Unused*) de 2 bits, actuellement non défini, devrait servir au contrôle de flux.

Le champ Longueur totale (**LEN,** *total LENgth field*) sur 16 bits indique la longueur totale, en octets, du datagramme en-tête compris. La longueur maximale est de 65 536 octets. Cette longueur maximale est toute théorique, les applications limitent d'elles-mêmes la taille des données utilisateur à 512 octets, ce qui correspond à une MTU de 576 octets.

Le champ *Identification* (**ID**) sur 16 bits : la valeur du champ ID, attribuée par la source[2], est générée de manière aléatoire par un algorithme initialisé par l'heure système. En cas de fragmentation, l'ID est recopiée par les systèmes intermédiaires dans tous les fragments du datagramme d'origine. L'ID permet, à l'hôte destinataire, d'identifier (N° identification et adresse IP) les différents fragments d'un même datagramme, il facilite ainsi le réassemblage.

Le champ suivant est composé de 3 bits dont le premier n'est pas utilisé. Le bit suivant dit bit **DF** (*Don't Fragment*, ne pas fragmenter), s'il est positionné à 1, demande au système intermédiaire de ne pas fragmenter le datagramme. Ce bit est utilisé, par exemple, quand le système d'extrémité est incapable de réassembler les différents fragments. Le système intermédiaire qui reçoit un tel datagramme doit soit le router dans sa totalité sur un sous-réseau où la MTU est compatible, soit le détruire. En cas de destruction, il en avertit la source par un message ICMP (*Internet Control Message Protocol*). Enfin, le bit **MF** (*More Fragment*) est positionné à 1 dans tous les fragments d'un même datagramme d'origine pour indiquer qu'un fragment suit. Il est à 0 dans le dernier fragment ou lorsqu'un datagramme n'a pas subi de fragmentation.

En cas de fragmentation, le champ *Offset* (13 bits) indique, en multiple de 8 octets, la position du premier bit du fragment dans le datagramme d'origine. En conséquence, tous les fragments, sauf le dernier, doivent avoir une longueur multiple de huit (voir § 10.3).

Le champ Durée de vie (**TTL**, *Time To Live*) sur 8 bits détermine, en principe en seconde, la durée de vie d'un datagramme. Cette valeur est décrémentée à chaque passage à travers une passerelle. Un datagramme avec un TTL nul n'est jamais acheminé sur le réseau, il est détruit. La passerelle qui détruit un datagramme envoie un message d'erreur ICMP à l'émetteur. Aucune estampille de temps ne figurant dans l'en-tête IP, les passerelles (routeur) n'ont pas la possibilité de mesurer le temps écoulé, elles se contentent alors de décrémenter ce champ de une unité ce qui revient à définir non pas une durée de vie, mais un nombre de sauts. Le TTL est généralement initialisé à 32 voire 64 sauts[3].

2. La RFC 791 indique que cette valeur est initialisée par la couche supérieure qui soumet le datagramme à IP. De ce fait, si l'algorithme de génération implémenté sur TCP est indépendant de celui implémenté dans UDP, un datagramme issu de TCP peut contenir le même identifiant que celui d'UDP. Même si la probabilité d'un tel événement est faible, la plupart des implémentations d'IP utilisent une variable commune gérée par le noyau.

3. On considère que toute machine dans l'Internet est accessible en 32 sauts. La valeur de ce champ a été portée à 64 quand l'Internet a franchi le mur de Berlin et la Grande Muraille de Chine.

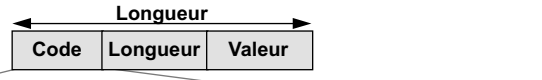
Le champ protocole (*Protocol*), 8 bits, indique à IP l'origine du champ données (protocole transporté, RFC 1700, *Assigned numbers*). Ce champ permet le multiplexage de flux. La figure 10.6 fournit quelques exemples de valeurs du champ protocole.

Valeur	Acronyme	Protocole
1	ICMP	*Internet Control Message Protocol*
2	IGMP	*Internet Group Message Protocol*
6	TCP	*Transmission Control Protocol*
8	EGP	*External Gateway Protocol*
17	UDP	*User Datagram Protocol*
89	OSPF	*Open Short Path First*

Figure 10.6 Quelques exemples de valeurs d'identifiant de protocole.

Le champ total de contrôle (*Header Checksum*), 16 bits, n'est calculé que sur l'en-tête IP. Le total de contrôle est le complément à 1 de la somme en complément à 1 des données de l'en-tête découpées en mots de 16 bits. Le total de contrôle est recalculé par chaque système intermédiaire (modification du champ TTL et fragmentation éventuelle). Le RFC 1141 indique une méthode de calcul simplifiée qui ne tient compte que de la décrémentation à 1 du champ TTL. En cas de fragmentation, le total de contrôle est intégralement recalculé.

Le champ option, de longueur variable, est codé : code option (type), longueur, valeur. Le premier octet, l'octet code, est un champ de bits dont les différentes valeurs et leur signification sont indiquées dans le tableau de la figure 10.7.



Bit	Fonction	Valeur		Commentaire
0	Copie	0		En cas de fragmentation, l'option n'est pas recopiée.
		1		L'option est recopiée dans le fragment.
1-2	Classe option	00		Datagramme ou supervision de réseau.
		01		Réservé pour une utilisation future.
		10		Test.
		11		Réservé.
		Classe	Valeur	Longueur
3-7	Numéro d'option	0	0	Fin de la liste d'options.
		0	1	Alignement d'octet.
		0	2	11 Restrictions de sécurité.
		0	3	var Routage lâche par la source.
		2	4	var Horodatage.
		0	7	var Enregistrement route.
		0	8	4 Identificateur de connexion.
		0	9	var Routage strict par la source.

Figure 10.7 Le codage et les options IP.

La longueur du champ option étant variable, celui-ci peut-être suivi de bits de bourrage pour assurer l'alignement de l'en-tête IP sur des mots de 32 bits. Coûteux en terme de traitement par les passerelles, le champ option est peu voire pas utilisé.

© Dunod – La photocopie non autorisée est un délit

10.3 LE CONTRÔLE DE LA FRAGMENTATION SOUS IP

La fragmentation d'un datagramme IP est contrôlée par les champs : longueur totale (LEN), offset (Offs) dans le segment, et le bit MF (*More Fragment*) du datagramme IP. Le champ offset indique, en multiples de 8 octets, la position du fragment dans le datagramme initial. Le fragment ainsi constitué ne peut avoir, pour longueur, que le multiple de huit le plus proche de la MTU, sauf pour le dernier fragment.

Ainsi, pour une MTU de 128 octets[4], la charge utile (niveau IP) ne peut être, au maximum, que de 108 octets (128 – 20 d'en-tête IP), soit une taille effective de 104 octets (13×8), si l'on tient compte de l'en-tête TCP (20 octets), la charge du premier fragment n'est que de 84 octets. La figure 10.8 illustre la fragmentation d'un datagramme IP de 576 octets. Pour faciliter la compréhension les valeurs des champs *Len* et *Offset* sont exprimées en décimal.

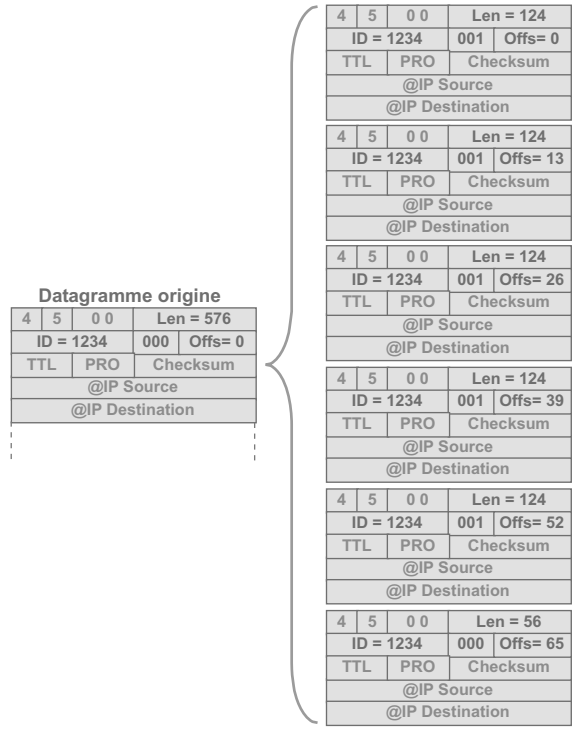


Figure 10.8 La fragmentation d'un datagramme IP.

Pour assurer le réassemblage, IP doit attendre l'arrivée de tous les fragments. Les opérations de fragmentation et de réassemblage sont coûteuses en terme de puissance de calcul et de mémoire. De plus, en mode datagramme, la perte d'un seul fragment provoque une reprise par la couche TCP de la totalité du segment fragmenté.

4. Valeur courante de la MTU d'un paquet X.25.

10.4 LES UTILITAIRES DE LA COUCHE RÉSEAU

10.4.1 Le protocole ICMP

Généralités

Le protocole ICMP (*Internet Control Message Protocol*, RFC 792) permet d'informer la source d'une erreur réseau (message d'erreur) ou de formuler une demande d'état à un système (message d'information). Les messages ICMP sont encapsulés dans un datagramme IP (Protocole = 1). La figure 10.9 représente la structure du message d'erreur ICMP et fournit quelques exemples de codage des différents champs.

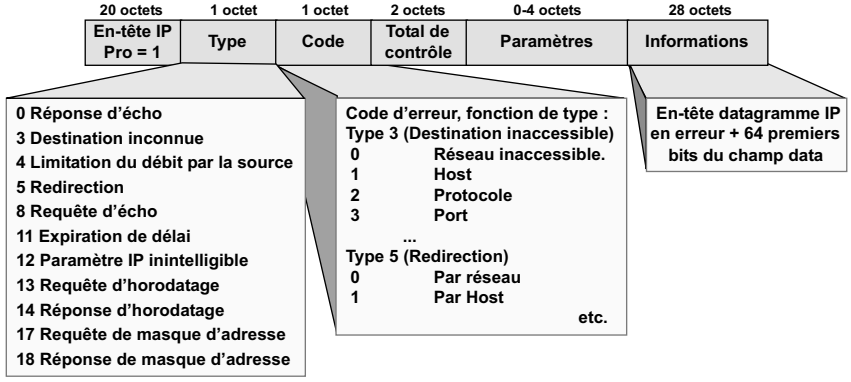


Figure 10.9 La structure du message d'erreur d'ICMP.

Le protocole ICMP ne fiabilise pas IP, c'est un protocole d'information. Ses différentes fonctions sont aussi utilisées par certains utilitaires. Par exemple, la commande PING (voir ci-dessous) utilise les messages de demande de réponse d'écho (type 0, 8). Le protocole **NTP** (*Network Time Protocol*) utilise la commande ICMP Timestamp (type 13, 14) pour synchroniser les horloges du réseau. Les estampilles temporelles sont exprimées en millisecondes depuis minuit TU (Temps universel).

Exemple de message ICMP, Obtention du masque de sous-réseau

Lorsqu'une station a besoin, pour se configurer, de connaître le masque de sous-réseau utilisé (*Netmask*) dans son réseau, elle peut émettre une requête (*Type*=17) de demande de masque de sous-réseau (figure 10.10). Celle-ci est émise à destination de la passerelle par défaut, si celle-ci est connue, sinon elle est diffusée à toutes les stations du réseau (*broadcast*). Les champs *Identificateur* et *Numéro de séquence* permettent d'associer une réponse à la requête d'origine.

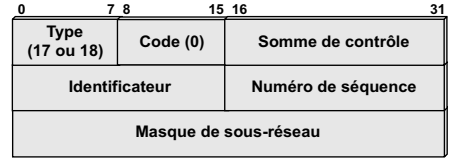


Figure 10.10 La requête de masque de sous-réseau.

© Dunod – La photocopie non autorisée est un délit

Les utilitaires utilisant les messages ICMP

➤ L'utilitaire PING

L'utilitaire **PING** (*Packet INternet Groper*) permet de tester l'accessibilité d'un système et d'évaluer le temps aller et retour entre le système source et le système cible. La commande PING envoie un message ICMP de demande d'écho vers la machine cible, celle-ci retourne une réponse d'écho (figure 10.11).

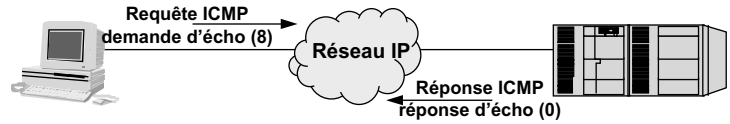


Figure 10.11 Principe de la commande PING.

La commande PING permet de tester une liaison TCP/IP de bout en bout, et, ainsi, de déterminer un éventuel élément défaillant :

– PING sur l'adresse 127.0.0.1 teste l'installation de la pile TCP/IP sur la machine source.
– Sur l'adresse IP de la machine source, elle vérifie que cette station est correctement configurée.
– Sur l'adresse de la passerelle par défaut, elle contrôle la validité du masque de sous-réseau et la configuration de la passerelle par défaut.
– PING sur l'adresse de l'interface de sortie (LS locale) valide la configuration de cette interface.
– Sur l'adresse de LS distante, elle s'assure que le lien WAN est établi et que les routeurs local et distant sont correctement configurés vis-à-vis du réseau source.
– Sur l'adresse de station distante, elle valide la configuration de bout en bout.
– Enfin, PING avec un nom d'hôte vérifie que le fichier « host » local ou que le serveur DNS est correctement renseigné.

La figure 10.12 illustre la structure du message ICMP d'écho utilisé par la commande PING.

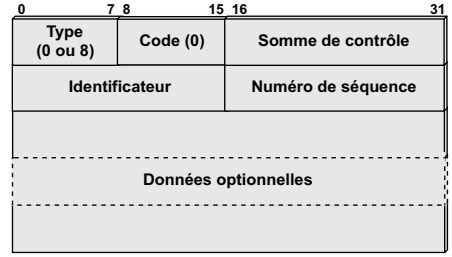


Figure 10.12 La structure du message d'écho utilisé par l'utilitaire PING.

Le numéro de séquence est initialisé à zéro et incrémenté à chaque envoi d'un datagramme PING. Le champ identificateur, lors de l'envoi de messages PING vers plusieurs destinataires, permet de différencier les réponses d'une séquence de PING. La réponse à une commande PING doit parvenir dans un délai maximal de 20 secondes, sinon la cible est déclarée inaccessible.

La commande PING émet une série de demandes d'écho, la figure 10.13 illustre la réponse à une commande PING sur une cible d'adresse 195.221.126.186. Chaque demande d'écho a été émise

avec un champ données de 32 caractères. L'information temps indique la durée entre l'émission de la requête et la réception de la réponse, c'est une approximation du RTT[5]. Le champ TTL, non présent dans toutes les implémentations, reproduit la valeur du champ TTL du datagramme IP reçu. Cette valeur est toujours délicate à interpréter, car elle dépend de la valeur initiale du TTL fixée par la machine cible. *A priori*, dans notre cas, on peut déduire du TTL que le champ a été initialisé à 64 (valeur recommandée par le RFC 1700 *Assigned Numbers*) et que onze nœuds intermédiaires ont été traversés (64 – 11 = 53). Certaines implémentations fixent à 255 le TTL des réponses d'Echo d'ICMP.

```
C:> Ping 195.221.126.186
Envoi d'une requête 'ping' sur 195.221.126.186 avec 32 octets de données :
Réponse de 195.221.126.186 : octets=32 temps=135 ms TTL=53
Réponse de 195.221.126.186 : octets=32 temps=140 ms TTL=53
Réponse de 195.221.126.186 : octets=32 temps=156 ms TTL=53
Réponse de 195.221.126.186 : octets=32 temps=156 ms TTL=53

Statistiques Ping pour 195.221.126.186:
   Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
   Minimum = 135 ms, Maximum = 156 ms, Moyenne = 146 ms
```

Figure 10.13 Exemple de commande PING.

➤ L'utilitaire Traceroute (Tracert)

L'utilitaire Traceroute dû à Van Jacobson permet de découvrir la route empruntée par un datagramme entre une source et une machine cible. Bien que le protocole IP soit en mode datagramme et qu'aucune stabilité de route ne soit garantie, on constate en pratique que des datagrammes successifs empruntent la même route. L'utilitaire Traceroute émet trois datagrammes IP successifs avec un TTL incrémenté de un à chaque nouvelle série de trois. La première série est émise avec un TTL de un, le premier nœud atteint décrémente le TTL, celui-ci étant alors à zéro, il élimine le datagramme et envoie à la source un message ICMP type 11 « *time exceeded* » (expiration de délai). Le premier nœud est ainsi découvert, l'utilitaire poursuit jusqu'à trouver la destination. Les requêtes Traceroute sont émises avec un numéro de port > 30 000, le nœud destination retourne un message ICMP de type 3, code 3 « port inaccessible ».

```
C:> Tracert 195.221.126.186
Détermination de l'itinéraire vers cnam-st-martin.rap.prd.fr [195.221.126.186]
avec un maximum de 30 sauts :

  1  237 ms   156 ms   140 ms  nssta107.francetelecom.net [193.252.253.123]
  2  156 ms   156 ms   156 ms  GE2-201.ncidf103.Puteaux.francetelecom.net
  3  156 ms   156 ms   156 ms  pos6-0.nraub103.Aubervilliers.francetelecom.net  [193.252.159.42]
  4  140 ms   156 ms   140 ms  pos13-3.ntaub201.Aubervilliers.francetelecom.net [193.252.103.18]
  5  156 ms   156 ms   156 ms  193.251.126.54
  6  140 ms   156 ms   140 ms  P14-0.PASCR2.Pastourelle.opentransit.net [193.251.128.105]
  7  156 ms   156 ms   155 ms  193.51.185.2
  8  140 ms   156 ms   140 ms  nri-b-pos11-0.cssi.renater.fr [193.51.179.10]
  9  156 ms   156 ms   156 ms  jussieu-pos4-0.cssi.renater.fr [193.51.180.157]
 10  140 ms   156 ms   140 ms  193.50.20.73
 11  156 ms   156 ms   155 ms  cr-cnam.rap.prd.fr [195.221.125.205]
 12  140 ms   156 ms   156 ms  cnam-st-martin.rap.prd.fr [195.221.126.186]

Itinéraire déterminé.
```

Figure 10.14 Exemple de commande Traceroute.

5. La commande PING n'est pas prioritaire dans les réseaux, par conséquent la valeur du RTT (Temps aller retour) constitue plutôt une borne maximale.

© Dunod – La photocopie non autorisée est un délit

La réponse, à une commande Traceroute, illustrée figure 10.14 indique nœud après nœud, les différents nœuds traversés, de la machine source à la machine cible. Chaque ligne indique le rang du nœud traversé, le temps aller retour (RTT) mis par chacun des trois datagrammes de la rafale, s'il est disponible le nom du nœud et son adresse IP, cette information permet de déterminer la position géographique du nœud et éventuellement l'opérateur. La requête ci-dessus a été émise initialement sur le réseau de France Télécom, puis acheminée par une passerelle de transit vers le réseau RENATER, enfin les datagrammes ont été relayés par une machine de l'Université de Jussieu avant d'atteindre le CNAM. En cas de dépassement du temps imparti, l'indication de temps est remplacée par une étoile.

10.4.2 La résolution d'adresses

Généralités

Les applications ne connaissent que l'adresse logique IP, alors que les données doivent être acheminées dans le réseau physique. À cette fin, la couche IP doit établir une correspondance entre l'adresse IP dans le réseau logique et l'adresse physique. Ce mécanisme s'appelle **mécanisme de résolution d'adresses**.

La résolution d'adresses dans les réseaux à diffusion

Dans les réseaux locaux, le protocole **ARP** (*Address Resolution Protocol*) permet à tout nœud du réseau d'obtenir l'adresse MAC[6] de la machine destination. La figure 10.15 illustre ce mécanisme. En 1, le nœud d'origine, d'adresse IP notée @IPa et d'adresse physique notée @Pha doit transmettre des données à la station d'adresse IP @IPc mais dont il ignore l'adresse physique. Il émet une demande de résolution d'adresses (ARP) sur le réseau physique à destination de la machine cible.

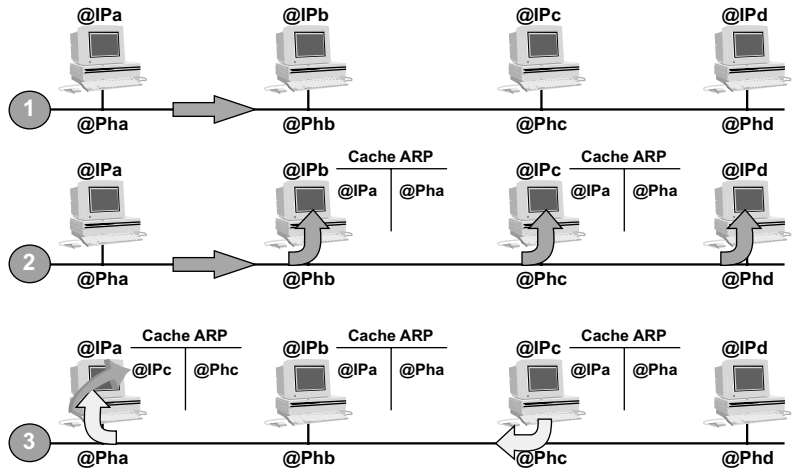


Figure 10.15 Le mécanisme de la résolution d'adresses.

6. Le format des adresses MAC ou adresses IEEE dites encore adresses physiques des interfaces LAN sur un réseau local a été décrit au chapitre 6 (Réseaux en mode paquet).

Cette demande est encapsulée, dans une trame MAC (Ethernet, Token Ring...) dont le champ adresse destination est à FF-FF-FF-FF-FF-FF (adresse de diffusion). En 2, tous les nœuds actifs sur le brin du réseau local, reconnaissant une demande ARP, en extraient l'adresse MAC origine et l'adresse IP origine et stockent ces valeurs, pour une éventuelle utilisation ultérieure, dans une table dite cache ARP. En 3, seule, la machine IPc qui a reconnu son adresse logique (@IPc) dans la requête répond en fournissant son adresse physique. Cette réponse est émise avec une adresse *unicast* puisque IPc connaît maintenant l'adresse physique de IPa. La réponse est stockée dans le cache ARP de la machine origine.

Lorsqu'une machine doit envoyer un datagramme à une machine appartenant à un autre réseau (résolution interréseaux), la résolution s'effectue en deux temps (figure 10.16). La machine origine réalise une première résolution d'adresses avec la passerelle, puis adresse les données à la passerelle qui elle-même émet une requête ARP sur le réseau destinataire pour connaître l'adresse MAC de la machine cible. Enfin, les données sont adressées à la machine cible.

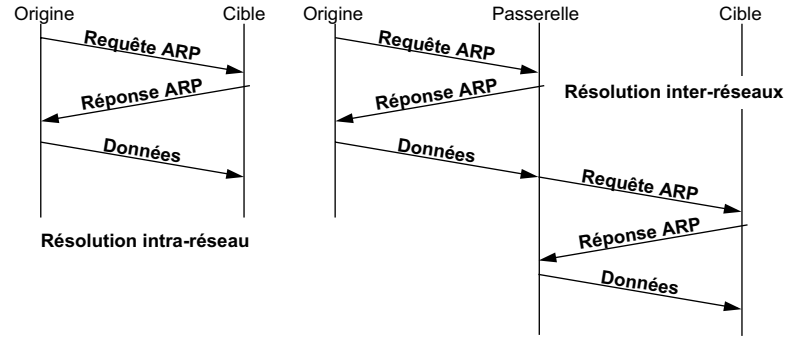


Figure 10.16 Le mécanisme de la résolution d'adresses.

Lorsque la machine origine ne connaît pas l'adresse logique de la passerelle, elle émet sa requête directement sur le réseau. La passerelle qui reconnaît l'adresse IP d'un hôte qu'elle sait joindre répond avec sa propre adresse physique (MAC adresse). La passerelle doit être configurée pour répondre à ce type de demande (Proxy-ARP).

Pour limiter le trafic de résolution d'adresses et éventuellement détecter une duplication d'adresses, toute machine s'envoie, lors de sa mise sous tension, une demande ARP (*gratuitous ARP*). La figure 10.17 illustre le format d'un paquet ARP.

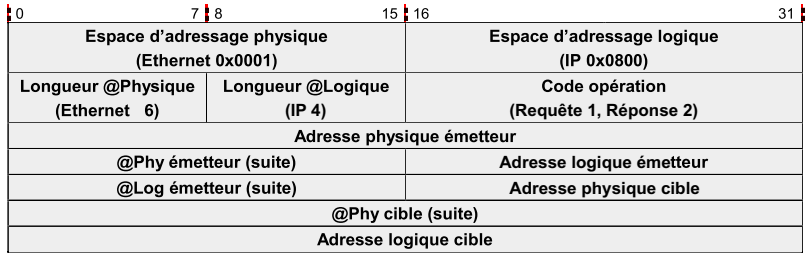


Figure 10.17 La structure du datagramme ARP.

À l'inverse du protocole ARP, le protocole **RARP** (*Reverse Address Resolution Protocol*) permet à une station qui ne dispose pas d'adresse IP (station sans disque, imprimante...) de s'en voir

© Dunod – La photocopie non autorisée est un délit

attribuer une. Le format du paquet RARP est identique à celui du protocole ARP. Seule, la valeur du champ *Code opération* est différente : 3 pour une requête et 4 pour la réponse. Une machine du réseau doit être configurée pour répondre à ces requêtes (serveur RARP). Le protocole RARP est aujourd'hui considéré comme obsolète.

La résolution d'adresses dans les réseaux NBMA[7]

Dans les réseaux sans diffusion, la résolution peut être statique, la table de correspondance est alors renseignée par l'administrateur (résolution statique) ou réalisée par un protocole particulier (résolution dynamique) comme c'est, par exemple, le cas dans les réseaux LAN ATM. Les techniques LAN ATM consistent à émuler sur un réseau ATM un réseau local. Par exemple, le RFC 1577 ou *Classical IP* (**CLIP**) définit un réseau IP sur un réseau physique ATM comme un sous-réseau logique (**LIS**, *Logical IP Subnetworking*). Un LIS est un ensemble de machines IP partageant un même préfixe d'adresse IP et connectées à un réseau ATM.

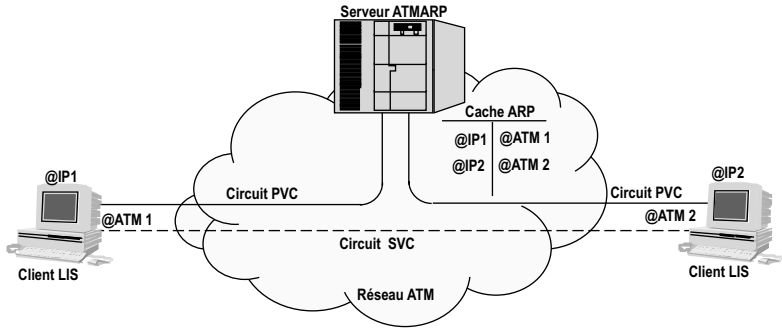


Figure 10.18 Le réseau LAN ATM dit Classical IP.

Les stations d'un même sous-réseau (LIS) communiquent directement entre elles après avoir établi un circuit virtuel. Pour établir ce circuit virtuel, la station source doit connaître l'adresse ATM de la machine IP distante. La résolution d'adresses est assurée par un serveur d'adresses (serveur ATMARP) qui, sur sollicitation d'une requête **ATMARP** (*ATM Address Resolution Protocol*), renvoie l'adresse ATM correspondante. Chaque réseau logique (LIS) possède une machine configurée en tant que serveur ATMARP (figure 10.18). Lors de la configuration d'un client LIS, celui-ci, outre son adresse ATM, est informé de l'adresse ATM du serveur ATMARP.

La figure 10.19 décrit le scénario de résolution d'adresses de ce type de réseau. Lors de sa mise sous tension, le client LIS établit un circuit virtuel avec le serveur ATMARP. Ce dernier émet alors, vers cette station, une requête **InARP** (*Inverse ARP*) pour apprendre son adresse IP. Le serveur ATMARP met alors son cache ARP à jour (table de correspondance @IP/@ATM).

Lorsqu'un client LIS veut entrer en relation avec un autre client du même LIS, il émet une requête ARP vers le serveur ATMARP (quelle est l'adresse ATM de la station IP ?), celui-ci lui fournit alors l'adresse ATM, le client LIS met son cache ATM à jour (@IP/@ATM), et établit un circuit virtuel avec cette station.

7. **NBMA**, *Non Broadcast Multiple Access*.

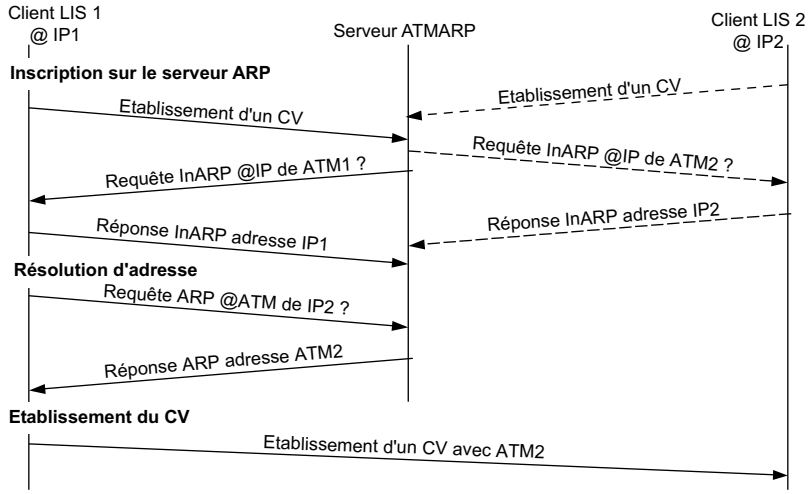


Figure 10.19 L'établissement d'un circuit virtuel entre deux clients LIS.

10.4.3 Les utilitaires de configuration

Généralités

Le protocole RARP permet à une station de se voir attribuer une adresse IP, les requêtes RARP utilisent une adresse de *broadcast* limité. De ce fait, elles ne sont pas retransmises par les routeurs, ce qui implique un serveur RARP par réseau (sous-réseau). Le masque de sous-réseau peut-être découvert par une requête ICMP. Mais, ce sont les seules informations que la machine peut obtenir. Le protocole **BOOTP** (*BOOTstrap Protocol*) permet à une machine sans disque de connaître l'intégralité des paramètres de configuration du réseau (adresse, masque, passerelle par défaut...). Le serveur BOOTP associe à l'adresse physique du client un profil. De ce fait, BOOTP n'est utilisable que dans un environnement relativement figé, ce qui en limite l'utilisation notamment avec l'introduction du concept de mobilité (ordinateurs portables). **DHCP** (*Dynamic Host Configuration Protocol*), considéré comme une évolution de BOOTP, autorise une configuration automatique des stations et permet la mobilité.

BOOTP

Le serveur de BOOTP ne fournit au client que le nom du fichier de boot à télécharger, ce fichier pouvant être éventuellement une image mémoire complète du système. Les machines utilisant BOOTP, par exemple les stations XWindows (X.11), n'ont besoin en mémoire morte (ROM) que d'un système réduit comportant au minimum une pile IP/UDP, les utilitaires BOOTP et **TFTP** (*Trivial File Transfer Protocol*).

La requête BOOTP est émise en *broadcast* (255.255.255.255) ; un routeur, configuré en agent relais (proxy), propage éventuellement la requête aux serveurs BOOTP situés sur d'autres segments du réseau.

Si le client BOOTP connaît son adresse il la précise, sinon il utilise l'adresse 0.0.0.0, de même, le client peut connaître le nom du fichier de configuration, dans ce cas il fournit le nom du fichier recherché. Par défaut, le serveur BOOTP renvoie l'adresse IP affectée au client, le nom du fichier

© Dunod – La photocopie non autorisée est un délit

de configuration et l'adresse de la machine où est stocké le fichier à télécharger, cette machine pouvant être le serveur BOOTP lui-même. Il reste alors au client à se connecter à cette machine pour télécharger, à l'aide de TFTP, le ou les fichiers nécessaires à son fonctionnement (système, logiciels...), cette procédure est appelée démarrage en deux temps.

BOOTP utilise IP et UDP, il doit donc assurer lui-même la fiabilisation de la transmission. Pour ce faire, il utilise le total de contrôle de UDP et assure les reprises sur temporisation. Pour soulager le travail du client, le bit DF du datagramme IP est positionné à 1 (ne pas fragmenter).

DHCP

Reprenant les principes de BOOTP, DHCP (RFC 1541) offre de véritables fonctions de configuration automatique des stations. Contrairement à BOOTP qui affecte de manière statique une adresse IP, le serveur DHCP détient un jeu d'adresses valides et les paramètres associés de configuration IP qui seront alloués dynamiquement aux clients DHCP. Les stations configurées par DHCP libèrent les adresses lorsqu'elles n'en ont plus besoin. DHCP propose trois mécanismes d'adressage :

- L'allocation manuelle, à l'instar de BOOTP ou RARP, DHCP alloue une adresse spécifique à un client. L'administrateur gère donc les adresses IP.
- L'allocation automatique, elle permet, lors d'une configuration initiale, d'attribuer automatiquement à une station une adresse IP choisie par le système parmi un pool d'adresses. La station conserve cette adresse tant qu'elle n'a pas été libérée explicitement par l'administrateur.
- L'allocation dynamique, dans ce mode de fonctionnement, DHCP alloue temporairement (bail) une adresse IP. En fin de bail, la machine peut en demander le renouvellement.

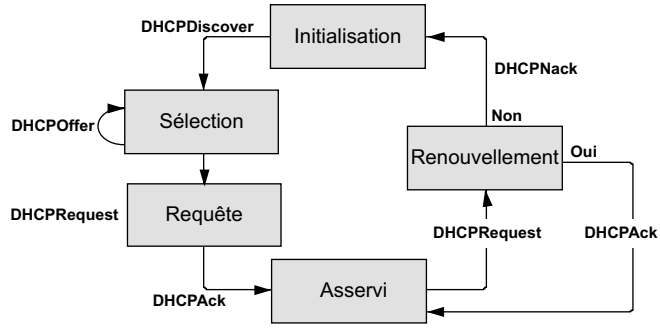


Figure 10.20 Les différents états d'un client DHCP.

La figure 10.20 décrit les différentes étapes d'une configuration automatique DHCP. La station, lors de son initialisation, diffuse un message d'exploration (**DHCPDiscover**). Tous les serveurs DHCP actifs sur le réseau formulent une offre de service (**DHCPOffer**). La station cliente passe alors dans l'état sélection. Lorsque la station a choisi un serveur DHCP (serveur élu), elle formule auprès de celui-ci une requête d'affectation d'adresse (**DHCPRequest**).

Le serveur DHCP sélectionné accuse réception de la requête (**DHCPAck**) en fournissant les éléments de configuration TCP/IP nécessaires à la station (adresse IP, masque de sous-réseau, adresse de la passerelle...) et la durée de validité de ces paramètres (bail). La station est alors dans l'état dit

« asservi ». Si elle en a la possibilité, elle mémorise les informations. Elle pourra les utiliser, lors des connexions futures, jusqu'à expiration du bail, échéance au bout de laquelle elle devra formuler une demande de renouvellement (**DHCPRequest**). La requête initiale ou le renouvellement peut être refusé par le serveur élu (**DHCPNAck**). La station est alors revenue à l'état initialisation.

Le message **DHCPRelease** permet au client de résilier son bail avant l'échéance de celui-ci. Le message **DHCPDecline** est utilisé par le client pour informer un serveur que son offre est invalide. Enfin, le message **DHCPInform** permet à une machine d'obtenir des paramètres de configuration supplémentaires.

DHCP utilise les mêmes ports (67 pour le serveur, 68[8] pour le client) et le même format de message que BOOTP, seul le dernier champ diffère (figure 10.21). Un serveur DHCP peut être configuré pour répondre aux requêtes BOOTP.

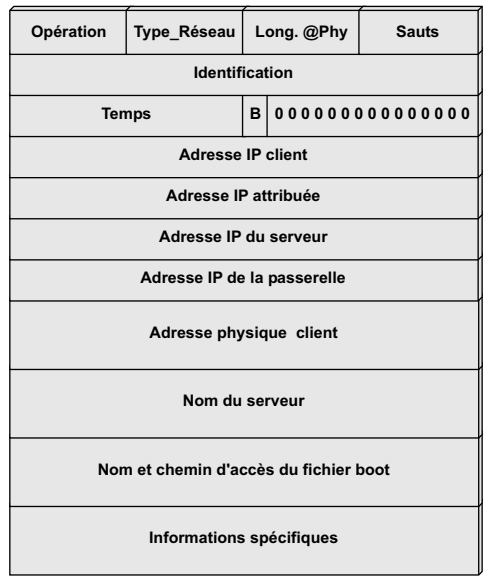


Figure 10.21 Le format des messages BOOTP et DHCP.

Le champ **Opération** (*Opcode*) sur un octet vaut 1 pour une demande et 2 pour une réponse. Le champ **Type_Réseau** (*Hardware type*) vaut généralement 1 (réseau Ethernet), le champ **Long. @Phy** (*Hardware address length*) vaut 6 quand le champ précédent est à 1 (adresse MAC). Le champ **Sauts** (*Hop count*) positionné à 0 par le client peut être utilisé par un serveur proxy pour indiquer le nombre d'agents ayant relayé la demande.

Le champ **Identification** (*transaction ID*) positionné par le client et recopié par le serveur permet d'associer une requête à sa réponse. Le champ **Temps** (*Number of seconds*) est défini par le client, ce champ évalue l'instant d'émission de la requête décompté depuis que le client a émis sa première

8. Le client aurait pu utiliser un port éphémère, mais compte tenu que la réponse BOOTP ou DHCP peut être diffusée (*broadcast*) et que la probabilité que deux machines (le client et une quelconque des machines du réseau) utilisent un même port éphémère n'est pas nulle, le client utilise un port réservé (port dit bien connu).

© Dunod – La photocopie non autorisée est un délit

requête. Il est utilisé par un serveur DHCP secondaire pour détecter la défaillance du serveur DHCP primaire.

Dans le champ suivant, seul le premier bit, le bit **B** (*Broadcast*) est utilisé, à 1 il indique que la réponse doit être faite en mode diffusion, à 0 la réponse est émise à l'attention de l'adresse MAC du client, c'est le mode de réponse normal.

Si le client connaît son adresse IP, il renseigne le champ **Adresse IP du Client** (*Client IP address*), sinon ce champ est à 0. Dans ce dernier cas dans la réponse, le champ **Adresse IP attribuée** (*Your IP address*) contient l'adresse IP affectée au client. Par défaut ce champ est à 0.

Le champ **Adresse IP du serveur** (*Server IP address*) contient l'adresse IP du serveur qui a répondu à la requête. De même, si le serveur et le client ne sont pas situés sur le même réseau, le champ **Adresse IP de la passerelle** (*Gateway IP address*) contient l'adresse de la dernière passerelle ayant relayé la réponse.

Le champ de 16 octets **Adresse physique du client** (*hardware address*) est renseigné par le client. L'adresse MAC n'occupant que 6 octets, les 10 octets inutilisés doivent être positionnés à 0.

Le champ de 64 octets **Nom du serveur** (*Server hostname*) peut éventuellement contenir le nom du serveur ayant fourni la réponse. De même, le serveur peut renseigner le champ **Nom et chemin d'accès au fichier de boot** (*Boot filename*). Ces champs sont remplis en clair et terminé par le caractère **Null** (ASCII 0).

Le champ **Informations spécifiques**, *vendor-specific area* est de 64 octets pour BOOTP renommé *option* et jusqu'à 312 octets pour DHCP. Ce champ est codé selon le triptyque « Code Option, Longueur, Valeur ». Il est notamment utilisé par DHCP pour différencier les différents types de message DHCP (figure 10.22).

Valeur (Type d'option)	Signification
1	DHCP_Discover
2	DHCP_Offer
3	DHCP_Request
4	DHCP_Decline
5	DHCP_Ack
6	DHCP_Nack
7	DHCP_Release
8	DHCP_Inform

Figure 10.22 Le codage des différents types de message DHCP (Option 53).

10.4.4 Conclusion

Les limitations de l'adressage, dues essentiellement à la structure à plat de l'adressage IP, conjuguées au succès d'Internet ont contribué à la pénurie d'adresses. Plusieurs solutions ont été imaginées pour pallier cette pénurie. Celle retenue, IPv6, porte l'espace d'adressage de 32 à 128 bits (voir chapitre 8).

10.5 D'IPv4 À IPv6

10.5.1 Les lacunes d'IPv4

IPng (*next generation*) ou IPv6 répond au besoin d'évolution de la communauté Internet et comble les faiblesses d'IPv4. La plus connue concerne l'espace d'adressage dont la structure à plat (Net_ID) est responsable de l'explosion des tables d'adressage (certains routeurs Internet ont plusieurs dizaines de milliers d'entrées dans leur table de routage) et dont la structure figée est responsable de la pénurie d'adresses. En faisant disparaître la notion de classe d'adresses, en autorisant l'agrégation d'adresses de réseaux contigus en un seul préfixe réseau et en organisant une affectation géographique des adresses, le CIDR (voir chapitre 8) a partiellement résolu ces problèmes. Cependant l'utilisation d'un adressage privé associé à la translation d'adresses (NAT) repousse les limites de l'espace d'adressage mais pénalise les performances.

Enfin, l'arrivée de nouvelles applications comme le multimédia et le besoin de services sécurisés ont motivé l'étude d'un nouveau protocole permettant d'augmenter l'espace d'adressage tout en conservant les grands principes qui ont fait le succès du protocole IP.

Les principales caractéristiques d'IPv6 sont :

- adressage étendu (128 bits au lien de 32) ;
- en-tête simplifié autorisant un routage plus efficace ;
- sécurité accrue en incluant des mécanismes d'authentification, de cryptographie et en garantissant l'intégrité des données ;
- implémentation d'un mécanisme de découverte de la MTU optimale. La fragmentation n'est plus réalisée dans le réseau mais par le nœud source ;
- suppression du champ *Checksum*, ce qui allège le travail des routeurs intermédiaires ;
- amélioration des aspects de diffusion (*Multicast*) ;
- intégration de fonctions d'autoconfiguration et de renumérotation.

10.5.2 Le datagramme IPv6

La structure du datagramme

Plusieurs solutions ont été envisagées pour augmenter l'espace d'adressage, la solution retenue passe l'adressage de 32 bits à 128 bits (2^{128} adresses soit plusieurs millions d'adresses par mètre carré de surface terrestre : 6,65 10^{23} @/m^2). Pour améliorer le traitement des datagrammes dans les routeurs, la structure même du datagramme a été modifiée en supprimant notamment le champ option et les champs devenus inutiles. Par conséquent, l'en-tête du datagramme est de longueur constante (40 octets), l'augmentation de longueur étant largement compensée par le gain de traitement d'une structure d'en-tête figée. La figure 10.23 compare les datagrammes IPv4 et IPv6. Les champs IPv4 qui n'ont aucune correspondance dans le datagramme IPv6 ont leur label grisé et en italique.

Les données relatives à la fragmentation (ID, Flags, Offset) disparaissent de l'en-tête. IPv6 implémente un mécanisme de découverte de la MTU. Si nécessaire, la fragmentation est réalisée par la source et le réassemblage par le destinataire ce qui allège considérablement le travail des routeurs intermédiaires. Cependant, si la fragmentation par le réseau s'avère indispensable, une extension d'en-tête est prévue à cet effet. L'en-tête étant de longueur fixe, le champ IHL (longueur

© Dunod – La photocopie non autorisée est un délit

de l'en-tête) est devenu inutile. De même, le calcul du total de contrôle a été supprimé, le mécanisme de contrôle de TCP incluant un pseudo en-tête IP est suffisant pour protéger les adresses.

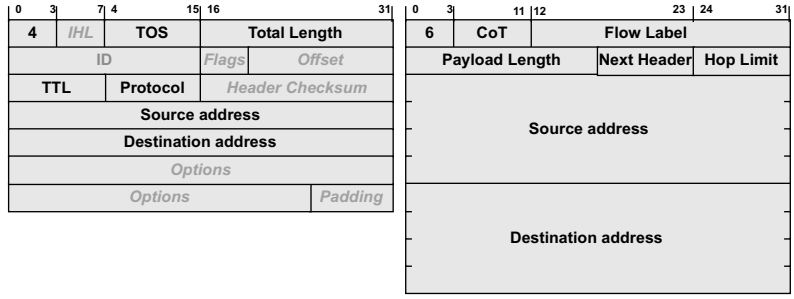


Figure 10.23 Les datagrammes IPv4 et IPv6.

Le champ TOS (*Type of Service*) trouve son équivalent en deux champs, un champ classe de trafic (**CoT**, *Class of Traffic*) sur 8 bits et une identification de flux (*Flow label*). Ce champ contient un identifiant attribué initialement par la source, il peut être assimilé à un identifiant de circuit virtuel, chaque routeur mémorise ce label et tente de router tous les datagrammes d'un même flux identiquement. Cette information va contribuer à la mise en place d'une véritable gestion de la qualité de service dans les réseaux IP et notamment faciliter le développement d'application de type voix. Le contexte ainsi créé est détruit sur temporisation (Timer d'inactivité). Le réseau ainsi défini est dénommé *soft-state*[9].

L'en-tête étant de longueur fixe, le champ longueur totale d'IPv4 (*Total length*) est remplacé par la taille des données transportées (*Payload length*). Enfin, Le champ *Protocol* d'IPv4 est remplacé par l'indication du type de l'en-tête suivant (*Next header*). Si aucune option n'est invoquée, ce champ contient l'identification du protocole transporté, la figure 10.24 indique les différentes valeurs de ce champ. Enfin, un compteur de sauts (*Hops Limit*) positionné par la source (valeur par défaut 64) et décrémenté de 1 par chaque nœud intermédiaire remplace le champ TTL d'IPv4, mais décompte ici de façon claire le nombre de sauts et non plus un temps interprété en nombre de sauts.

Le traitement des options ou en-têtes d'extension

➤ Généralités

Des extensions d'en-tête remplacent les options d'IPv4. Ces extensions sont ignorées des routeurs, seule l'extension **Hop-by-Hop** (proche en proche) est traitée par tous les routeurs. Afin de garantir des performances optimales, les options doivent apparaître dans un ordre prédéfini. Seule extension traitée par les routeurs, l'extension *Hop-by-Hop* doit apparaître en premier. La figure 10.25 illustre le chaînage des en-têtes.

9. On peut classer les réseaux à états en deux catégories. Dans la première, le contexte est créé à l'initiative de l'appelant par un message spécifique et est détruit par un message de libération (notion de circuit virtuel). Ce type de réseau est aussi appelé *hard-state*. Dans les seconds, le contexte est déduit du flux de données. Désignée sous le terme de *soft-state* par opposition au *hard-state*, cette technique allège les réseaux : il n'y a pas de mécanisme explicite de création de circuit virtuel. Cependant, il n'y a aucune garantie de maintien du contexte durant toute la transmission.

Valeur	Type	Désignation
0	Option	Hop-by-Hop
4	Protocole	IPv4
6	Protocole	TCP
17	Protocole	UDP
43	Option	Routing Header
44	Option	Fragment Header
45	Protocole	Interdomain Routing Protocol
46	Protocole	ReSsource reserVation Protocol
50	Option	Encapsulation Security Payload (IPsec)
51	Option	Authentification Header (Ipsec)
58	Protocole	ICMP
59		No Next Header
60	Option	Destination Options Header

Figure 10.24 Les valeurs du champ Next Header.

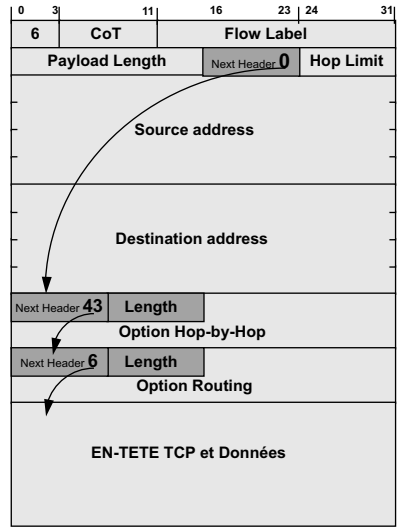


Figure 10.25 Principe du chaînage des en-têtes.

➤ Exemples d'extension d'en-tête

Extension Proche en Proche (0)

Cette extension, la première de la série, est la seule à être traitée par tous les routeurs traversés. La longueur de l'extension (champ *Length*) est exprimée en mots de 64 bits-1 mot. Cette extension est un champ d'option codé selon le triptyque classique <Type d'option, Longueur, Valeur>. Les différentes options définies sont :

– Des champs de bourrage, type 0 pour 1 octet de bourrage, type 1 pour une longueur de plus de 2 octets (alignement de l'extension sur un multiple entier de mots de 64 bits).

– *Router Alert* (type 5), utilisée pour indiquer au routeur qu'il doit examiner le contenu du champ données (message **ICMP** ou **RSVP**).

© Dunod – La photocopie non autorisée est un délit

– *Jumbogramme* (type 194), ce champ d'extension spécifie la longueur des données (valeur sur 4 octets) quand celle-ci dépasse 64 ko. Dans ce cas, le champ longueur des données de l'entête IPv6 contient la valeur 0.

Extension Routage (43)

Cette extension permet d'imposer une route à un paquet. Actuellement, seul le routage par la source est défini (type 0). Ce routage peut être soit strict, le routeur suivant doit alors être le voisin du routeur courant, soit lâche (*Loose*), le routeur peut alors consulter ses tables pour choisir la route à prendre pour joindre le routeur suivant de la liste. En fait, l'extension routage par la source contient une liste de routeurs à traverser.

Extension Fragmentation (44)

La fragmentation dans un réseau *best effort* pénalise les performances. Même si IPv6 introduit un mécanisme de découverte de la MTU, certaines applications[10] considérant que le réseau assure la fragmentation remettent à la couche transport (UDP) des données trop importantes. Dans ces conditions, la couche IPv6 doit réaliser la fragmentation à l'émission, le réassemblage est réalisé par le destinataire. Le format de cette extension reprend les informations de segmentation d'IPv4 (figure 10.26)

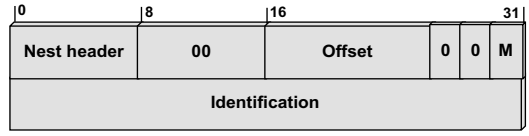


Figure 10.26 Le format de l'extension fragmentation.

Les différents champs ont la même signification, à l'exception du bit DF inutile puisque la fragmentation n'est pas traitée par les routeurs traversés. Le bit M informe qu'un fragment suit. À l'instar d'IPv4, le champ *Offset* sur 13 bits indique en multiple de 8 octets, la position du premier bit du fragment dans le datagramme d'origine. Enfin, le champ identification, recopié dans tous les fragments d'un même paquet, permet l'identification par le destinataire de tous les fragments du paquet initial.

Extension Destination (60)

Codée de manière similaire à l'extension *hop-by-hop*, cette extension est traitée par le destinataire, elle introduit le concept de mobilité du destinataire, un mobile pouvant toujours être joint par son adresse principale. Les options destinations permettent de gérer l'association entre une adresse locale sur le réseau d'accueil et l'adresse principale du mobile.

10. C'est le cas notamment de NFS (*Network System File*) qui est un véritable système de gestion de fichier à travers un réseau IP.

10.6 IP ET LA MOBILITÉ

10.6.1 Généralités

La notion de mobilité est apparue avec l'avènement des ordinateurs portables. Cependant si ces ordinateurs permettent de se déplacer, il restait à résoudre le problème d'accès aux applications en leur masquant le déplacement du mobile, c'est ce problème que résout l'**IP Mobile** (RFC 2002, *IP Mobility Support*).

La mobilité recouvre deux notions distinctes. La première consiste à accéder à ses données depuis un point d'accès fixe d'un réseau étranger au réseau d'appartenance. L'ordinateur a été déplacé mais reste fixe durant la connexion, on parle alors d'**ordinateurs nomades** ou de macro-mobilité. La seconde, rendue possible par l'apparition des réseaux hertziens autorise l'ordinateur à rester en contact avec son réseau d'appartenance alors qu'il se déplace et éventuellement change de réseau d'accueil, on parle alors d'**ordinateurs mobiles**. Bien que la dénomination du protocole soit IP mobile, *IP Mobility Support* est mal adapté aux changements rapides de réseau d'accueil.

L'IP mobile est un enrichissement du protocole IP pour permettre à un ordinateur mobile (nomade) d'accéder à ses applications depuis n'importe quel réseau d'accueil sans qu'il soit besoin de le reconfigurer : l'ordinateur mobile communique en utilisant son adresse IP d'origine.

10.6.2 Le principe de la mobilité sous IPv4

La mise en relation des correspondants distants

L'agent mobile possède une adresse principale dite encore adresse mère (*Home address*, @IPh) dans son réseau d'origine (réseau de domiciliation ou *Home network*) et se voit attribuer une adresse temporaire (*Care_of address*, @IPv) dans le réseau visité (*Foreign network*). La mobilité devant être transparente aux applications, le mobile utilise son adresse principale pour communiquer, par conséquent toutes les réponses sont adressées à son réseau d'origine. Dans ce réseau (*Home network*), un routeur IP, doté d'un agent IP mobile (agent domestique, ou *Home agent*), intercepte les messages à destination du mobile et lui réexpédie à son adresse temporaire (*Care_of address*). On distingue deux modes de réexpédition. Le premier dit réexpédition par agent extérieur nécessite dans le réseau visité la présence d'un agent relais (*Foreign agent*), c'est cet agent relais qui attribue l'adresse temporaire au mobile. La figure 10.27 illustre ce mode de fonctionnement.

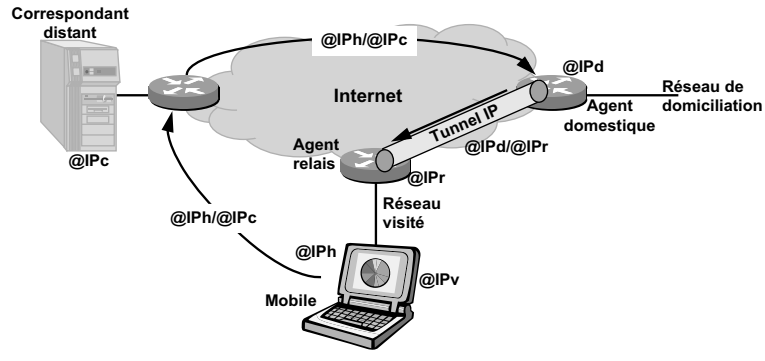


Figure 10.27 La mobilité d'IPv4.

© Dunod – La photocopie non autorisée est un délit

L'échange dans le sens mobile vers son correspondant distant ne pose aucun problème particulier ; l'échange utilise l'adresse d'origine du mobile (source : @IPh) et l'adresse du correspondant distant (destination : @IPc). La mobilité étant transparente à l'ordinateur distant, celui-ci adresse sa réponse à l'adresse IP du mobile dans son réseau de domiciliation (destination : @IPh). Ces messages sont interceptés par l'agent domestique et réexpédiés vers le réseau visité. Pour cela, le message IP reçu du correspondant distant est encapsulé dans un datagramme IP (IP dans IP, RFC 2003) dont les adresses correspondent à celles des deux agents (domestique et relais). L'ensemble forme un tunnel IP dont le format général de l'unité de données est illustré en figure 10.28.

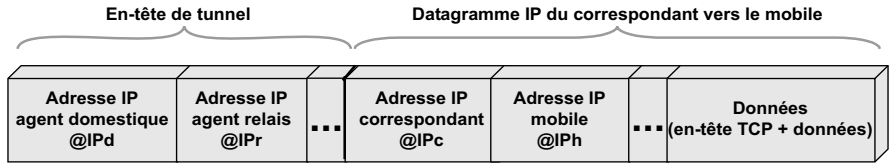


Figure 10.28 Le format du datagramme de tunnel IP.

Les différents champs de l'en-tête d'encapsulation ont la même signification que dans l'IP traditionnel. L'en-tête de tunnel comporte les adresses source (initiateur du tunnel, *Tunnel entry point*), l'adresse destination (*Tunnel exit point*). Le champ version vaut 4 ; la longueur de l'en-tête (IHL) indique en mots de 32 bits la taille de l'en-tête du tunnel, sa valeur est 5 ; le champ longueur totale indique la taille totale du nouveau datagramme, c'est-à-dire l'en-tête IP du tunnel, l'en-tête IP du datagramme encapsulé et la charge utile du datagramme (*Playload*) ; la valeur du bit DF (*Don't Fragment*) est la même que celle du datagramme encapsulé. Le champ *Protocol* est fixé à 4 (IPv4 dans IP). Dans le réseau visité, l'adresse du mobile (*Care_of address*) n'est pas obligatoirement utilisée pour adresser les messages au mobile, ce peut être une adresse partagée par plusieurs visiteurs, l'agent relais utilise alors la *home address* du mobile pour relayer les messages vers le visiteur.

Le second mode de fonctionnement, dit réexpédition par colocataire, n'utilise pas d'agent relais dans le réseau visité. Le tunnel IP est de « bout en bout », c'est le mobile qui gère alors la mobilité, en particulier le « détunnelage » des datagrammes IP qui lui sont réexpédiés par son *Home agent*. Dans ce mode de fonctionnement, c'est généralement un serveur DHCP qui attribue l'adresse temporaire, c'est le mode d'attribution de l'adresse temporaire qui détermine le mode de fonctionnement. Si l'adresse est attribuée par un agent extérieur, le mode de fonctionnement est le mode réexpédition par agent extérieur, si l'adresse est attribuée par DHCP, c'est le mode de fonctionnement dit réexpédition par agent colocataire.

L'encapsulation IP dans IP ajoute un *overhead* important au datagramme (20 octets), aussi, le RFC 2004 a-t-il défini un mode d'encapsulation « allégé » dit « *Minimal Encapsulation for IP* ». Cette encapsulation n'utilise qu'un seul en-tête IP et ajoute entre l'en-tête IP modifié et la charge utile un en-tête **MFH** (*Minimal Forwarding Header*) ne contenant que les adresses source et destination du datagramme d'origine. Les informations de l'en-tête IP modifié et l'en-tête MFH permettent de reconstituer le datagramme d'origine.

Dans l'en-tête IP, les adresses source et destination indiquent les points d'entrée et de sortie du tunnel, elles remplacent les adresses source et destination du datagramme d'origine qui elles, sont recopiées dans l'en-tête minimal. La valeur du champ *Protocol* du datagramme d'origine est recopiée dans le champ *Protocol* de l'encapsulation minimale et est remplacée par la valeur 55.

Le bit **S** (*Original **S**ource Address*) indique si l'adresse source d'origine est présente dans l'en-tête. Le total de contrôle (*checksum*) ne porte que sur l'en-tête minimal.

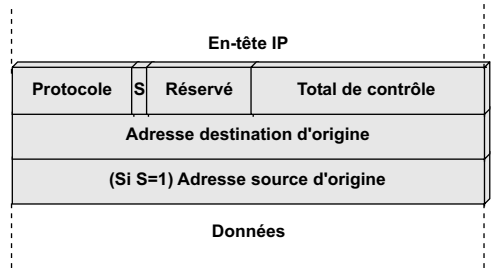


Figure 10.29 L'encapsulation minimale.

La gestion de la mobilité

➤ Découverte de l'agent extérieur

Avant d'établir toute communication, le mobile doit s'enregistrer auprès de son agent domestique (agent mère) et de l'agent relais du réseau d'accueil. Pour cela il lui faut d'abord, sur son réseau d'accueil, découvrir l'agent relais.

Dès qu'il se connecte à un réseau, un ordinateur émet un message ICMP de découverte de routeur, c'est ce mécanisme qui est utilisé par l'agent mobile. Quand ce dernier se connecte à un réseau extérieur, il émet un message de découverte d'agent en mode *broadcast* ou en *multicast* (224.0.0.11). L'agent extérieur, ainsi averti de la présence d'un visiteur, renvoie le message d'annonce de routeur en y ajoutant l'extension (*Mobility agent extension*), représentée figure 10.30. Le mobile peut alors s'enregistrer auprès de l'agent relais.

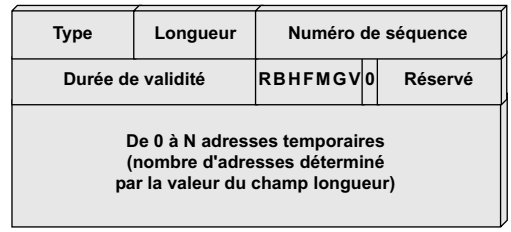


Figure 10.30 L'extension du message ICMP d'annonce de routeur.

L'extension de mobilité est identifiée par la valeur Type de message à 16. Le champ Longueur indique la longueur totale du message (sauf les champs Type et Longueur), cette longueur est égale à $6 + 4N$ où N représente le nombre d'adresses de réexpédition contenu dans le message, N peut valoir 0. Le champ Numéro de séquence permet de détecter la perte d'un message. Le champ Durée (*Registration lifetime*) indique en secondes la durée de l'association, tous les bits à 1 signifie que l'association est permanente. La signification des bits du champ suivant est indiquée figure 10.31. Le champ suivant est inutilisé (bits à zéro). Enfin suit le champ Adresses de réexpédition qui indique les adresses de réexpédition gérées par cet agent relais. Si au moins une adresse est indiquée, le bit F doit être à 1. Le nombre d'adresses est déterminé par la valeur du champ Longueur.

© Dunod – La photocopie non autorisée est un délit

Bit	Nom	Signification
R	*Registration*	L'enregistrement auprès de l'agent relais est obligatoire pour pouvoir utiliser la *Care_of address*.
B	*Busy*	L'agent relais ne peut accepter de nouvel enregistrement.
H	*Home agent*	L'agent local offre les services d'agent domestique (*Home agent*).
F	*Foreign agent*	L'agent local offre les services d'agent relais (*Foreign agent*).
M	*Minimal encapsulation*	L'agent implémente un tunnel utilisant l'encapsulation minimale.
G	*GRE encapsulation*	L'agent implémente un tunnel utilisant l'encapsulation GRE (*Generic Routing Encapsulation*).
V	*Van Jacobson compression*	L'agent supporte la compression d'en-tête Van Jacobson.
R	*Reserved*	Réservé, les bits non utilisés doivent être à zéro.

Figure 10.31 La signification des bits du champ de bits.

Pour assurer l'acheminement des datagrammes, le mobile doit être identifié par l'agent domestique et par l'agent extérieur. Cette procédure porte le nom d'enregistrement du mobile.

➤ Principe de l'enregistrement du mobile

La procédure d'enregistrement permet à un mobile de s'enregistrer auprès de l'agent relais (agent extérieur) du réseau visité et auprès de l'agent domestique de son réseau d'origine. Elle permet aussi de renouveler ou d'annuler une demande de réexpédition. Dans le mode « réexpédition par agent extérieur », le processus d'enregistrement comporte quatre étapes (figure 10.32).

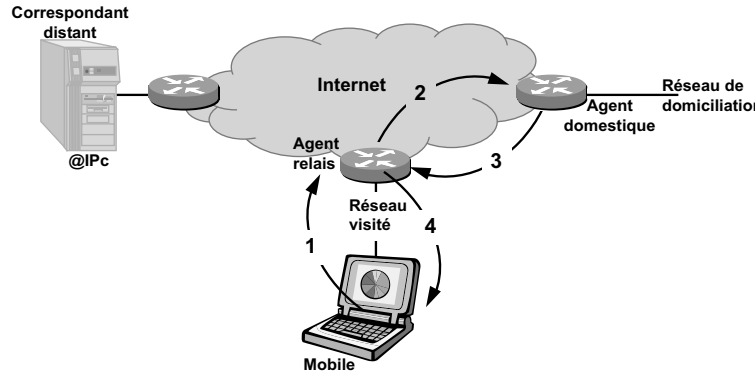


Figure 10.32 La schématisation des procédures d'enregistrement.

Le mobile s'enregistre (1) auprès de l'agent extérieur (*Registration request*), celui-ci mémorise la demande et la relaie (2) à l'agent domestique du réseau d'origine qui l'acquitte (3) (*Registration reply*), enfin celui transmet l'acquittement au mobile (4). Lorsque l'adresse obtenue est du type réexpédition par agent colocataire, le mobile s'enregistre directement auprès de son agent relais. Les messages *Registration request* et *Registration reply* utilisent le transport UDP et le port 434.

Le champ *Type* identifie le message. Le champ suivant diffère selon qu'il s'agit d'un message d'enregistrement ou d'une réponse. La figure 10.34 fournit l'interprétation de ces champs. Le champ *Lifetime* correspond à une demande ou à une allocation de temps de vie de l'association.

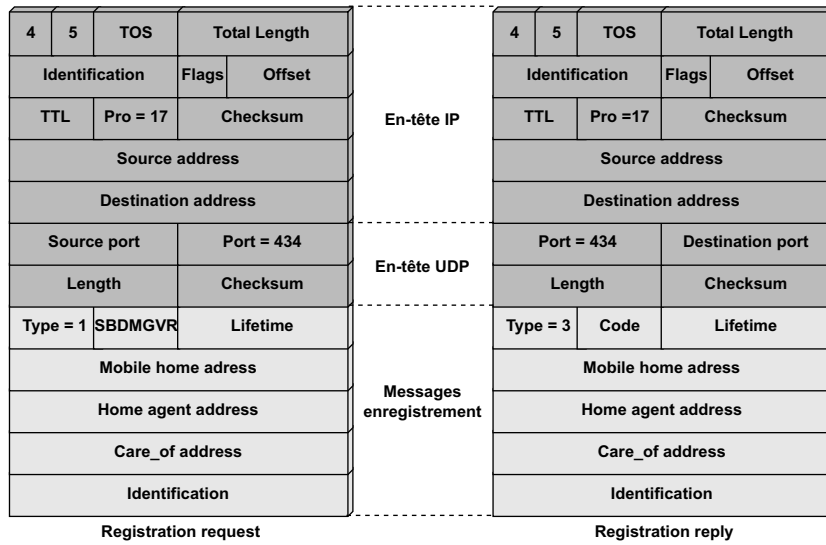


Figure 10.33 Le format des messages d'enregistrement.

À zéro il met fin à la réexpédition, tout à 1, la durée est « infinie ». L'agent domestique et l'agent relais peuvent modifier cette valeur dans leur réponse. Le champ *Identification* permet d'associer une requête à sa réponse.

Bit	Nom	Signification
S	*Simultaneous*	Adresse simultanée, et non pas de remplacement.
B	*Broadcast*	Demande de réexpédition vers le mobile des broadcasts de son réseau d'origine.
D	*Domicile*	Le mobile met en œuvre la réexpédition par agent colocataire.
M	*Minimal encapsulation*	Utiliser l'encapsulation minimale.
G	*GRE encapsulation*	Utiliser l'encapsulation GRE.
V	*Van Jacobson compression*	Utiliser la compression d'en-tête Van Jacobson.
R	*Reserved*	Réservé, les bits non utilisés doivent être à zéro.

Code	Signification
0	Acceptation de l'enregistrement.
66	Refus pour insuffisance de ressource par l'agent domestique.
69	Refus par l'agent domestique, la durée demandée (*life time*) est trop importante.
130	Refus pour insuffisance de ressource par l'agent relais.
131	Refus par l'agent relais pour défaut d'authentification.
136	Refus par l'agent relais : adresse inconnue.

Figure 10.34 La signification du champ de bits et quelques valeurs du champ code.

Notons que, pour assurer la communication entre les machines du réseau mère et le mobile, l'agent domestique doit être configuré en proxy ARP pour que les datagrammes à destination du mobile lui soient transmis. À charge pour lui de les rerouter vers le réseau visité.

© Dunod – La photocopie non autorisée est un délit

10.6.3 La mobilité dans IPv6

La mobilité IPv6 est une évolution de la mobilité IPv4 qui, profitant des nouvelles fonctionnalités d'IP, simplifie et optimise la mobilité. Notamment l'agent relais (*Foreign agent*) disparaît, seul le mode réexpédition par colocataire est valide.

Dans la mobilité IPv6, un mécanisme spécifique permet à chaque nœud en communication avec le mobile d'apprendre et de mémoriser l'adresse temporaire du mobile (association adresse mère/adresse temporaire). Lorsqu'un nœud doit adresser un datagramme au mobile, s'il possède une association pour l'adresse mère du mobile, il utilise l'option IPv6 « en-tête de routage » pour adresser directement le datagramme au mobile dans le réseau visité (optimisation du routage), sinon il envoie le datagramme vers le réseau mère, ce datagramme intercepté par l'agent domestique est réacheminé par encapsulation vers le réseau visité (figure 10.35).

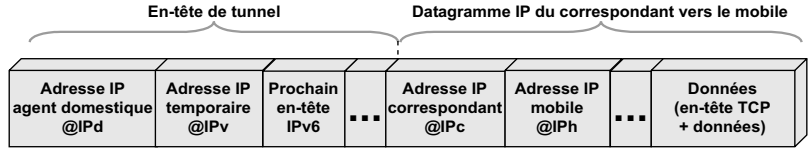


Figure 10.35 L'encapsulation IPv6 dans IPv6.

La mobilité IPv6 définit quatre nouvelles options destination :

– Mise à jour de l'association (**BU**, *Binding Update*), utilisée par le mobile pour informer un correspondant ou son agent mère de son adresse temporaire (*Care_of address*). Pour éviter toute substitution d'adresse (mascarade), tout datagramme comportant cette option doit inclure un en-tête d'authentification. La figure 10.36 représente cette option.
– Acquittement de l'association (**BAck**, *Binding Acknowledge*), message d'acquittement de la mise à jour d'association. Ce message doit obligatoirement comporter un en-tête d'authentification.
– Demande de mise à jour de l'association (**BR**, *Binding Request*), utilisé par tout nœud en correspondance avec le mobile pour rafraîchir une association.
– Adresse mère (**HA**, *Home Address*), permet au mobile depuis son réseau visité d'utiliser son adresse temporaire comme adresse source, tout en fournissant au destinataire son adresse mère.

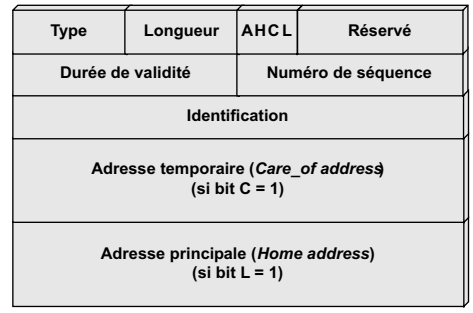


Figure 10.36 L'option mise à jour d'association.

Utilisé pour informer un correspondant ou son agent mère de sa nouvelle adresse temporaire (*Care_of address*), l'option mise à jour d'association comporte les informations nécessaires à l'association : adresse temporaire/adresse principale. Le champ longueur exprime en octets la longueur totale de l'option. Le champ Durée de validité à la même signification qu'en mobilité IPv4. Le numéro de séquence permet de détecter la perte de message. Le bit « **A** » à 1 indique qu'il s'agit d'un message d'acquittement et le bit « **H** » à 1 demande au destinataire d'agir en tant qu'agent domestique (*Home agent*). L'adresse de réexpédition (*Care_of address*) est celle contenue dans le champ adresse temporaire de l'option si le bit « **C** » est à 1, sinon il s'agit de l'adresse IP source de l'en-tête IP. Les bits « **L** » (*Home Link-Local Address*) et « **H** » positionnés simultanément à 1 indiquent que le nœud destinataire doit agir en tant que *proxy*.

10.6.4 Conclusion

Le développement d'interfaces radio de plus en plus performantes (UMTS...) ne peut que mettre en évidence un besoin croissant de mobilité. Cependant, la mobilité telle que nous venons de la définir ne convient qu'aux ordinateurs nomades. Lorsque le changement de réseau visité est rapide et fréquent, les mécanismes ci-dessous génèrent trop d'*overhead* procédural et par conséquent sont inadaptés. Aussi le concept a-t-il été étendu, en particulier par l'introduction du concept de micro-mobilité ou IP cellulaire (figure 10.37).

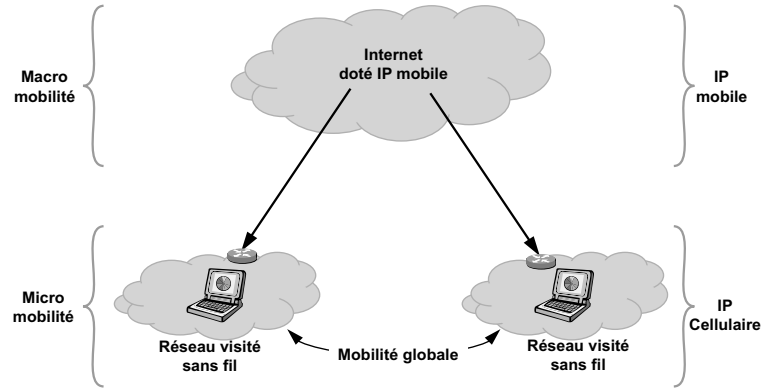


Figure 10.37 La définition du concept de mobilité.

10.7 L'ENCAPSULATION GRE

Devant la multiplication des modes de tunneling dans IP (RFC 1234, 1226, 1241, 1479), le RFC 2784 propose une encapsulation générique devant se substituer à toutes les autres formes de tunnels IP (**GRE**, *Generic Routing Encapsulation*). L'encapsulation GRE permet de transporter dans un datagramme IP tous les protocoles référencés par le RFC 1700 (*Assigned numbers*). L'encapsualtion GRE ne fait qu'intercaler entre l'en-tête IP de tunnel et le paquet transporté, une identification du protocole transporté (figure 10.38).

L'en-tête de tunnel IP contient les informations relatives au point d'initialisation et de terminaison du tunnel (adresses source et destination), le champ protocole est fixé à 47 (encapsulation

© Dunod – La photocopie non autorisée est un délit

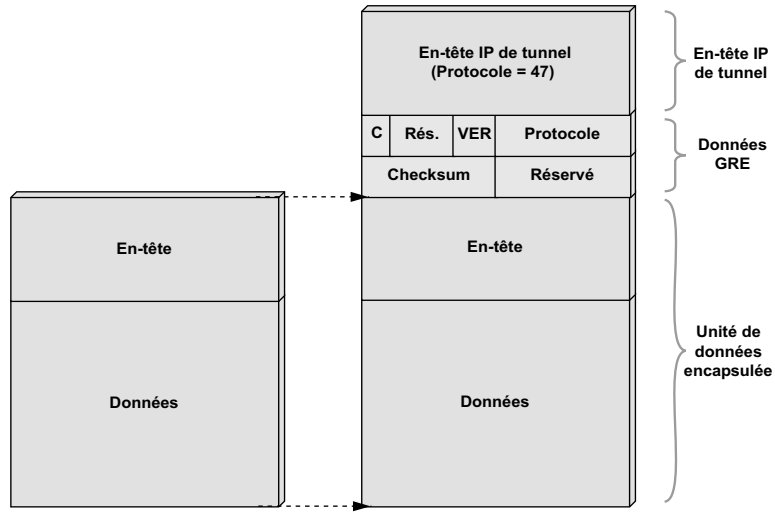


Figure 10.38 L'encapsulation GRE.

GRE). L'en-tête GRE a pour objet essentiel l'identification du protocole transporté, c'est en principe l'Ethertype de ce protocole. Ainsi, par exemple, IP dans IP voit cette valeur égale à 0x800. Le bit C à 1 valide le champ *Checksum*, dans ce cas il est calculé sur l'en-tête GRE et la charge utile transportée.

L'équipement qui termine le tunnel (adresse IP destination) « désencapsule » la charge utile et traite ces données selon les règles de traitement du protocole indiqué dans l'en-tête GRE.

En associant plusieurs interfaces virtuelles (plusieurs adresses IP) à un même équipement, il est possible d'initialiser et de maintenir, entre deux équipements plusieurs tunnels IP. Ce concept, en isolant les flux de différentes origines, introduit la notion de **VPN** (*Virtual Private Network*) et permet de masquer, à un réseau public, l'utilisation dans les sites d'extrémité d'adresses privées.

10.8 CONCLUSION

Le protocole IP, imaginé à une époque où seules des informations de type texte transitaient dans les réseaux, a su, en raison de sa simplicité originelle, s'adapter et représente pratiquement aujourd'hui le seul protocole mis en œuvre dans les réseaux. Cependant, sa nouvelle version (*IP next generation* ou IPv6), même si elle apporte des améliorations sensibles surtout en matière de sécurité, ne devrait envahir les réseaux privés que dans quelques années.

EXERCICE

Exercice 10.1 Table ARP

L'un des établissements d'une entreprise utilise la plage d'adresse 10.0.0.0 de la classe A (RFC 1918). On considère quatre machines de cet établissement dont les noms et adresses sont donnés (figure 10.39).

Nom	@IP	@MAC
Pierre.Entreprise.com	10.99.43.27	MAC_1
Jacques.Entreprise.com	10.163.12.254	MAC_2
Alfred.Entreprise.com	10.189.12.27	MAC_3
Martine.Entreprise.com	10.126.43.254	MAC_4

Figure 10.39 Le plan d'adressage.

1. Quel est le NET_ID de ce plan d'adressage ?
2. Quel est le nombre de bits nécessaires pour réaliser deux sous-réseaux (SubNet_ID) tels que Pierre et Martine appartiennent au même sous-réseau et que Jacques et Alfred appartiennent à un autre sous-réseau ? On rappelle que les bits du Net_ID et du SubNet_ID doivent être contigus. Donnez le masque correspondant.
3. Quel est le nombre de bits minimum et nécessaire pour qu'aucune des machines n'appartienne au même sous-réseau ? Donnez le masque correspondant.
4. Pour permettre la communication entre les deux sous-réseaux de la question 2, on relie les brins Ethernet de ces deux sous-réseaux par un routeur configuré en proxy ARP (c'est lui qui répond en lieu et place des stations connectées sur ses autres liens). Si on affecte à chaque interface LAN de ce routeur la première adresse disponible (Net_Host=1), quelles sont les adresses affectées ? Représentez l'ensemble par un schéma.
5. En admettant que toutes les stations aient communiqué entre elles et qu'aucune entrée n'ait été effacée, quel est le contenu de la table ARP de la station de Pierre ? Pour cette question, on affectera des adresses MAC fictives à chaque interface du routeur : MAC_R1 et MAC_R2.
6. L'établissement envisage de raccorder son réseau à Internet. Est-ce possible en l'état. Quelle est la difficulté et quelle solution proposeriez-vous ?

Chapitre **11**

Les protocoles de transport : TCP et UDP

11.1 GÉNÉRALITÉS

Le réseau IP assure un transfert de données non fiable (remise pour le mieux ou *best effort*), dans ces conditions les programmes d'application doivent prendre en compte toutes les défaillances éventuelles du réseau et en particulier :

- la détection et la reprise sur erreur ;
- la perte de données dues à la saturation des mémoires tampons des éléments actifs du réseau, phénomène connu sous le nom de congestion ;
- le déséquencement des données.

Afin de faciliter le développement d'applications au-dessus d'un réseau IP, il est nécessaire de masquer aux programmeurs l'ensemble de ces problèmes. Ce rôle est normalement dévolu à la couche transport. **TCP** (*Transmission Control Protocol*) est un protocole de niveau transport en mode connecté (figure 11.1).

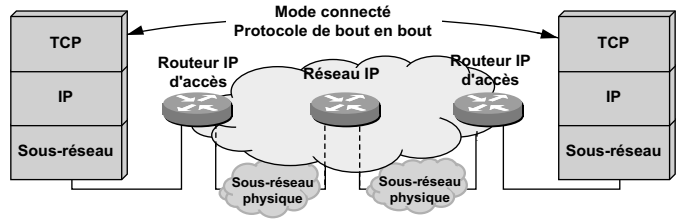


Figure 11.1 La transmission Protocol.

S'appuyant sur un protocole réseau non fiable (*Best effort*), TCP garantit la délivrance des données en séquence, il en contrôle la validité et organise les éventuelles reprises sur erreur ou sur temporisation, enfin, il effectue un contrôle de flux de bout en bout et met en œuvre un mécanisme de détection et de guérison de la congestion.

11.2 LES MÉCANISMES DE BASE DE TCP

11.2.1 La notion de connexion de transport

La notion de connexion de transport est quelque peu différente de celle de circuit virtuel de niveau réseau. En effet, un circuit virtuel réseau résulte de l'association d'identifiants de liaisons en point à point entre les différents nœuds d'un réseau afin d'y définir un chemin à travers celui-ci. La connexion de transport permet de voir, au niveau applicatif, le réseau comme un lien virtuel entre deux applications actives sur les systèmes d'extrémité. Ce n'est pas un lien virtuel de machine à machine, mais d'application à application.

L'identification de ce « circuit virtuel » ne peut prendre en compte que des éléments connus et identifiant de manière unique les processus communicants distants. En TCP, la connexion de transport est complètement définie par l'association de différents identifiants (figure 11.2) :

– l'identifiant des processus d'extrémité ou **port**,
– l'identifiant des systèmes d'extrémité ou adresses **IP**,
– l'identifiant du **protocole** de transport utilisé.

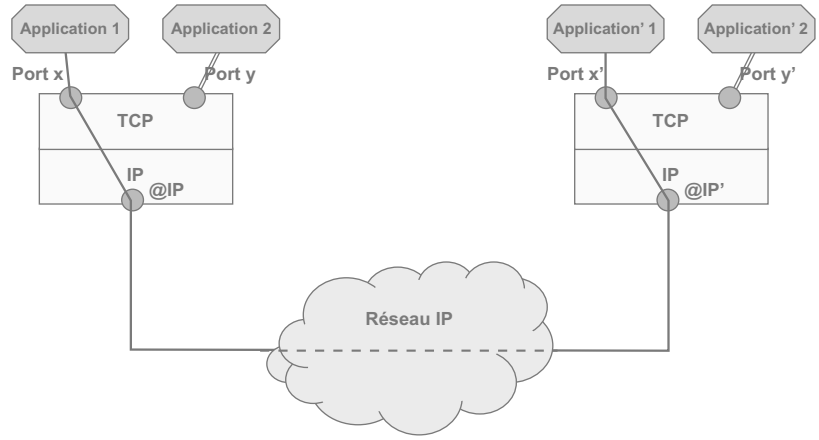


Figure 11.2 La connexion de transport.

L'association de ces identifiants :

$$\{\textbf{protocole, port destination, @IP destination, port source, @IP source}\}$$

est désignée sous le terme de *socket* (RFC 793). En fait, la notion de *socket* est cependant beaucoup plus large ; dans le monde UNIX, une *socket* définit une interface de programmation ou **API**, *Application Programming Interface*. L'environnement Microsoft définit un concept identique : les WinSock.

11.2.2 Notion de multiplexage de connexion de transport

Un même système peut exécuter plusieurs applications, il doit donc être capable d'établir et de distinguer plusieurs connexions de transport (multiplexage des connexions de transport). C'est le

concept de port qui autorise le multiplexage des connexions de transport, un port identifie une extrémité de la connexion. La figure 11.3 illustre la notion de multiplexage de connexion de transport, l'application terminal virtuel (Telnet) est identifiée par le numéro de port 23. Un client qui veut établir une session Telnet fait appel au port distant 23, tandis que localement, pour distinguer cette connexion des autres, il attribue un numéro de port quelconque et unique sur cette machine (> 1 024).

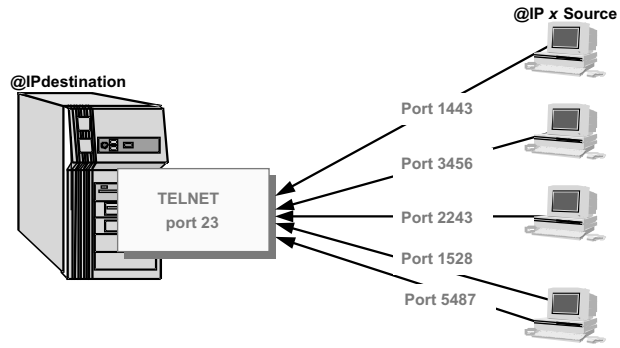


Figure 11.3 Le multiplexage des connexions de transport.

Les 1 024 premières valeurs sont réservées. Les ports identifiés par ces valeurs sont dits **référencés** ou encore ports bien connus (*Well known ports*), ces ports sont liés à des applications spécifiques. Le tableau de la figure 11.4 fournit quelques exemples de numéro de port tels qu'ils sont décrits dans le RFC 1700 (*Assigned numbers*).

Nom du service	Numéro de port/ protocole	Alias	Commentaire
echo	7/tcp		
ftp-data	20/tcp		Protocole de transfert de fichiers
ftp	21/tcp		
telnet	23/tcp		Émulation de terminal
domain	53/udp	nameserveur	Serveur de noms de domaine
x400	104/tcp		Courrier ISO
pop3	110/tcp	postoffice	Bureau de poste
nbsession	139/tcp	netbios_ssn	Session de service Netbios

Figure 11.4 Exemples de numéros de ports référencés (extrait du RFC 1700).

Les ports référencés permettent ainsi, à une application dite cliente, d'identifier une application sur le système distant. L'extrémité de la connexion cliente est identifiée par un numéro de port attribué dynamiquement par le processus appelant (figure 11.5). Ce numéro de port est dit port dynamique ou éphémère. Dans la figure 11.5, le port 23 est un port référencé, les ports *xxxx* sont des ports éphémères attribués par le processus appelant et permettant au système distant d'identifier le flux de données (multiplexage des connexions de transport).

© Dunod – La photocopie non autorisée est un délit

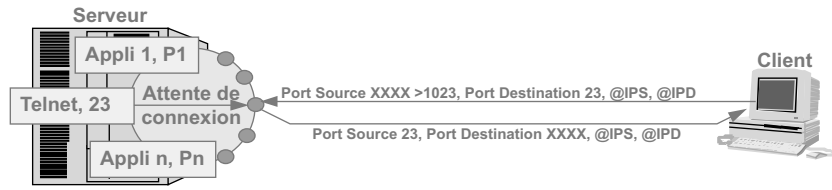


Figure 11.5 Le référencement de la connexion de transport.

11.2.3 L'établissement de la connexion de transport

L'ouverture de connexion de TCP est très similaire à celle de TP4 ISO, c'est une ouverture avec validation en trois phases. Cependant, TCP définit deux modes d'ouverture : le mode passif et le mode actif. Dans le mode passif, TCP est en attente d'une demande d'ouverture en provenance d'un autre système (défini ou non). Dans le mode actif, TCP adresse une demande de connexion à un autre système identifié (figure 11.6).

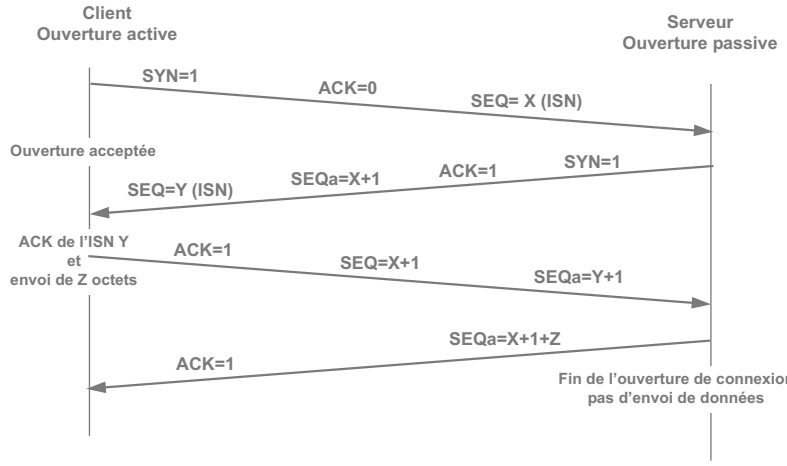


Figure 11.6 L'ouverture d'une connexion en trois temps.

L'ouverture et la fermeture de connexion sont gérées par 2 bits de l'en-tête TCP : le bit SYN et le bit FIN. Ces bits, positionnés à 1, indiquent respectivement une demande d'ouverture de connexion et de rupture de connexion. Pour fiabiliser la connexion et détecter d'éventuels segments perdus, TCP numérote les données transmises. Si HDLC dénombre les trames, TCP compte les octets et ainsi pour chaque segment TCP transmis, il identifie la position (*Offset*), dans le flux de données, du premier octet du segment transmis. Pour des raisons expliquées ci-après, les compteurs ne sont pas initialisés à zéro en début de transmission, mais à une valeur dite ISN (**ISN**, *Initial Sequence Number*). Lors de l'ouverture de connexion, chaque entité informe son correspondant de cette valeur (initialisation des compteurs de part et d'autre).

Ainsi, figure 11.6, pour ouvrir une connexion, l'entité cliente émet une requête de connexion avec le bit SYN positionné à 1, le champ Numéro de séquence (SEQ) contient alors la valeur d'initialisation du compteur d'émission (*X*). Si le destinataire (le serveur) accepte cette connexion, il y répond avec un message dans lequel le bit SYN est à 1, il fournit sa valeur d'initialisation (*Y*)

et acquitte l'ISN de l'appelant en positionnant le bit ACK à 1. L'ACK à 1 indique que le champ Numéro de séquence acquitté contient un acquittement valide (X+1), c'est-à-dire que le prochain segment qu'il doit recevoir portera le numéro de séquence X+1. L'appelant procède de même, il acquitte le numéro de séquence (Y+1). La connexion est ouverte (connexion en trois temps).

La connexion de transport est *full duplex*, chaque sens étant indépendant l'un de l'autre. Il peut être mis fin à un échange dans un sens sans pour cela mettre fin à l'échange dans l'autre sens (semi-fermeture). La fin d'un échange dans un sens peut donc être tout à fait dissociée de la fermeture. La fermeture définitive n'est effective que lorsque chaque sens a clos son échange. La fermeture est dite douce ou négociée évitant ainsi toute perte de données dans le réseau (il n'y a pas de couche session pour contrôler le dialogue).

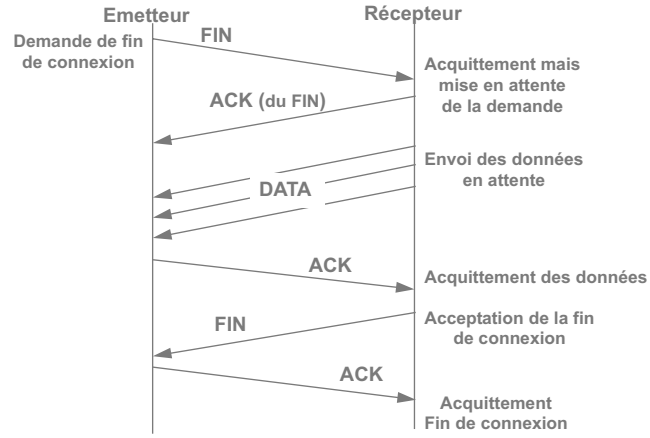


Figure 11.7 La fermeture négociée de TCP.

La figure 11.7 illustre le mécanisme de fermeture douce. Lors de la demande de déconnexion de A (bit Fin = 1). B acquitte la demande de fermeture dans le sens A vers lui, mais s'il a encore des données à envoyer, il les émet, lorsqu'il n'a plus de données à transmettre, il clôt son échange par une demande de déconnexion (Fin = 1). Celle-ci est validée par A, la connexion est fermée.

11.2.4 Le mécanisme contrôle de l'échange

L'ISN

À l'instar d'autres protocoles, pour fiabiliser la connexion et de détecter d'éventuels segments perdus, TCP numérote les octets transmis (numéros de séquence sur 32 bits) et il identifie, dans chaque segment, la position (*Offset*), dans le flux de données, du premier octet de ce segment.

TCP peut, sur un même couple de ports, accepter une nouvelle connexion après fermeture de la précédente. Ainsi, des données appartenant à l'ancienne connexion et retardées dans le réseau peuvent alors être prises en compte sur la nouvelle connexion. Pour différencier ces connexions, TCP attribue à chaque connexion un numéro de séquence initial (**ISN**, *Initial Sequence Number*) différent. Ainsi, le décomptage des octets transmis ne démarre pas à 0, mais à une valeur initialisée

© Dunod – La photocopie non autorisée est un délit

à partir d'une horloge interne[1]. La probabilité pour que le numéro de séquence du segment retardé de la précédente connexion corresponde au numéro de séquence attendu de la nouvelle connexion est très faible.

La gestion des acquittements

TCP utilise le mécanisme de l'anticipation et met en œuvre la technique de la fenêtre glissante, chaque bloc émis doit être acquitté immédiatement. Cependant, supposons une application de type terminal asynchrone (Telnet). L'application cliente émet, pour chaque touche frappée, un segment contenant le caractère et l'application serveur renvoie ce caractère en écho (écho distant), la couche transport envoie un accusé de réception pour chaque message émis (figure 11.8 gauche).

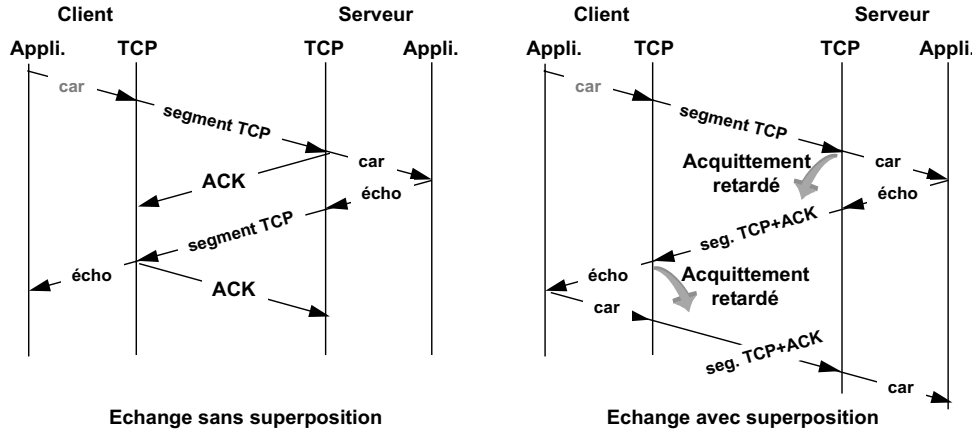


Figure 11.8 Principe de la superposition.

Si on considère l'ensemble des en-têtes TCP et IP, soit 40 octets par message, pour 1 caractère d'utile on a transmis 122 caractères ! Un moyen simple d'augmenter l'efficacité de cette transmission serait de profiter de l'envoi du caractère en écho pour transmettre l'information d'acquittement (figure 11.8 droite). C'est le principe de la superposition (*Piggybacking*), un même segment peut transporter non seulement des données, mais aussi l'acquittement de segments précédents reçus.

Ainsi, pour optimiser l'échange de données, TCP retarde les acquittements dans l'attente de données à transmettre. Pour ne pas nuire à l'interactivité des applications, ce délai d'attente est généralement compris entre 200 ms et 500 ms. Ce retard à l'acquittement ne concerne que les données arrivées en séquence. En cas de réception de données hors séquence, l'acquittement des dernières données reçues correctement est émis immédiatement.

TCP n'acquitte que les données correctement reçues, il n'utilise pas la technique d'acquittement négatif[2] comme le fait HDLC (trame REJ ou SREJ d'HDLC). En effet, l'arrivée de données hors

1. Ce mécanisme a les mêmes objectifs que le gel de référence de TP4 d'ISO. Le compteur d'initialisation est incrémenté toutes les quatre microsecondes, un même ISN est donc tiré toutes les 4 heures 30 environ.

2. TCP n'utilise pas explicitement d'acquittement négatif, mais la réception de trois acquittements successifs de même valeur est assimilée à la réception d'un acquittement négatif. Dans ce cas, le TCP source réémet immédiatement le segment pointé par le champ ACK.

séquence n'implique pas nécessairement une erreur de transmission, mais peut-être un simple retard dans le réseau (IP, mode datagramme). Dans ces conditions, même si les données sont correctement reçues, TCP ne les acquitte pas si leur numéro de séquence est supérieur à celui attendu. Cependant, dans ce cas, il renvoie un acquittement contenant le numéro de séquence attendu. La retransmission des données erronées s'effectue sur temporisation.

Examinons ce mécanisme illustré par la figure 11.9. Pour simplifier la compréhension les données ont été numérotées en N° de segment et non en octets. Ainsi, dans cet exemple, le destinataire a correctement reçu les segments 1 et 2 le segment 3 erroné est ignoré. Compte tenu du mécanisme d'anticipation, le destinataire reçoit les segments 4, 5 et 6. La réception du segment 4, hors séquence, provoque l'émission immédiate d'un acquittement précisant le numéro de segment attendu, c'est-à-dire le 3. Toutes les données reçues hors séquencement sont mémorisées, mais non expressément acquittées, c'est toujours le dernier segment reçu en séquence qui est acquitté. Ainsi l'émetteur reçoit plusieurs acquittements du segment 2 (segment attendu 3). L'émetteur ne réagit pas en effet, IP est un réseau en mode *best effort*, il ne garantit pas la non-duplication des données. Cependant, s'il reçoit trois accusés de réception d'un même segment, il effectue alors immédiatement une retransmission du segment demandé (N° d'octets).

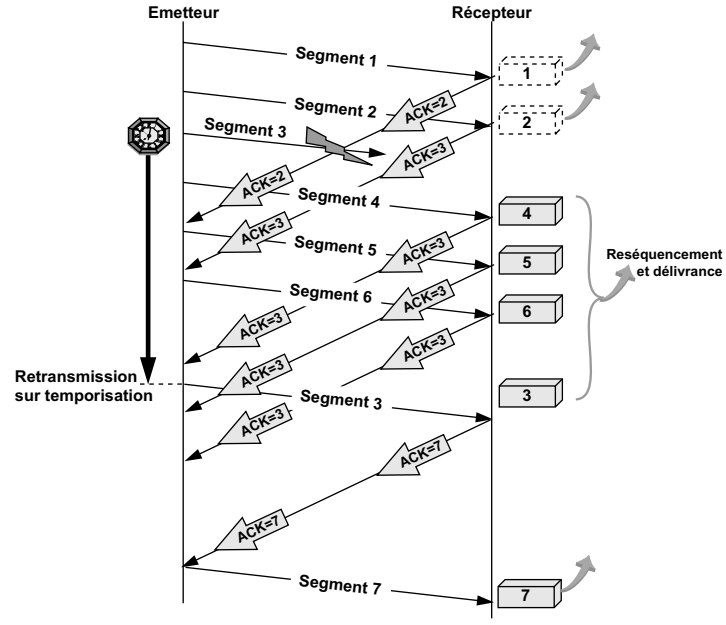


Figure 11.9 La reprise sur temporisation.

Dans notre cas, ne recevant pas d'acquittement du segment 3 (N° attendu 4) avant l'échéance du temporisateur, l'émetteur renvoie le segment 3, et cesse toute émission en attente de l'acquittement de ce block. À réception du segment 3, le récepteur acquitte l'ensemble des segments correctement reçus (acquittement cumulatif). Ainsi, l'acquittement indique que le destinataire est en attente du segment 7. Cette technique permet d'optimiser la transmission en évitant une retransmission de données reçues correctement.

Rappelons que ce sont des octets qui sont transmis et décomptés. En cas de reprise, le TCP émetteur peut émettre un segment plus grand que celui devant être retransmis. De ce fait, certains

© Dunod – La photocopie non autorisée est un délit

octets des segments suivants (5, 6, 7) déjà reçus pourront éventuellement l'être de nouveau. C'est le TCP destination qui gérera la duplication des octets reçus.

La gestion des temporisations

Les délais d'acheminement dans un réseau IP dépendent de nombreux facteurs et en particulier :

– du débit du ou des réseaux traversés,
– de la charge de ceux-ci,
– de la stabilité de route (mode datagramme)...

Dans ces conditions, il ne peut être fait d'hypothèses précises sur les délais d'acheminement et par conséquent sur la valeur des temporisateurs. La reprise sur temporisation (**RTO**, *Retransmission Time Out*) est l'un des facteurs de performance d'un protocole, un délai trop faible conduit à des retransmissions inutiles, un délai trop important à une baisse des performances globales. TCP devant s'adapter à tout type de réseau met en œuvre un mécanisme dynamique de détermination et d'ajustement du RTO. Ce mécanisme permet la prise en compte des variations du temps de transfert dans le réseau, variations pouvant être dues à une variation de charge dans le réseau ou à un changement de route. À cette fin, TCP mesure en permanence le temps écoulé entre l'émission d'un segment et la réception de l'acquittement qui acquitte ce segment (**RTT**, *Round Trip Time*). La figure 11.10 illustre le mode de calcul du RTO.

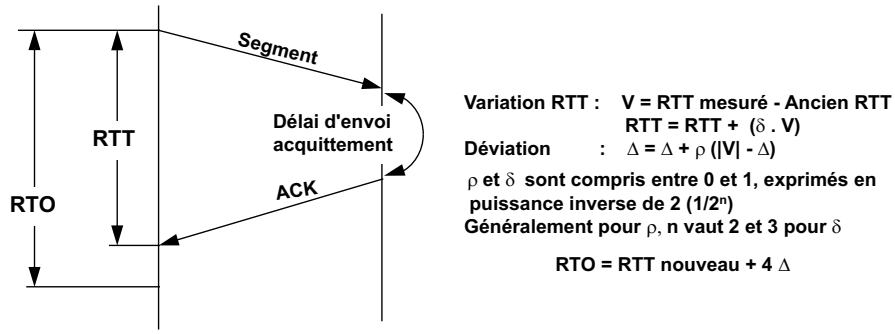


Figure 11.10 Détermination du RTO.

En cas de reprise sur temporisation, TCP fait l'hypothèse d'un accroissement des délais et non d'une perte de segment suite à une erreur. Pour éviter des retransmissions de données correctement reçues, lors de la deuxième retransmission d'un même segment sur temporisation, TCP double la valeur du RTO, à la troisième reprise il le quadruple... De même, lors d'une retransmission, TCP n'évalue pas le RTT, en effet il peut recevoir, en retard, l'acquittement du segment précédemment émis et en déduire alors un RTT trop fort.

11.2.5 Le contrôle de flux et de congestion

Définitions

Contrôle de flux et de congestion sont des mécanismes similaires souvent confondus ; aussi rappelons que :

– le **contrôle de congestion** consiste à contrôler le débit d'émission d'une source en fonction de la capacité du sous-réseau physique réel ;

– le **contrôle de flux** consiste à contrôler le débit d'émission d'une source en fonction de la capacité de réception du destinataire.

Si le contrôle de flux est un mécanisme de point à point entre deux entités communicantes directement reliées. Le contrôle de congestion est, en principe, un mécanisme de surveillance du trafic interne au réseau. Dans un réseau en mode datagramme, ces contrôles ne peuvent être réalisés dans le réseau, ces mécanismes sont alors reportés sur les machines d'extrémité (algorithme distribué). Contrôle de flux et de congestion sont alors réalisés par des mécanismes semblables ; en effet, le contrôle de flux veille à ce qu'aucune donnée ne soit perdue par saturation des *buffers* du destinataire et le contrôle de congestion s'assure qu'aucune donnée ne soit perdue par saturation des mémoires d'un quelconque nœud interne au réseau, il s'agit donc, dans les deux cas, de contrôler le débit de la source. La figure 11.11 illustre les différents cas possibles.

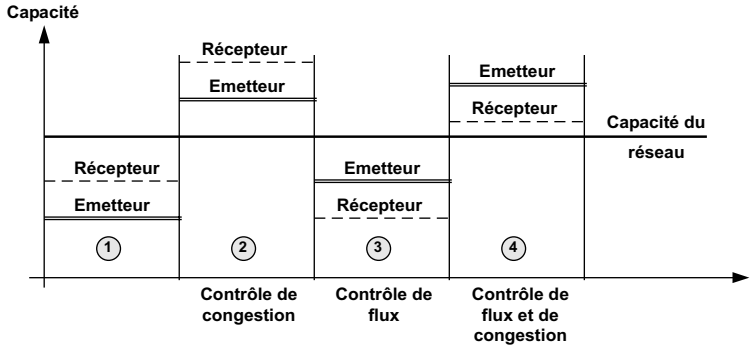


Figure 11.11 Le contrôle de flux et de congestion.

Dans la partie 1 de la figure 11.11 la capacité du récepteur est supérieure aux possibilités l'émetteur, le contrôle de flux n'intervient pas. De même, les possibilités de l'émetteur étant inférieures au trafic assimilable par le réseau, il n'y a aucun risque de congestion résultant de cet échange. Dans la seconde partie, le récepteur a toujours une capacité d'accueil supérieure aux possibilités de l'émetteur, mais celles-ci sont supérieures au débit disponible sur le réseau, le contrôle de congestion doit intervenir pour veiller à ce que l'émetteur ne sature pas le réseau. Dans la troisième partie, il n'y pas de risque de congestion, mais le récepteur doit informer l'émetteur de ses capacités réduites (contrôle de flux). Enfin, la quatrième partie cumule l'action du contrôle de flux et de congestion. En résumé, dans un réseau en mode datagramme, le contrôle de flux et celui de congestion participent du même mécanisme : asservir le débit de la source sur les capacités du récepteur et sur celles du réseau, c'est donc un mécanisme de contrôle par crédit accordé à la source (fenêtre). À cet effet, TCP gère deux fenêtres, une de contrôle de congestion et une de contrôle de flux. Ces deux fenêtres sont indépendantes l'une de l'autre, le TCP émetteur limite ses émissions à la plus petite des deux valeurs :

W_émission = Min [W_contrôle_de_flux (Indication du récepteur), W_congestion]

Hors état de congestion, la fenêtre de contrôle de flux et celle de contrôle de congestion sont identiques.

© Dunod – La photocopie non autorisée est un délit

Le contrôle de flux

➤ Principe

Le contrôle de flux est traité de manière analogue à celui de la couche transport d'ISO. Il s'agit d'un mécanisme à **fenêtre dynamique** ou **contrôle de flux explicite**. Le crédit accordé est un crédit d'octets et non pas de TPDU comme TP4 d'ISO. Ce mécanisme peut conduire à un blocage des systèmes en cas de réduction de la fenêtre, par le destinataire, et de déséquencement dans l'arrivée des informations d'évolution de la fenêtre. TP4 d'ISO résout ce problème par la sous-numérotation des ACK, TCP n'y apporte aucune solution.

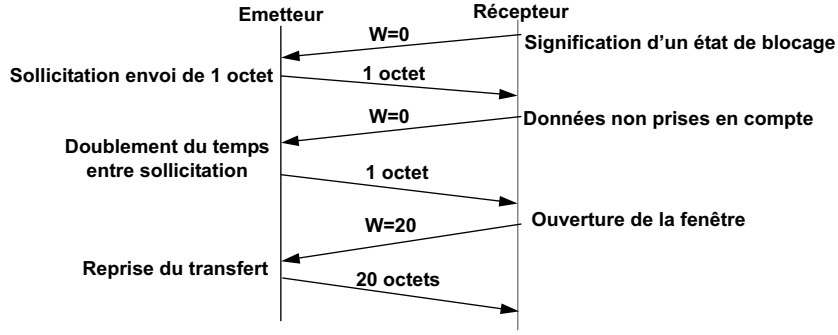


Figure 11.12 Principe du contrôle de flux par TCP.

Dans la figure 11.12, le *buffer* du récepteur est plein, ce dernier ne peut plus accepter de données. Il en informe l'émetteur en positionnant dans l'acquittement le champ Fenêtre à 0. L'émetteur cesse ses émissions. Cependant, pour maintenir l'état actif de la connexion, l'émetteur sollicite périodiquement le récepteur en lui envoyant 1 octet de données. Tant que le récepteur ne peut accepter de données, il ignore l'octet reçu, et continue de signaler une valeur de la fenêtre à zéro. Le processus se poursuit jusqu'à ce que le récepteur débloque la situation en ouvrant la fenêtre.

➤ Notion de fenêtre stupide (*Silly Window Syndrome, SWS*)

Supposons que le *buffer* du récepteur se vide lentement. Il va ouvrir la fenêtre d'une petite quantité, l'émetteur va alors immédiatement envoyer des données. La fenêtre se referme. L'équilibre ne sera trouvé que par l'envoi de petits segments. Le réseau est alors mal utilisé. Plusieurs mécanismes, côté émetteur et récepteur, peuvent être utilisés pour éviter ce phénomène. Notamment le récepteur ne peut rouvrir la fenêtre que lorsque celle-ci a atteint la valeur minimale comprise entre :

– la taille maximale du segment[3] de données convenue (**MSS**, *Maximum Size Segment*),
– et la moitié de la mémoire allouée à la connexion.

Du côté émetteur, il suffit de mémoriser les données pour éviter l'envoi de petits segments (groupage).

3. Une option de TCP permet d'indiquer à la source la taille maximale de segment admise par le destinataire.

Le contrôle de la congestion

➤ Principe

Le mécanisme décrit ci-dessus concerne l'asservissement de la cadence d'émission sur les capacités de réception du destinataire, il réagit en fonction de l'occupation de la mémoire tampon du récepteur ; il s'agit d'une technique de contrôle de flux. La congestion se détecte, soit par un allongement des temps de transit : les acquittements sont retardés, soit par une perte de données : les acquittements n'arrivent pas ! TCP considère que toute perte de segment (reprise sur temporisation) est due à un état de congestion.

À chaque segment perdu, le TCP émetteur réduit ses émissions (gestion d'une fenêtre de congestion) par réduction dichotomique de la fenêtre de congestion et, pour ne pas surcharger de réseau de retransmissions peut-être inutiles, il augmente la valeur du *timer* de retransmission (RTO). Lors de la disparition de la congestion, si TCP procédait de façon inverse (augmentation exponentielle de la fenêtre de congestion), le système serait en état instable oscillant entre les deux états congestion/pas congestion. Aussi tout démarrage du système adopte une technique simple, la fenêtre de congestion est fixée à 1 et s'accroît à chaque réception d'acquittement (démarrage lent), l'objectif étant la recherche du débit maximal autorisé par le réseau. Cette recherche peut être limitée par la fenêtre de contrôle de flux si celle-ci est inférieure aux capacités de réseau.

➤ Le démarrage lent et l'évitement de congestion

Deux techniques de démarrage lent et de traitement de la congestion peuvent être mises en œuvre par TCP/IP, le principe en est le même. Une phase de démarrage, dite démarrage lent (*Slow start*) fixe la fenêtre de congestion à un segment. À chaque accusé de réception reçu, cette fenêtre est doublée (figure 11.13).

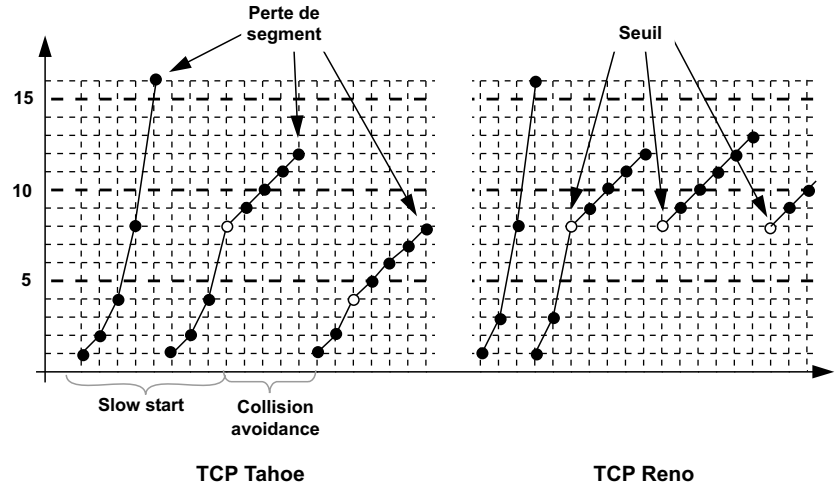


Figure 11.13 Le démarrage lent et l'évitement de congestion.

Toute perte de segment est supposée due à un état de congestion. Dès que celle-ci apparaît, une phase de redémarrage est réinitialisée. Mais pour éviter un retour rapide à l'état de congestion, dès que les segments émis ont atteint la moitié de la fenêtre de congestion, la progression n'est plus exponentielle mais linéaire (évitement de congestion ou *collision avoidance*). Cet algorithme (TCP

© Dunod – La photocopie non autorisée est un délit

Tahoe) utilise mal les ressources du réseau puisqu'il redémarre une phase d'émission à 1 segment. L'autre version dite Reno, la plus implémentée, ne refait que la phase d'évitement de congestion, cernant ainsi mieux le débit maximal permis.

11.3 LE MESSAGE TCP ET LES MÉCANISMES ASSOCIÉS

11.3.1 La structure du segment TCP

TCP ne définit qu'un seul format de segment contre dix pour les messages de transport du modèle de référence. De ce fait, l'en-tête de TCP est prévu à la fois pour le transport des données, la gestion des acquittements et l'envoi de commandes (figure 11.14).

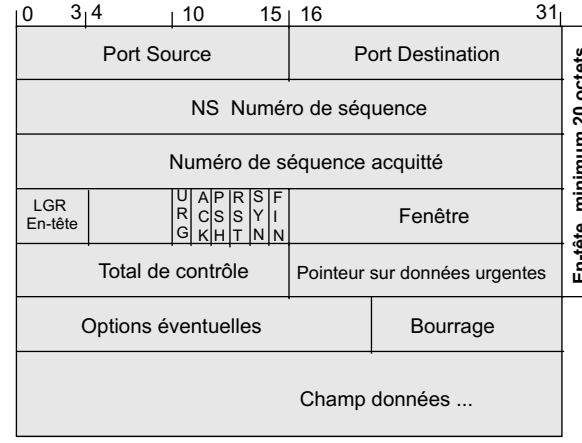


Figure 11.14 La structure de la TPDU ou segment TCP.

Les différents champs de l'en-tête du segment sont :

– **Numéro de port** (deux fois 16 bits), valeurs spécifiées à la connexion, et identifiant celle-ci. Le port du programme appelé est soit connu, soit défini lors d'une phase d'identification (login) et passé à l'appelant en réponse.
– **Numéro de séquence** sur 32 bits, une valeur initiale et aléatoire (**ISN**, *Initial Sequence Number* ou numéro de séquence initial) est définie et acquittée par chaque système d'extrémité lors de la phase de connexion. Le numéro de séquence indique le rang du premier octet du segment transmis, les octets sont décomptés depuis le début de la connexion (Ns = ISN + Nb octets transmis + 1). Le numéro de séquence du premier octet de données transmis est (ISN +1).
– Le **numéro de séquence acquitté** indique le numéro du prochain octet attendu, c'est-à-dire le numéro de séquence du dernier segment reçu, incrémenté de la taille des données reçues.
– **Longueur de l'en-tête** ou *offset* (4 bits) indique la longueur de l'en-tête du segment TCP en multiples de 4 octets. La valeur 5 correspond à taille minimale de l'en-tête TCP (20 octets). Le champ longueur d'en-tête pointe sur le début des données.
– Un espace de 6 bits est disponible.

– Le champ Drapeau contient six indicateurs[4] :

  a) **URG** valide le contenu du champ « pointeur sur données urgentes ». Si ce bit est positionné à 1, le segment transporte des données à traiter en urgence.
  b) **ACK**, le bit ACK à 1 valide le contenu du champ « numéro de séquence acquitté ».
  c) **PSH**, TCP peut, pour des raisons d'efficacité du protocole, attendre d'avoir suffisamment de données à transmettre pour former un segment (algorithme de Nagle). L'indicateur *Push* permet de demander à l'émetteur de transmettre immédiatement les données en attente et au destinataire de les traiter sans retard. Par exemple, l'application terminal virtuel associe, au caractère retour chariot (CR), la commande PSH.
  d) **RST**, suite à la détection d'une anomalie grave sur le réseau, RST demande au destinataire de réinitialiser la connexion.
  e) **SYN**, à 1 ce bit correspond à une demande de connexion, cet indicateur valide l'échange et l'acquittement des numéros de séquence initiaux (ISN).
  f) **FIN**, ce drapeau correspond à une demande de déconnexion émise par l'un des interlocuteurs. Le destinataire d'une demande de déconnexion n'est pas obligé de s'exécuter (rupture de connexion négociée).

– Le champ **fenêtre** (2 octets) indique, en octets, la valeur de la fenêtre en réception, cette valeur varie dynamiquement en fonction de l'état du récepteur (contrôle de flux).
– Le **total de contrôle** (*Checksum*) est calculé sur l'ensemble du segment TCP, en-tête compris, le mode de calcul en est expliqué ci-dessous.
– Le **pointeur sur données urgentes** pointe sur le dernier octet urgent du champ de données. Dans TCP, il n'y a pas de notion de données express, les données comprises entre le début du champ données et la valeur du pointeur données urgentes sont traitées, en priorité, par le destinataire.

11.3.2 Le contrôle d'erreur

TCP et UDP utilisent tous les deux la même technique de contrôle d'erreur. Deux objectifs sont assignés au total de contrôle :

– s'assurer que les données transmises n'ont pas été altérées durant le transfert ;
– garantir que les données sont délivrées au bon destinataire.

À cet effet, TCP utilise une technique particulière. Pour le calcul, il adjoint au segment TCP (ou UDP) un pseudo en-tête contenant, notamment, les adresses IP source et destination. L'inclusion de ces adresses dans l'en-tête de contrôle permet de protéger celles-ci par le total de contrôle. Le calcul du total de contrôle porte donc sur les données, l'en-tête TCP (ou UDP) et le pseudo en-tête IP (figure 11.15). Le récepteur effectue le calcul de la même manière, il reconstitue le pseudo en-tête à l'aide de sa propre adresse IP et des informations extraites de l'en-tête IP du datagramme reçu (adresse IP...). Cette manière de procéder garantit l'intégrité des données et la délivrance au bon destinataire, mais est en violation avec la règle d'indépendance des couches.

4. Un segment TCP où les bits SYN, URG, PSH et FIN sont à 1 et qui ne contient qu'un octet de données est nommé « paquet Kamikaze ».

© Dunod – La photocopie non autorisée est un délit

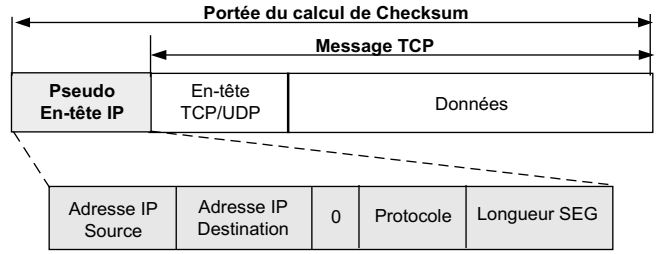


Figure 11.15 La portée du contrôle d'erreur dans UDP et TCP.

Le mode de calcul est identique à celui mis en œuvre par IP. Il s'agit du complément à 1 de la somme en complément à 1 des mots de 16 bits du segment TCP (UDP), pseudo en-tête inclus. Le pseudo en-tête n'est pas transmis, il est reconstitué par le destinataire.

11.3.3 La « bufferisation » des données

Pour optimiser la transmission, TCP attend, avant de transmettre des données, que le *buffer* d'émission soit plein (réduction des *overhead*). Cette technique est dénommée groupage (*clumping*). Certaines applications, notamment les applications de type terminal virtuel, peuvent exiger la transmission immédiate. La demande de positionnement du bit PUSH contraint le TCP émetteur à transmettre les données sans attendre, et le TCP récepteur à délivrer, immédiatement les données reçues à l'application. Le mécanisme du *clumping* est illustré figure 11.16.

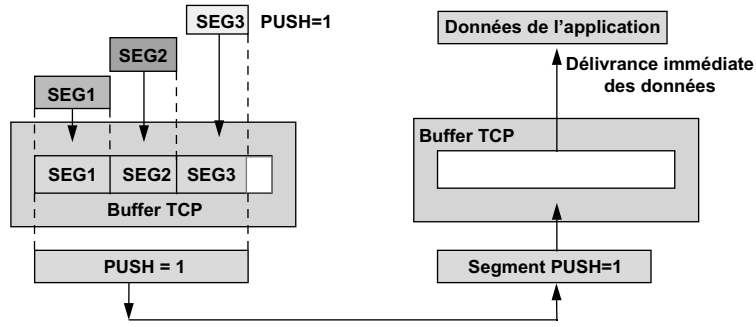


Figure 11.16 La fonction du bit PUSH.

Ainsi, par exemple, le bit PUSH est positionné à la fin de chaque séquence Commande/Réponse d'une application interactive et lors du dernier bloc d'un transfert de fichier sous FTP.

11.4 LES OPTIONS DE TCP

Les options de TCP définissent les paramètres de la connexion. Les principales concernent la détermination de la taille maximale des segments à échanger (MSS), le calcul du temps de transit dans le réseau TCP (RTT) et la taille de la fenêtre de transmission.

11.4.1 La taille des segments

Lors de l'établissement de la connexion de transport, l'option **MSS** (*Maximum Segment Size*) permet l'annonce, et non la négociation, de la taille maximale de segment que le système d'extrémité peut admettre. Cette option ne peut apparaître que dans un message d'ouverture (bit SYN=1). À défaut d'annonce si l'application est locale, la MSS correspondra à la MTU du réseau diminuée des en-têtes TCP et IP, soit 40 octets. Dans le cas contraire (applications distantes), la MTU est fixée à 576 octets et la MSS à 536 octets (figure 11.17). Cette valeur garantit une charge utile minimale de 512 octets aux données de l'application.

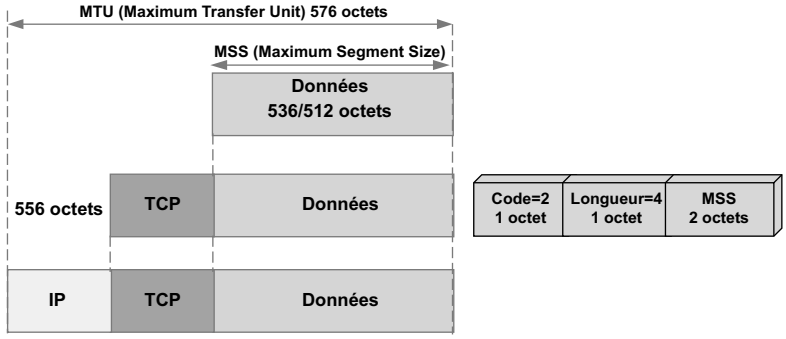


Figure 11.17 La relation entre MTU et MSS, et le format de l'option.

11.4.2 L'option d'estampille horaire

Les performances globales de TCP reposent sur la détermination du RTT, donc sur la mesure du délai d'acheminement aller et retour dans le réseau. La plupart des implémentations de TCP réalisent cette mesure en calculant le temps entre l'émission d'un segment et la réception d'un acquittement. Compte tenu que TCP n'accuse pas expressément un segment mais plusieurs (acquittement cumulatif), le RTT calculé, dans ces conditions, n'est acceptable que si la fenêtre est petite. La mesure du délai de transit dans le réseau pourrait être obtenue en indiquant dans le segment TCP l'heure d'émission et, à partir de l'heure de réception en déduire le temps de transit. Ce mode de calcul nécessiterait que tous les routeurs du réseau soient synchronisés sur une horloge unique, ce qui n'est pas envisageable. L'option d'estampille horaire permet à TCP de déterminer avec précision le délai aller et retour dans le réseau, temps de traitement du destinataire compris. La figure 11.18 représente le format de l'option d'estampille horaire.



Figure 11.18 Le format de l'option estampille horaire.

Le TCP émetteur indique sur 32 bits l'instant d'émission dans le champ réservé à cet effet, ce champ sert de référence temporelle. Le TCP destinataire retourne cette option en écho en indiquant son instant d'émission. Le RTT est déterminé par l'émetteur par différence entre l'instant d'émission de l'estampille horaire et l'instant de réception de son écho. L'estampille horaire du récepteur ne sert qu'à lever les ambiguïtés en cas d'acquittement retardé ou autre.

© Dunod – La photocopie non autorisée est un délit

11.4.3 Le TCP et les réseaux à haut débit

Les performances maximales d'un protocole à anticipation sont atteintes lorsque le crédit de l'émetteur, exprimé en temps d'émission, correspond au délai aller et retour dans le réseau (RTT). Le volume de données correspondant porte le nom de fenêtre. Elle a pour valeur :

$$\text{Fenêtre en bits} = \text{débit du lien (réseau)} \times \text{RTT}$$

Cette valeur est dénommée, en TCP, **capacité du réseau**. La figure 11.19 indique pour quelques exemples de réseaux cette valeur.

Débit	Capacité en octets		
	RTT 100 ms	RTT 200 ms	RTT 500 ms
64 kbit/s	800	1 600	4 000
128 kbit/s	1 600	3 200	8 000
256 kbit/s	3 200	6 400	16 000
512 kbit/s	6 400	12 800	32 000
1 024 kbit/s	12 800	25 600	64 000
2 048 kbit/s	25 600	51 200	128 000
34 Mbit/s	51 200	102 400	256 000

Figure 11.19 La capacité du réseau.

Dans l'en-tête du segment TCP, l'expression de la taille de la fenêtre de TCP est limitée à 16 bits, ce qui correspond à une capacité de 65 535 octets (2^{16}). Dans ces conditions, TCP est mal adapté aux réseaux dont le produit Débit par RTT est important (réseaux dits *Long Fat Network*, **LFN**, ou réseau éléphant !). En effet, une fenêtre plus petite que la capacité du réseau provoque, dans l'attente d'un acquittement, l'arrêt des émissions. Aussi pour adapter TCP aux réseaux à haut débit où aux réseaux à latence importante (liaison satellite), la capacité de numérotation de la fenêtre a été accrue (option d'échelle de fenêtre, RFC 1323). L'option d'échelle de fenêtre ne peut être invoquée que lors de l'ouverture de connexion (SYN), elle ne peut être mise en œuvre que si les deux parties l'invoquent[5]. L'option d'échelle indique en puissance de 2 le décalage de la fenêtre. Ainsi si la valeur est de 1, la fenêtre utilisée sera de $65\,535 \times 2^1$, si le décalage est de 2 la valeur de fenêtre est de $65\,535 \times 2^2$... La figure 11.20 illustre le format de l'option d'échelle de fenêtre.

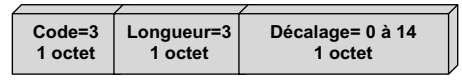


Figure 11.20 L'option échelle de fenêtre.

Les en-têtes TCP devant être alignés sur des mots de 32 bits, si nécessaire, l'option « alignement d'en-tête » de longueur totale 1 octet (code option 1) est utilisée. La liste d'options est toujours terminée par l'option « fin de liste d'options » (code=0).

5. Si une des extrémités peut accepter l'option d'échelle, mais ne veut pas l'utiliser pour ses émissions, elle accepte l'option distante en invoquant elle aussi l'option d'échelle mais avec une valeur nulle.

11.5 LE MODE DATAGRAMME (UDP)

Certaines applications et en particulier les applications temps réel nécessitent des temps de traitement optimisés, d'autres n'ont que très peu de données à envoyer, comme, par exemple le service de noms (DNS), d'autres encore n'ont nullement besoin d'un service sécurisé comme l'offre TCP, c'est par exemple de cas des informations de gestion des réseaux (SNMP). Dans tous ces cas, les mécanismes mis en œuvre par TCP s'avèrent lourds et pénalisent les performances. Aussi, un mode de transport allégé a-t-il été défini, ce mode est appelé UDP (*User Datagram Protocol*).

Le segment (datagramme) UDP ne contient que les champs ports source et destination (deux fois 2 octets, les valeurs attribuées sont différentes de celles de TCP), le champ longueur totale du datagramme (en-tête compris sur 2 octets), le champ total de contrôle (2 octets) et les données utilisateurs (figure 11.21). Le *checksum* UDP est calculé comme celui de TCP pseudo en-tête IP compris. Son utilisation est facultative, en cas de non-utilisation le champ *Checksum* est mis à zéro.

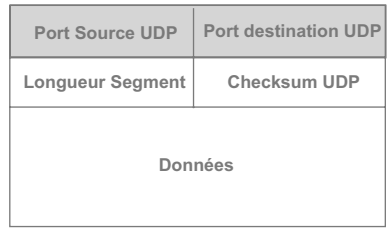


Figure 11.21 Le format du segment UDP.

11.6 CONCLUSION

La pile protocolaire TCP/IP offre deux modes de transport, un mode assuré, TCP, qui garantit la délivrance de données, assure le contrôle de flux et de congestion, et un mode allégé, UDP, gage de performance mais sans garantie de délivrance. Les applications traditionnelles utilisent TCP pour sa fiabilité, tandis que les applications dites temps réel comme la voix et la vidéo s'appuient sur UDP. Dans un réseau à bande passante limitée, les applications de type vidéo non soumises au contrôle de flux pénalisent les applications traditionnelles (figure 11.22).

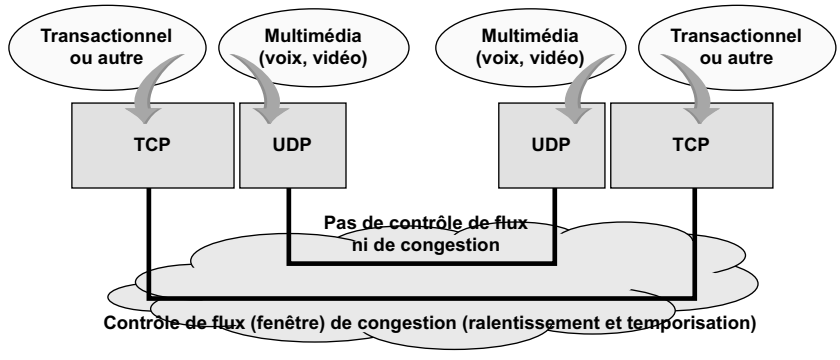


Figure 11.22 Le partage de la bande passante par TCP et UDP.

© Dunod – La photocopie non autorisée est un délit

Entre les applications du type transfert de fichiers et les applications temps réel, les applications du type transactionnel nécessitent la fiabilisation de TCP et les performances d'UDP. Le RFC 1379 décrit une extension de TCP dénommée T/TCP (*Extending TCP for Transaction-Concepts*) afin d'adapter celui-ci à l'environnement transactionnel.

EXERCICES

Exercice 11.1 Trace TCP/IP

La trace reproduite ci-dessous (figure 11.23) a été réalisée sur réseau de type Ethernet. Analysez et fournissez toutes les informations relatives au protocole utilisé. Dans la deuxième trame proposée, ne commentez que les parties intéressantes vis-à-vis de ce qui a déjà été commenté dans la première trame.

```
Captured at:  +00:03.934
Length: 114    Status: Ok
OFFST DATA                                                  ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 60 3C EF 00 00 1C 06 A4 FE 80 00 64 01 D0 80  .`<.........d...
0020: 08 29 00 17 04 2B 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D3 00 00 FF FB 01 FF FD 01 0D 0A 0D 0A   .r.............
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56  UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65   Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00 9F 59  vsa00).........Y
0070: 6E FC                                             n.

Captured at:  +00:04.771
Length: 64    Status: Ok
OFFST DATA                                                  ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 29 3C F2 00 00 1C 06 A5 32 80 00 64 01 D0 80  .)<......3..d...
0020: 08 29 00 17 04 2B 47 A8 BA 62 01 A3 96 1B 50 18  .)...+G..b....P.
0030: 20 00 D2 14 00 00 63 00 00 08 00 00 69 55 A1 FF   .....c.....iU..
```

Figure 11.23 La trace TCP/IP.

La structure générale de l'encapsulation du datagramme IP dans une trame Ethernet est donnée figure 11.24.

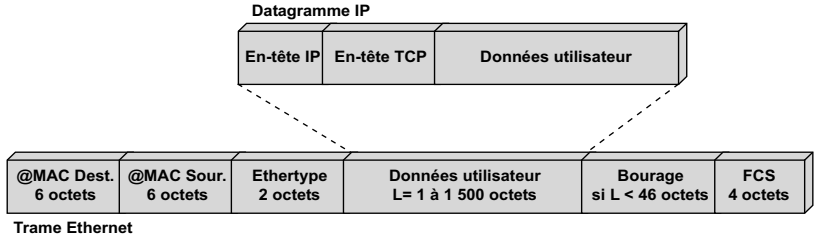


Figure 11.24 L'encapsulation de TCP/IP dans une trame MAC Ethernet V2.

Exercice 11.2 Efficacité de TCP

Si l'option d'extension de fenêtre n'est pas utilisée, quelle est l'efficacité d'une liaison satellite (RTT # 500 ms) dont le débit nominal est de 1 Gbit/s ? Dans ces conditions, quel devrait être le débit de la liaison pour obtenir une efficacité maximale ?

Exercice 11.3 Comparaison transport TCP et transport ISO

Rapprochez les protocoles de transport TCP et ISO en en faisant ressortir les similitudes et les différences.

© Dunod – La photocopie non autorisée est un délit

Chapitre **12**

TCP/IP et les applications

12.1 INTRODUCTION

Contrairement à ce qui est fréquemment écrit, l'environnement TCP/IP ne possède pas de couche application, mais des applications indépendantes les unes des autres. Celles-ci s'appuient directement sur TCP ou UDP et non sur des services de niveau application comme le font les applications du modèle de référence (entité d'application dans le modèle OSI). Le programmeur doit intégrer à ses applications tous les services manquants de l'environnement TCP. Ce chapitre n'a pas pour objectif de décrire toutes les applications définies par une RFC mais seulement quelques-unes d'entre elles parmi les plus mises en œuvre.

12.2 LES NOTIONS D'ANNUAIRE

12.2.1 Généralités

Un annuaire est un système permettant, à partir d'une information, d'en connaître une autre. L'annuaire téléphonique fournit, à partir d'un nom, le numéro de téléphone et généralement l'adresse de la personne concernée. Un annuaire électronique[1] est une base de données consultable par une application, il délivre à cette dernière les informations nécessaires à son bon fonctionnement. Par exemple, une application peut consulter un annuaire pour y connaître les droits d'un utilisateur.

1. Un annuaire électronique est une base de données, une base de données n'est pas un annuaire. Ce qui distingue essentiellement un annuaire d'une base de données, c'est l'utilisation que l'on en fait. Un annuaire offre essentiellement des services de consultation, alors qu'une base de données offre en plus des services de mise à jour (application de type transactionnel).

12.2.2 Le service de noms (DNS)

Principe

Rappelons que le nommage est une notion complémentaire de celle de l'adressage, l'un désigne l'objet (objet nommé) l'autre sa localisation[2]. Dans l'environnement TCP/IP, le service de noms consiste simplement à associer un nom à une adresse IP (résolution de noms). Ce service peut être rendu simplement par lecture d'un fichier local (ect/host, figure 12.1) ou par consultation d'un annuaire électronique : le **DNS**[3], base de données distribuée s'appuyant sur les protocoles de transport UDP et TCP (messages de plus de 512 octets). Le port 53 est utilisé dans les deux cas (TCP et UDP).

```
# Copyright (c) 1993-1999 Microsoft Corp.
#
# Ceci est un exemple de fichier HOSTS utilisé par Microsoft TCP/IP
# pour Windows.
#
# Ce fichier contient les correspondances des adresses IP aux noms d'hôtes.
# Chaque entrée doit être sur une ligne propre. L'adresse IP doit être placée
# dans la première colonne, suivie par le nom d'hôte correspondant. L'adresse
# IP et le nom d'hôte doivent être séparés par au moins un espace.
#
# De plus, des commentaires (tels que celui-ci) peuvent être insérés sur des
# lignes propres ou après le nom d'ordinateur. Ils sont indiqués par le
# symbole '#'.
#
# Par exemple :
#       Adresse IP       Nom                   Commentaire
#       102.54.94.97     rhino.acme.com        # serveur source
#       38.25.63.10      x.acme.com            # hôte client x

        127.0.0.1        localhost             # cette machine
```

Figure 12.1 Exemple de résolution de nom par fichier.

D'origine **IAB** (*Internet Activities Board*), le DNS est une base de données distribuée basée sur le modèle relationnel client/serveur. La partie cliente, le solveur (*resolver)*, est chargée de résoudre la correspondance entre le nom symbolique de l'objet et son adresse réseau. En introduisant un nommage hiérarchique et la notion de domaine (chaque nœud de la hiérarchie peut être un domaine ou sous-domaine de nommage), le DNS présente les avantages suivants :

– gestion simplifiée du nommage (nommage hiérarchique) ;
– délégation et répartition des responsabilités d'attribution de noms et d'administration par domaine de nommage ;
– duplication possible de la base (notion de serveur maître ou primaire et de serveur secondaire), le serveur secondaire pouvant répondre à une requête si le serveur principal est occupé. La mise à jour se fait uniquement sur le serveur maître avec réplication automatique des données modifiées sur le serveur secondaire ;
– indépendance vis-à-vis d'un constructeur, les *resolvers* DNS sont, en principe, disponibles dans tous les environnements TCP/IP.

2. Dissociant l'objet de sa localisation géographique, certains désignent le nom sous le terme d'adresse logique. Or, le concept IP de réseau logique tend plutôt à réserver à l'adressage du réseau logique le terme d'adresse logique.

3. De façon plus stricte : **DNS** (*Domaine Name System*) désigne l'ensemble des organismes qui gèrent les noms de domaine, **DNS** (*Domain Name Service*) correspond au protocole d'échange d'information entre les domaines, enfin **DNS** *(Domain Name Server*) représente le serveur de noms.

L'espace de nommage

Les noms sont organisés selon une structure arborescente hiérarchique (arbre inversé) appelée **espace de nommage** (figure 12.2). La racine est au sommet, son nom de domaine est vide, elle est symbolisée par un point « • ». Le nombre de niveaux est limité à 127. Un nom ne peut dépasser 255 caractères et chaque niveau est limité à 63 caractères. La RFC 1032 préconise de limiter à 12 caractères le nom attribué à chaque niveau (nœud). Il n'y a pas de distinction Minuscule/Majuscule. S'ils sont dans des domaines différents, des nœuds peuvent avoir des noms identiques.

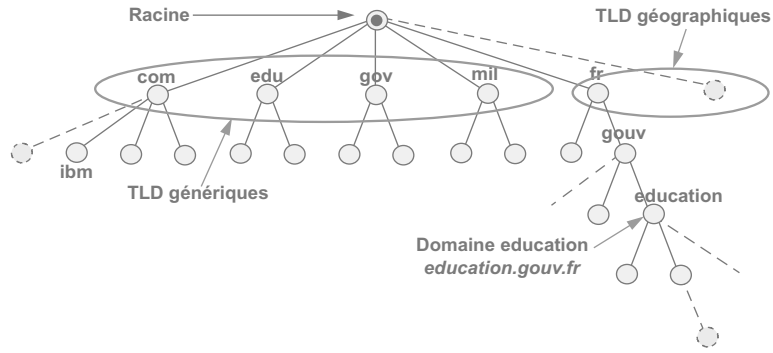


Figure 12.2 La structure de l'espace de nommage.

Les premiers niveaux de la hiérarchie de la figure 12.2 ou **TLD** (*Top Level Domain*), gérés par l'**ICANN** (*Internet Corporation for Assigned Names and Numbers*) sont regroupés en deux ensembles : les gTLD (*generic* TLD, TLD génériques) et les ccTLD (*country code* TLD, TLD géographique). La gestion en est confiée à des organismes régionaux (*Registry*) et la commercialisation à des organismes privés (*Registrar*). En France c'est AFNIC (Association française pour le nommage Internet en coopération) qui gère l'espace de nom « .fr » et la commercialisation en est assurée par Renater, Tiscali Telecom, Globenet...

Aucune signification n'est imposée aux noms de domaine, sauf pour le premier niveau :

- **com**, organisations commerciales possédant, en principe, des implantations sur plusieurs domaines géographiques (ibm.com) ;
- **edu**, établissements d'enseignement (réservé aux établissements des États-Unis, mit.edu) ;
- **gov**, établissements gouvernementaux (États-Unis, nsf.gov) ;
- **mil**, organisations militaires américaines (États-Unis, army.mil) ;
- **net**, organisations du réseau Internet (bull.net) ;
- **org**, organisations non commerciales et non gouvernementales à but non lucratif (ong.org) ;
- **int**, organisations internationales (onu.int) ;
- **arpa**, domaine réservé à la résolution de nom inversée ;
- **aero**, domaine réservé aux entreprises du secteur aéronautique ;
- **biz**, pour les entreprises commerciales ;
- **coop**, pour les coopératives ;
- **museum**, pour les musées ;

© Dunod – La photocopie non autorisée est un délit

– **name**, pour les particuliers ;
– **pro**, pour les professions libérales ;
– domaines nationaux dont la dénomination est limitée à deux caractères (fr, uk, it...).

Dans le réseau Internet, la racine (*Root*) est l'élément de base de toute la hiérarchie sur laquelle repose le fonctionnement d'Internet. Aussi la gestion des TLD de premier niveau est-elle répartie sur 15 serveurs répartis à travers le monde. Ces serveurs appartiennent au domaine ***root-servers.net***. Le serveur maître A.root-server.net (États-Unis) est géré par VeriSign Global Registry Services, les autres serveurs sont des serveurs miroirs désignés sous les noms de B.root-servers.net, C.root-servers.net... K.root-servers.net (sous la responsabilité du RIPE NCC et situé en Grande Bretagne)...

La résolution de nom

➤ Principe

Un nœud est désigné par l'arborescence complète de son nom (**FQDN**, *Fully Qualified Domain Name*). La résolution est l'opération qui consiste à mettre en relation le nom du nœud et son adresse IP. Le client DNS ou solveur (*Resolver*) est un programme de type *daemon*. Sur sollicitation d'un programme demandeur, il est chargé d'émettre les demandes et de traduire les réponses. Lors de la configuration d'une station IP, on lui fournit son nom de domaine, l'adresse de son serveur local de noms et, éventuellement, une liste ordonnée de serveurs de noms.

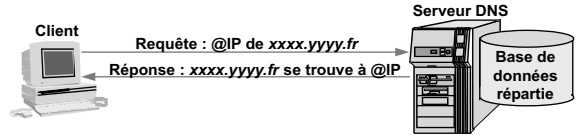


Figure 12.3 La résolution de nom.

Le client solveur (figure 12.3) interroge le serveur de noms local. Si la recherche est infructueuse le serveur local interroge le serveur de niveau supérieur (recherche récursive) ou le client interroge lui-même d'autres serveurs (requête itérative).

Lorsque le programme d'application formule une demande, le *resolver* interroge son cache (figure 12.4 gauche) : si la correspondance Nom/@IP y est déjà enregistrée, il fournit directement la réponse au programme demandeur.

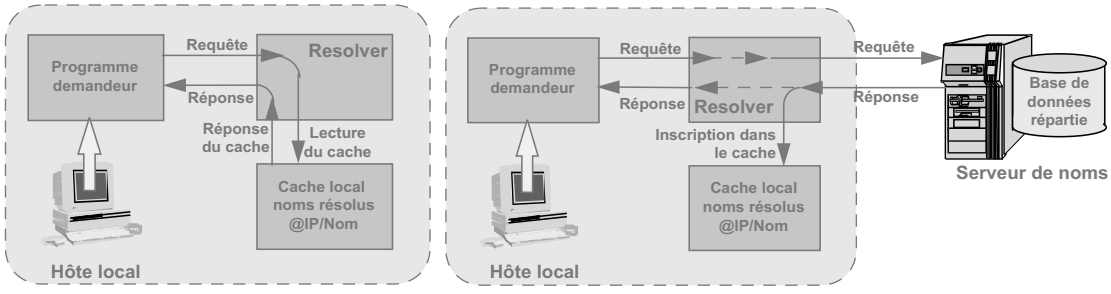


Figure 12.4 Le fonctionnement du resolver.

Sinon, il émet une requête au serveur DNS. Celui-ci résout la demande, directement ou par requêtes itératives ou récursives. Le solveur analyse la réponse, met à jour son cache et fournit la réponse au demandeur (figure 12.4 droite).

D'une manière générale, une recherche de type récursif consiste à déléguer à un serveur de noms la responsabilité de la résolution, tandis qu'une requête itérative consiste à formuler autant de questions que nécessaire. En principe, un client émet des requêtes de type récursif, charge au serveur d'émettre, si besoin, des requêtes de type itératif pour rechercher la réponse.

➤ Résolution inverse

À l'instar de la résolution d'adresses (RARP), la résolution de noms inverse permet d'obtenir, à partir de l'adresse IP, le nom de la machine. Le domaine arpa, sous-domaine in-addr, a été prévu à cet effet (figure 12.5).

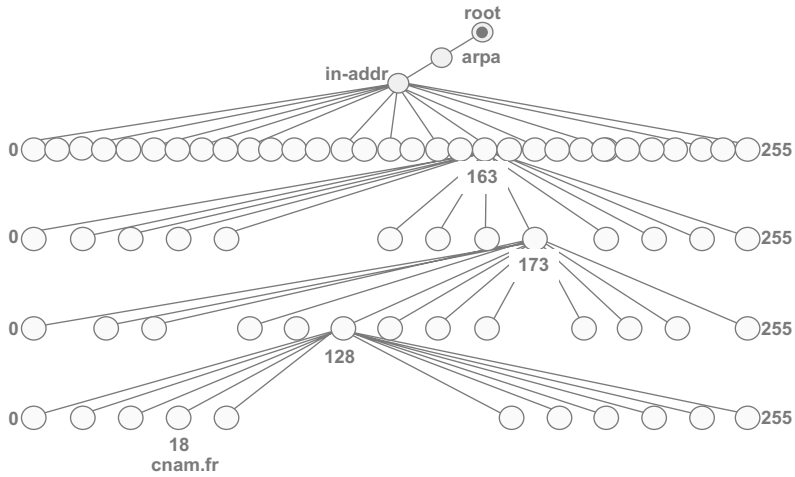


Figure 12.5 L'arbre de résolution inverse.

L'arbre inverse considère l'adresse comme un nom : par exemple l'adresse du Conservatoire national des Arts et Métiers (163.173.128.18) est traduite par 18.128.173.163.in-addr.arpa. À chaque octet de l'adresse IP correspond un nœud de l'arbre. Chaque sous-domaine ainsi défini comporte 256 sous-domaines. Le quatrième niveau correspond au nom du serveur connaissant le nom de domaine associé à cette adresse.

➤ Structure des messages

La figure 12.6 illustre la structure générale d'un message DNS. Le message est composé d'un entête de 12 octets suivi de quatre champs de longueur variable.

Le champ **Identification**, positionné par l'émetteur, permet à celui-ci d'établir une correspondance entre une demande et une réponse. Le champ **Paramètres** est un champ de bits (*flags*), il indique l'opération concernée (figure 12.7).

Les quatre champs suivants indiquent le nombre de questions (*QDCount*), le nombre de réponses (*ANCount*), le nombre de champs d'entrée dans le champ autorité (*NSCount*) et enfin le nombre d'entrées dans le champ information supplémentaire (*ARCount*). La figure 12.8 illustre le champ question d'un message DNS.

© Dunod – La photocopie non autorisée est un délit

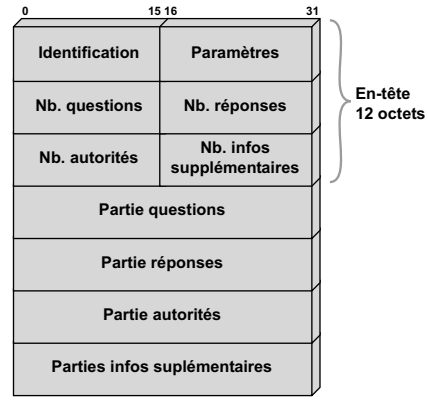


Figure 12.6 Le format général des messages DNS.

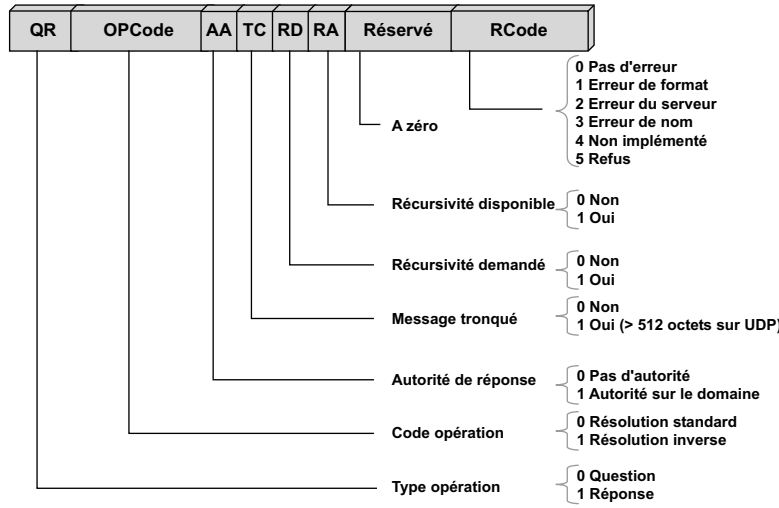


Figure 12.7 Les champs de bits de l'en-tête du message DNS.

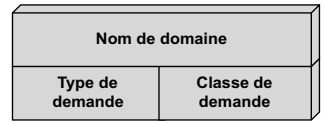


Figure 12.8 Les champs Question d'un message DNS.

Le champ Nom de Domaine (*Qname*), de longueur variable, contient le nom du nœud dont l'adresse est recherchée. Le nom ou label est codé selon une syntaxe spécifique : [longueur du label, , label lui-même], le champ label est terminé par un 0. Cette valeur correspond à la longueur du nom de la racine (figure 12.9).

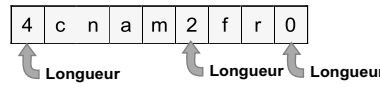


Figure 12.9 Le codage du nom de domaine recherché.

Le champ suivant précise la nature de la demande (adresse IPv4 Type A, valeur 1 ; Nom du serveur ayant autorité sur le domaine, Type NS, valeur 2...). Le champ Classe de la demande vaut généralement 1 (adresse Internet). Les champs Nom de domaine, Type et Classe du message de réponse ont une signification similaire à celle des champs correspondants du message de question (figure 12.10).

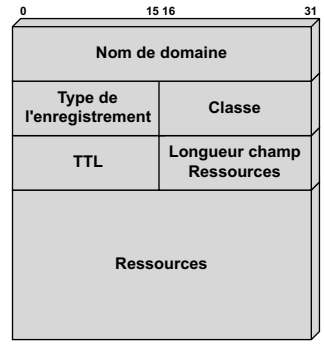


Figure 12.10 Le format du champ Réponse du message DNS.

Le nom de domaine est le nom du domaine auquel appartient le ou les enregistrement(s) de données contenu(s) dans le champ Ressources. Type et Classe indiquent le type et la classe. Le champ TTL (*Time to Live* ou temps de vie) contient un entier de 16 bits indiquant en secondes la durée pendant laquelle le client peut conserver la réponse en mémoire cache. Enfin, le champ Longueur champ Ressources indique en octet la longueur du champ Ressources. La figure 12.11 associe à un type de question, le contenu du champ Ressources.

Type de question	Valeur	Longueur réponse	Réponse
A	1	Variable	Adresse IP
NS	2	Variable	Nom de domaine de l'*host* ayant autorité dans le domaine concerné
CNAME	5	Variable	Nom canonique du serveur
HINFO	13	4 octets	Indique sur 2 octets le type de CPU et sur 2 octets le type d'OS
MX	15	Variable	Échange de courrier
PTR	15	Variable	Nom de domaine pointant sur une localisation particulière
AXFR	252	Variable	Requête pour transfert de zone
ANY	255	Variable	Requête pour tous les enregistrements

Figure 12.11 Le format du champ Réponse du message DNS.

Les champs « Partie autorités » et « Partie informations complémentaires » ont le même format que la partie « Réponse ».

© Dunod – La photocopie non autorisée est un délit

➤ UDP ou TCP ?

Le protocole DNS utilise indifféremment le transport TCP ou UDP et, dans les deux cas, le port 53. Les messages UDP sont limités à 512 octets (hors en-tête). Sous UDP, lorsque la réponse dépasse 512 octets, celle-ci est envoyée au client tronquée à 512 octets avec le bit **TC** positionné à 1 (*Tron-Cation*, message tronqué). En principe, le résolveur émet alors une nouvelle requête sur TCP. Il est possible de forcer l'utilisation de TCP, mais ceci au détriment des performances. Cependant, TCP sera toujours utilisé pour effectuer les transferts de zone.

12.2.3 La généralisation de la notion d'annuaire

Généralités

Un annuaire est une base de données structurée contenant un ensemble d'information et offrant des services simples pour y accéder. En établissant une relation entre un nom réseau et une adresse réseau, le DNS limite son usage à l'accès aux ressources du réseau. Cependant, dans un système d'information, d'autres données doivent être fréquemment consultées :

– les données téléphoniques ;
– l'identification et l'authentification des utilisateurs ;
– l'inventaire du matériel...

D'où l'idée de développer un annuaire unique enregistrant toutes les données nécessaires à l'exploitation du système d'information. Cette approche a été formalisée en premier par la norme X.500, la figure 12.12 illustre le modèle architectural de cet annuaire.

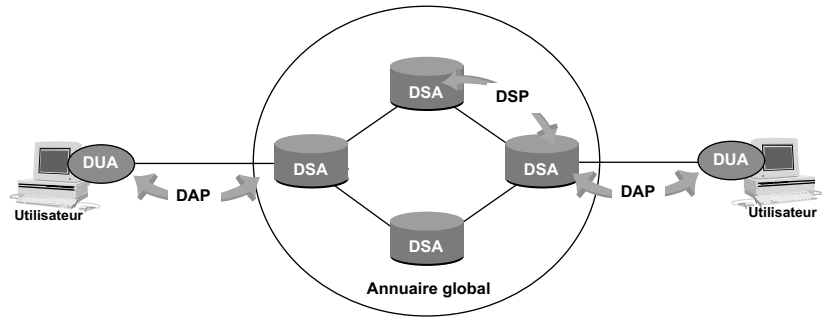


Figure 12.12 L'architecture générale d'un annuaire X.500.

L'annuaire X.500 est une base de données répartie, dont l'ensemble des éléments constitue un annuaire global. Chaque base est hébergée par un système désigné sous le nom de **DSA** (*Directory System Agent*) et maintient une partie de la base d'information (**DIB**, *Directory Information Base*). Les informations contenues dans l'annuaire sont organisées selon une structure arborescente (**DIT**, *Directory Information Tree*). L'utilisateur accède aux informations via une interface (composant) non défini par la norme (**DUA**, *Directory User Agent*). Si la description de l'agent d'accès (DUA) est hors du champ de la norme, les échanges entre le DUA et un DSA sont complètement définis par le protocole **DAP** (*Directory Access Protocol*). De même, les échanges entre les DSA sont régis par le protocole **DSP** (*Directory System Protocol*).

La répartition des informations sur plusieurs serveurs nécessite une fonction de synchronisation des informations contenues dite aussi réplication. Cette synchronisation est généralement assurée par un logiciel spécifique nommé **méta-annuaire**.

LDAP

Devant la complexité de l'annuaire X.500, issu du modèle OSI, en 1993 l'université du Michigan simplifia le protocole d'accès (DAP) et l'adapta à l'environnement TCP/IP. Ce nouveau protocole d'accès aux informations fut dénommé **LDAP** (*Lightweight Directory Access Protocol*, léger DAP). Très vite des études ont été entreprises par IETF pour faire de LDAP un annuaire natif à part entière (1995). Respectant le modèle d'information de X.500, LDAP peut aussi être considéré comme un moyen d'accès à tout annuaire (LDAP ou autres) respectant la représentation des données d'X.500. La figure 12.13 illustre la structure générale des données de LDAP (X.500).

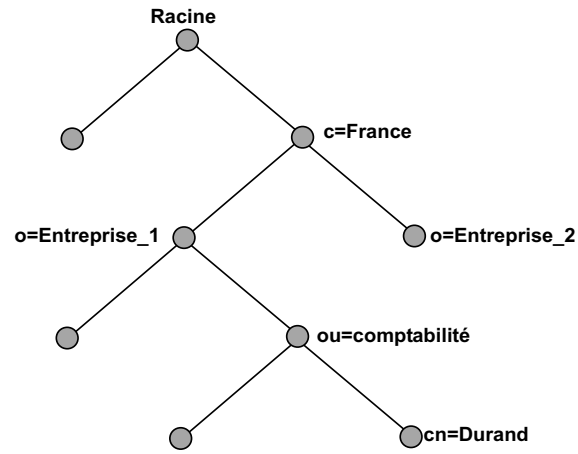


Figure 12.13 Exemple (simplifié) d'arbre d'annuaire (DIT).

Dans l'annuaire, la représentation d'un objet correspond à une entrée d'annuaire (entry) ; Ainsi, l'objet M. Durand peut être distingué dans l'annuaire par son nom relatif (**RDN**, *Relative Distinguished Name*) dont la syntaxe d'écriture est :

{type d'attribut = valeur de l'attribut} soit ici {cn = Durand}

où **cn** représente le type d'attribut (**cn**, *common name*). Si un seul attribut est insuffisant pour désigner sans ambiguïté une entrée, on en utilise plusieurs pour désigner l'entrée. Ainsi, par exemple, le nom complet (**DN**, *Distinguished Name*) de M. Durand est :

{c=France, o=Entreprise_2, ou=comptabilité, cn=Durand}

La figure 12.14 fournit, pour illustration, quelques attributs opérationnels définis par le standard LDAPv3.

© Dunod – La photocopie non autorisée est un délit

Attribut	Description
c (*country*)	Code pays en 2 lettres selon le standard ISO 3166
cn (*common name*)	Nom de l'objet
description	Description de l'objet
distinguishedName	Nom distingué, utilisé par d'autres attributs par héritage
givenName	Prénom de la personne
houseIdentifier	Identification d'un bâtiment
initials	Initiales d'une personne
o (*organization*)	Entreprise de la personne
sn (*surname*)	Nom de famille d'une personne
street	Nom de rue
title	Titre de la personne (M. Mme, Melle)
u (*organization unit*)	Service de l'entreprise
uid (*userid*)	Identifiant unique de l'objet

Figure 12.14 Les exemples d'attribut.

12.3 LE TRANSFERT DE FICHIERS

Le transfert de fichiers est l'une des applications les plus utilisées sur les réseaux. Le modèle TCP/IP en décline deux versions. L'une allégée (**TFTP**, *Trivial File Transfer Protocol*) nécessitant peu de mémoire et pouvant tenir en mémoire morte des machines sans disque (terminal X, par exemple) et permettre ainsi le téléchargement du système. TFTP s'appuie sur UDP. L'autre version, **FTP** (*File Transfer Protocol*) constitue un véritable système de manipulation de fichiers à distance.

12.3.1 TFTP (*Trivial File Transfert Protocol*)

TFTP permet le transfert de données en lecture (**RRQ**, *Read ReQuest*) ou en écriture (**WRQ**, *Write ReQuest*) de fichiers en ASCII (mode dit netascii) ou en flux d'octets (mode dit octet). En mode ASCII, mode par défaut, le fichier est structuré en lignes, TFTP insère à la fin de chaque ligne les caractères CR/LF (*Carriage Return/Line Feed*, voir tableau des codes ASCII figure 1.7). Le transfert a lieu par bloc de 512 octets numérotés. La fin du transfert est indiquée par un message de données dont la longueur est inférieure à 512 octets (figure 12.15).

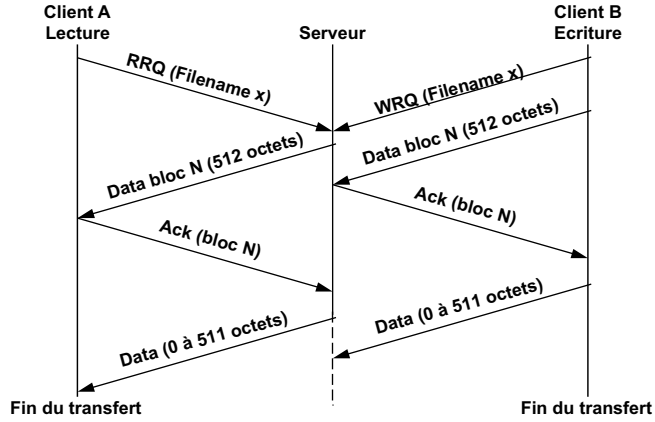


Figure 12.15 L'échange TFTP.

TFTP s'appuie UDP, c'est donc à lui de gérer les paquets perdus. Le protocole est du type *Send and Wait* (émettre et attendre), chaque extrémité gérant une reprise sur temporisation (transmission symétrique). Si ce procédé fiabilise la transmission, il peut provoquer une duplication des échanges. En effet (figure 12.16), supposons que l'ACK du paquet N soit retardé, l'émetteur procède, sur temporisation, à la retransmission du paquet de ce paquet. À réception de l'ACK de N, l'émetteur envoie N+1, qui sera acquitté, à la réception du second ACK de N, il renvoie encore N+1, ces deux blocs seront acquittés...

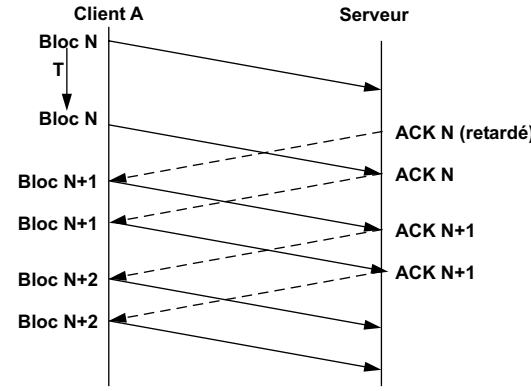


Figure 12.16 Le syndrome de l'apprenti sorcier.

TFTP n'utilise que les 5 types de messages (Opcode) décrits figure 12.17. Le nom de fichier, le mode et les messages d'erreur sont codés en ASCII. La fin de chaque libellé est indiquée par le code ASCII « 0 ». En principe, un message d'erreur peut se substituer à un ACK, une retransmission est alors réalisée. Cependant, dans la plupart des implémentations, un message d'erreur provoque l'arrêt du transfert.

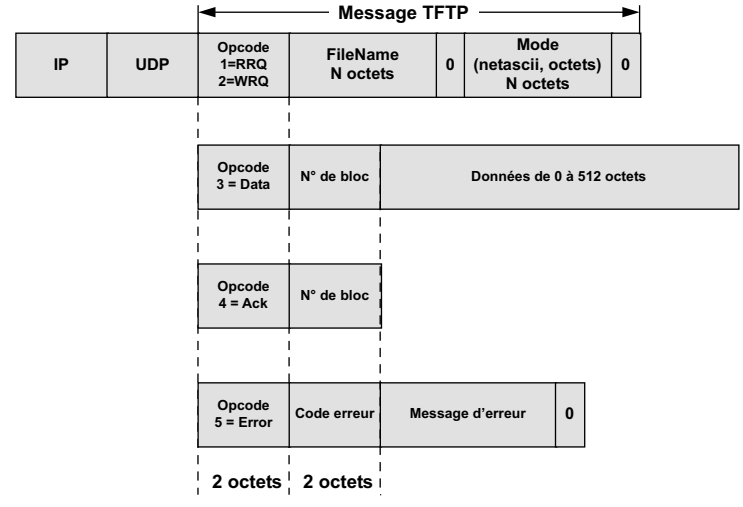


Figure 12.17 Le format des messages TFTP.

© Dunod – La photocopie non autorisée est un délit

Notons que TFTP attend les appels sur le port 69, or, contrairement à TCP, UDP ne gère pas le multiplexage des connexions sur **un** port. Pour remédier à cette lacune, TFTP attend les appels de connexions TFTP sur le port réservé 69 (messages RRQ ou WRQ) et répond sur un port éphémère que le client détectera dans la réponse (port source du message UDP de réponse).

12.3.2 FTP (*File Transfert Protocol*)

L'originalité de FTP est d'ouvrir pour chaque session FTP deux connexions simultanées. L'une sur le port 21 (FTP), l'autre sur le port 20 (FTP_Data). La première connexion, connexion de contrôle ou de service, sert à l'échange des messages FTP (connexion de signalisation), l'autre au transfert de données (figure 12.18). La demande de connexion FTP est établie sur le port 21 et reste active durant toute la session FTP (connexion permanente). La connexion de transfert sur le port 20 n'est active que durant le transfert effectif d'un fichier (connexion temporaire).

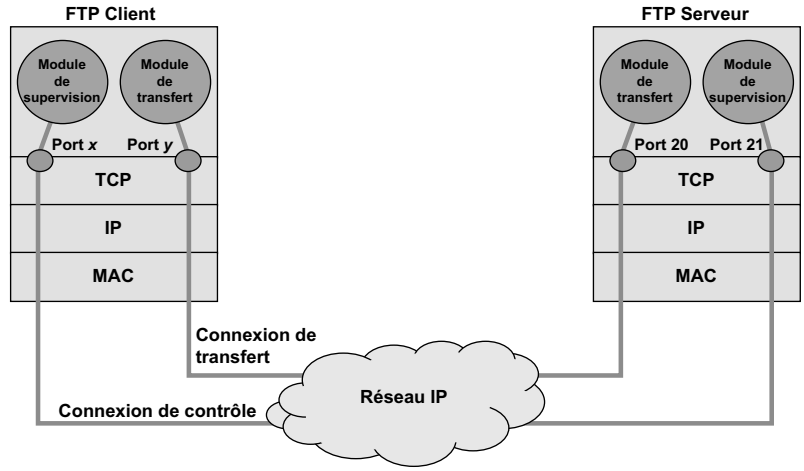


Figure 12.18 Les deux connexions de FTP.

FTP permet de spécifier :

– le type de fichiers (ASCII, binaire, EBCDIC) ;
– la structure du fichier (par défaut flux d'octets) ;
– le mode de transmission (flux d'octets – valeur par défaut – ou mode bloc).

Contrairement à TFTP, FTP réalise un contrôle d'accès avant l'acceptation de toute connexion. En principe, il faut posséder un compte sur le serveur FTP pour pouvoir s'y connecter. La session FTP commence par une procédure de type « *login* » : nom d'utilisateur, mot de passe. Il est aussi possible de se connecter sans compte (invité). Dans ce cas, le nom d'utilisateur est *anonymous* et le mot de passe *guest* (connexion FTP anonyme). Généralement, lorsqu'un serveur admet les connexions anonymes, l'accès est limité par l'administrateur à un seul répertoire dit « répertoire public ».

La figure 12.19 fournit, à titre d'exemple, les commandes les plus courantes de FTP. La commande HELP liste l'ensemble des commandes disponibles sur un serveur.

Commande	Description
FTP	Invocation du service FTP, la phase de login suit.
USER nom-utilisateur	Spécifie le nom de l'utilisateur.
PASS mot-de-passe	Mot de passe du compte utilisateur.
CWD nom-de-chemin	Spécifie un répertoire de travail sur le serveur FTP.
PORT hôte-port	Indique au serveur une adresse IP (hôte) et un numéro de port.
RETR nom-de-fichier	Indique au serveur le nom du fichier à transférer (*get*).
STOR nom-de-fichier	Indique au serveur le nom du fichier à recevoir (*put*).
DELE nom-de-fichier	Demande au serveur d'effacer nom-de-fichier.
RMD nom-de-chemin	Suppression d'un répertoire sur le serveur.
MKD nom-de-chemin	Création d'un nouveau répertoire sur le serveur.
PWD	Demande au serveur de retourner le nom du répertoire courant.
LIST nom-de-chemin	Liste tous les fichiers du répertoire nom-de-répertoire.
ABOR	Arrête toutes les commandes en cours et ferme les connexions.
QUIT	Termine la session et ferme la connexion de contrôle.

Figure 12.19 Les listes des commandes usuelles de FTP.

12.4 L'ÉMULATION DE TERMINAL (Telnet)

12.4.1 Principe de Telnet

Le terminal virtuel est un logiciel en mode client/serveur. Le terminal serveur émule vis-à-vis d'un applicatif sur la machine serveur un terminal local avec lequel l'application échange des messages, tandis que sur une machine distante, cliente de l'application, un terminal dit client est émulé sur un terminal physique. L'échange se fait en deux temps. Le premier a lieu entre le terminal client réel et le terminal serveur virtuel, le second entre le terminal serveur virtuel et l'application. Cette approche est illustrée figure 12.20.

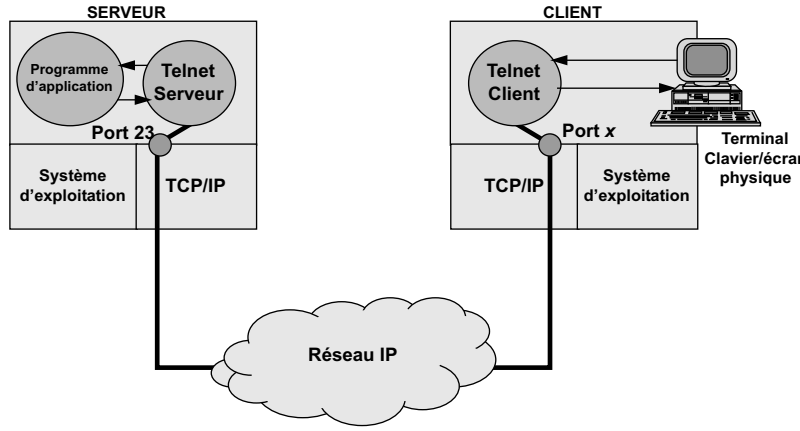


Figure 12.20 Principe du terminal virtuel.

Les systèmes client et serveur pouvant être tout à fait différents, le terminal virtuel (**NVT**, *Network Virtual Terminal*) définit une syntaxe d'échange : le code ASCII US à 7 bits. Chaque entité

© Dunod – La photocopie non autorisée est un délit

doit, éventuellement, réaliser l'adaptation nécessaire vis-à-vis du système hôte. L'échange se réalisant par octet, le bit de poids fort est toujours positionné à 0, sauf pour la valeur 255 (0xFF) qui signale que les caractères qui suivent sont une séquence de commande (caractère **IAC**, *Interprest As Command*). Une option de Telnet autorise l'emploi de caractères sur 8 bits ; dans ce cas, pour assurer la transparence dans le champ de données du caractère IAC (caractère 255), il est doublé.

12.4.2 Les commandes et les modes de fonctionnement

S'adressant à divers systèmes, Telnet doit être capable de s'adapter au mieux aux capacités de chacune des extrémités. Aussi, divers modes de fonctionnement sont possibles et de nombreuses options peuvent être négociées par chacune des entités communicantes (négociation symétrique).

La requête de négociation est un ensemble de trois caractères : <IAC, requête, option>. Les différentes requêtes et les réponses possibles sont :

- **WILL**, l'émetteur sollicite l'accord pour l'option qui suit, le récepteur accepte (DO) ou refuse (DONT) ;
- **DO**, l'émetteur demande au récepteur d'utiliser l'option, le récepteur accepte (WILL) ou refuse (WONT) l'utilisation de l'option qui suit ;
- **WONT**, l'émetteur invalide une option, le récepteur ne peut qu'accepter (DONT) ;
- **DONT**, l'émetteur demande au récepteur d'invalider une option, le récepteur ne peut qu'accepter (WONT).

Seuls, deux modes de fonctionnement de Telnet sont utilisés aujourd'hui, ce sont le mode ligne (LINEMODE) et le mode caractère (terminal asynchrone). Dans le premier mode le terminal assure lui-même la gestion de l'affichage, les échanges entre le serveur et le terminal utilise le mode bloc (ligne). Dans le second mode, c'est le serveur qui gère l'affichage (écho du caractère frappé, ou écho distant). Par exemple, lors du lancement d'une application qui nécessite le mode caractère comme l'éditeur ***vi*** de UNIX, le serveur envoie la suite :

< IAC, WILL, ECHO>

Ce qui correspond à demander au terminal de passer en mode écho de caractère (*Will Use Echo Data*).

Le client signifie son accord par la commande :

<IAC, DO, ECHO> (*Start Use Echo Data*)

Lors de la sortie du programme en cours, le mode de fonctionnement précédent est restauré par la demande d'invalidation de l'option ECHO <IAC, WONT, ECHO>.

Les tableaux de la figure 12.21 fournissent la liste des principales commandes et des options Telnet.

Le terminal Telnet ne permet pas seulement de se connecter pour une session de travail sur une machine distante, il a longtemps été utilisé comme terminal de consultation de données sur différents serveurs (météo...). Le déploiement d'Internet et des navigateurs rend cette dernière utilisation obsolète.

Commande	Valeur dec.	Valeur Hex.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (*Start Use*)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (*Will Use*)
GA	249	F9	Continuer (*Go Ahead*)
EL	248	F8	Effacer une ligne (*Erase Line*)
EC	247	F7	Effacer un caractère (*Erase Character*)
AO	245	F5	Arrêter l'édition (*Abort Ouput*)
IP	244	F4	Interrompre le processus (*Interrupt Process*)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (*Non OPeration*)
EOR	239	EF	Fin d'enregistrement (*End of Record*)

Nom	Valeur dec.	Valeur Hex.	Signification
Transmit Binaire	00	00	Transmission en mode 8 bits.
Echo	01	01	Écho des données introduites au clavier (*Echo Data*).
Suppress go ahead	03	03	Passage en mode caractère.
Linemode	34	22	Passage en mode ligne.
Carriage Return	10	0A	Retour chariot, Positionne le curseur en début de ligne.
Line Feed	13	10	Passage à la ligne suivante.

Figure 12.21 Les principales commandes et options Telnet.

12.5 LES NOTIONS DE MIDDLEWARE

12.5.1 Définitions

Le *middleware* peut être vu comme un complément de services réseau autorisant un dialogue entre applications de type client/serveur (figure 12.22). Sous cette appellation, on désigne généralement les différents outils de développement qui permettent d'offrir aux applications une interface d'accès aux différents services du réseau (**API**, *Application Programming Interface*), il est le lien entre le *hardware* (l'environnement réseau) et le *software* (les applications).

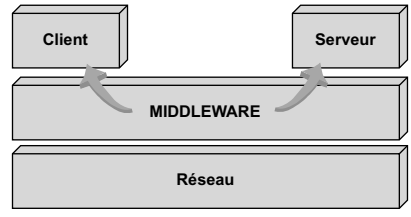


Figure 12.22 La position du middleware.

Dans l'environnement OSI, le *middleware* correspond aux couches 5 (Session), 6 (Présentation), 7 (Application). D'une manière générale, on distingue plusieurs types de *middleware* :

– Le ***middleware* par file d'attente**, le client dispose ses messages dans la file d'attente du serveur. Celui-ci les traite à leur tour et émet la réponse.

© Dunod – La photocopie non autorisée est un délit

– Le ***middleware* par appel de procédure distante**, ce mode rend les procédures distantes indépendantes des procédures clientes. La localisation de l'application serveur est inconnue du client qui y accède *via* les services d'un annuaire.
– Le ***middleware* orienté objet**, ce type de *middleware* intègre aux communications inter-application les propriétés de la technologie objet : encapsulation, héritage. C'est une adaptation du *middleware* à file d'attente à la technologie objet. Le programme n'a pas à connaître la localisation du serveur, il ne connaît que l'objet.

De même, plusieurs modes de fonctionnement peuvent être distingués (figure 12.23) :

– Le **mode asynchrone**, le client émet son message. Pendant l'attente de la réponse, il poursuit le traitement en cours (parallélisme des tâches élémentaires).
– Le **mode synchrone**, lorsque le client a émis son message, il se met en attente de la réponse.
– Le **mode non connecté**, aucune relation n'est établie entre le client et le serveur. Le mode non connecté implique un fonctionnement synchrone des applications.
– Le **mode connecté**, un contexte propre à chaque application est créé et maintenu, ce mode autorise le fonctionnement de type asynchrone.

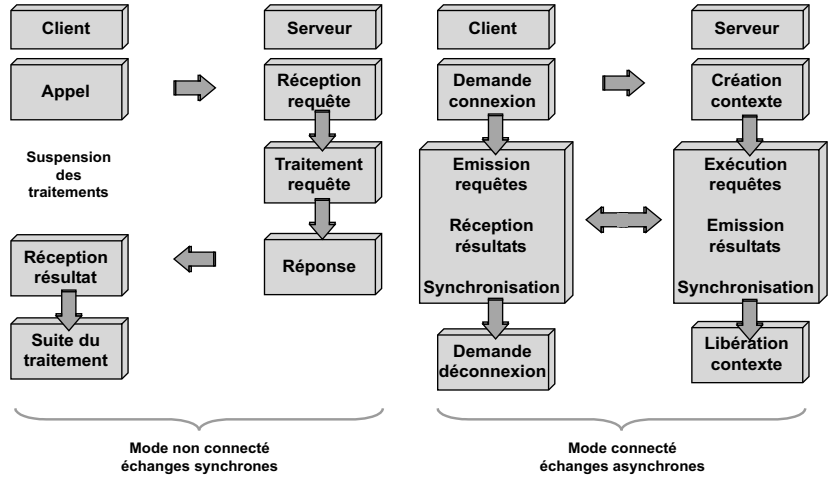


Figure 12.23 Le middleware et les modes de fonctionnement.

12.5.2 Les exemples d'outils *milddleware* dans TCP/IP

*RPC (*Remote Procedure Call*)*

En programmation traditionnelle, les programmes et les procédures sont liés pour ne former qu'un seul programme. Le concept **RPC** (procédures éloignées) suppose que le programme principal et les procédures forment des programmes séparés (figure 12.24)

Des procédures dites « *stubs* » remplacent les procédures conventionnelles. Elles portent le même nom que les procédures qu'elles remplacent et génèrent le code d'appel à la procédure distante correspondante. Le programmeur développe trois composantes :

– le programme principal de l'application cliente ;
– l'ensemble des procédures composant l'application serveur ;
– enfin, la description des échanges entre le client et le serveur (langage **IDL**, *Interface Definition Language*).

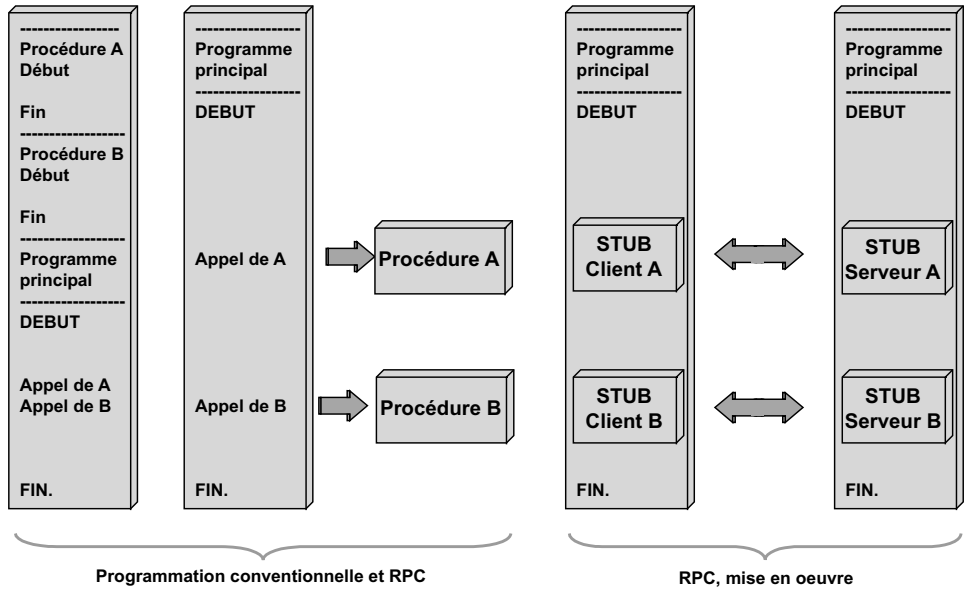


Figure 12.24 La programmation traditionnelle et RPC.

Lorsque ces composants sont développés, il convient de :

– générer les *stubs* client et serveur (compilateur IDL) ;
– construire l'exécutable client (compiler le programme principal, les stubs clients et lier les codes objets obtenus) ;
– enfin, construire l'exécutable serveur (compiler le programme, les *stubs* et les lier).

La figure 12.25 illustre les interactions entre le programme client et le programme serveur. Elle met en évidence l'une des fonctions essentielles des *stubs* : l'adaptation du format des données. Le RPC ne définit aucune syntaxe de transfert, cette approche facilite les implémentations et garantit l'indépendance totale des systèmes. Cependant, elle nécessite de la part de chaque entité de résoudre le problème de conversion de syntaxe des messages, chaque machine émettant ses données dans son format local.

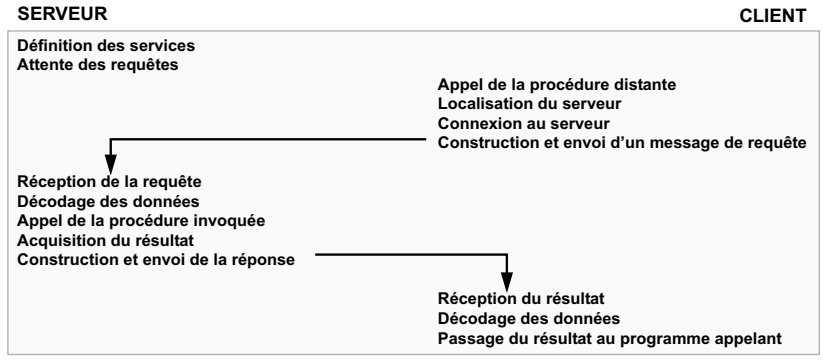


Figure 12.25 L'illustration des mécanismes d'échange de messages.

© Dunod – La photocopie non autorisée est un délit

Les sockets

Les *sockets* constituent un élément du *milddleware* de bas niveau, elles mettent en relation une application cliente et une application serveur qui ne voient les couches de communication qu'à travers de l'API *socket*. Les *sockets* permettent d'établir un lien en mode connecté ou en mode non connecté à travers le réseau. Elles sont supportées par tous les compilateurs « C » et offrent un ensemble de primitives listées dans la figure 12.26.

Primitives	Fonctions
socket()	Initialise le contexte (descripteur), retourne un identificateur par tous les autres appels.
bind()	Permet de spécifier un numéro de port.
connect()	Permet d'établir une communication active entre un serveur et un client.
listen()	Place la *socket* en état d'attente, elle spécifie le nombre de sessions acceptées.
accept)	Permet au serveur de recevoir une communication entrante, elle crée pour ce client une nouvelle *socket*.
read()	Permet de lire le message reçu en mode connecté.
write()	Permet d'émettre un message en mode connecté
recvfrom()	Permet de lire le message reçu en mode non connecté.
sendto	Permet d'émettre un message en mode non connecté
close()	Libère la connexion et la socket associée.

Figure 12.26 Liste des primitives de l'environnement socket.

La figure 12.27 illustre l'enchaînement des différentes primitives.

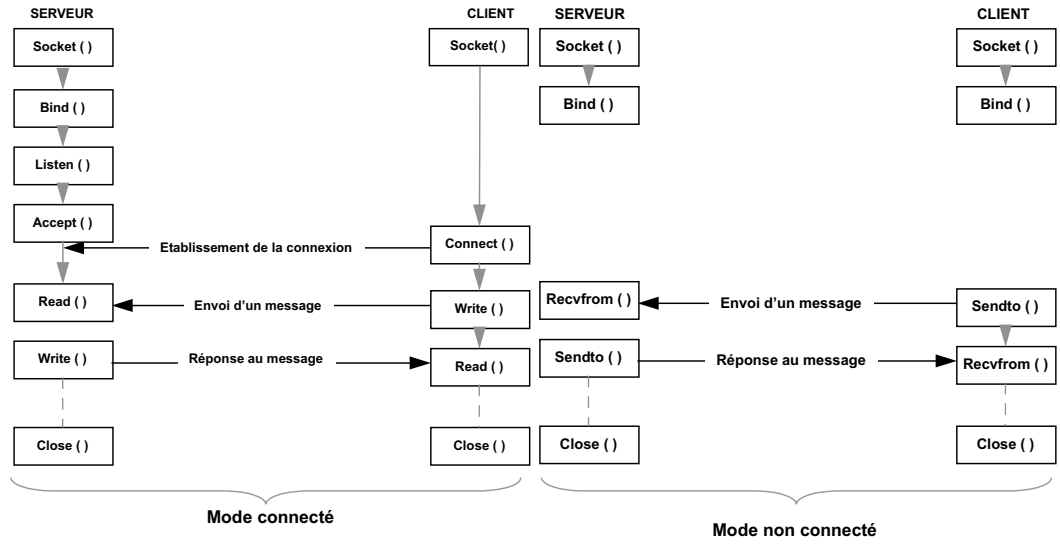


Figure 12.27 L'enchaînement des différentes primitives.

12.5.3 Internet et le *middleware*

Le Word Wide Web (WWW)

Le WWW constitue la dernière génération des serveurs d'information. Développé par le **CERN** (Centre européen de la recherche nucléaire), le Web est constitué d'un ensemble de serveurs d'information pointant les uns sur les autres par des hyperliens contenus dans les documents consultés.

La convivialité des systèmes clients (navigateur) et la richesse fonctionnelle apportée par le concept d'hyperlien ont contribué au succès rapide des serveurs Web qui sont devenus le standard de développement de bases d'information sur le Net. Les principaux logiciels permettant le développement, la mise en œuvre et la consultation d'information organisée en page en mode hypertexte sont les suivants :

– **HTTP** (*HyperText Transport Protocol*) constitue le protocole de type question/réponse de transfert de fichiers hypertextes entre un serveur Web et un client Web. La figure 12.28 liste les méthodes offertes par HTTP pour manipuler des documents.
– **HTML** (*HyperText Markup Language*) définit le format d'un document et la syntaxe de description des pages, remplacé aujourd'hui par **XML** *(eXtensible Markup Language*).
– **URL** (*Uniform Resource Locators*) définit le format de l'adresse (localisation) d'un document à importer. La syntaxe est la suivante :

Protocole://Nom du serveur/Répertoire/Nom de fichier.

Les URL permettent l'accès depuis le navigateur Web à toutes les formes de documents sur le Web.

– « http:// » pour les serveurs Web,
– « ftp:// » pour les serveurs FTP,
– « gopher:// » pour accéder aux services Gopher.

Un document est dit hypertexte quand il contient des liens vers d'autres documents (hyperliens) et hypermédia s'il pointe vers des documents contenant des images et/ou du son.

Méthodes	Actions
OPTIONS	Permet de connaître les options ou les contraintes associées à une ressource désignée par son URL.
GET	Permet, si l'URL désigne un document de l'obtenir, si l'URL désigne un programme de lui fournir des paramètres et de demander son exécution.
HEAD	Similaire à la méthode GET, mais fournit des informations dites méta-informations contenues dans l'en-tête du document.
POST	Similaire à la méthode GET, mais est utilisé pour le transfert des données du client vers le serveur généralement par l'intermédiaire d'un formulaire.
PUT	Permet d'écrire des données sur le serveur (mise à jour de documents...).
DELETTE	Détruit la ressource pointée par l'URL (généralement désactivée).
TRACE	Outil de « débogage » qui visualise l'information reçue du serveur.

Figure 12.28 Les différentes méthodes d'HTTP v1.1.

© Dunod – La photocopie non autorisée est un délit

Le logiciel client

S'il est toujours possible de se connecter à Internet à l'aide des logiciels clients spécifiques à chaque service invoqué, il est aussi possible de s'y connecter au travers d'un logiciel unique dit « navigateur Web ». Ces navigateurs donnent accès aux services d'Internet *via* une interface unique (figure 12.29).

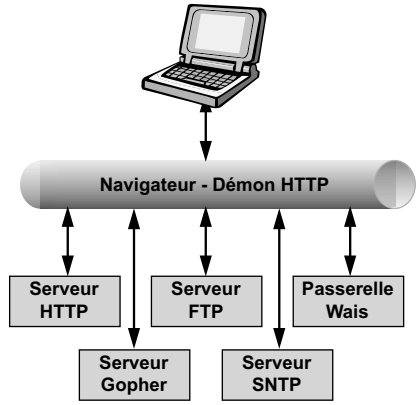


Figure 12.29 Le navigateur, interface aux services d'Internet.

Les navigateurs fonctionnent selon le mode/clients serveur. En principe, le client n'est qu'un terminal passif chargé de l'affichage des pages HTML. Cependant, la puissance de calcul des machines clientes autorise le serveur à invoquer celles-ci pour l'exécution de certaines tâches. L'utilisateur n'a aucun contrôle sur ces petits programmes qui peuvent donc poser des problèmes de sécurité. Ces programmes ou routines dénommés « *applet* » (en français : appliquette !) sont des scripts chargés par le navigateur et interprété par l'interpréteur « Java » (machine virtuelle). Cette approche assure l'indépendance totale entre le développement et la machine cliente.

La figure 12.30 illustre une session d'échange entre un serveur HTTP (port 80[4] par défaut) et un client HTTP.

12.6 CONCLUSION

Le protocole TCP/IP n'offre qu'un service de transport, le *middleware* le rend transparent aux applications. Cependant, TCP/IP est en principe un protocole d'extrémité. Les réseaux de transport (WAN), pour des raisons historiques et de performance, utilisent d'autres protocoles. TCP/IP est alors transporté en mode tunnel dans ces protocoles. L'étude de ces réseaux fait l'objet des chapitres suivants.

4. Pour des raisons de sécurité certains serveurs n'utilisent pas le port par défaut. Il faut alors préciser ce dernier lors de l'appel : http://exemple.fr:8080, le service est accessible sur le port 8080.

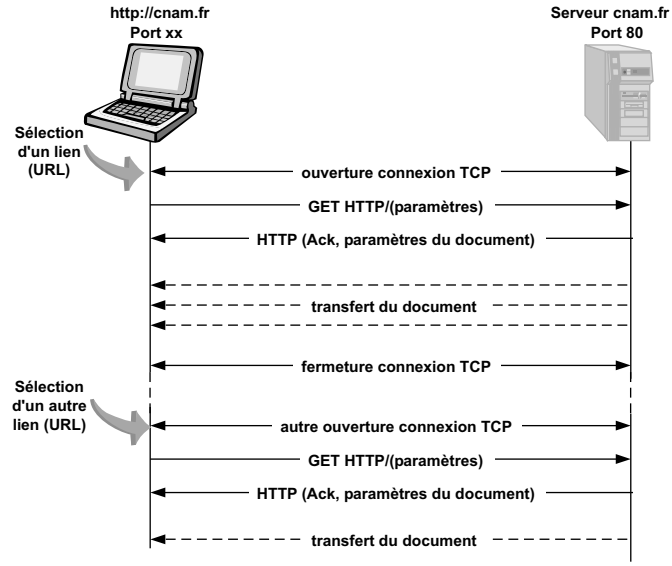


Figure 12.30 Les échanges entre un navigateur et un serveur HTTP.

EXERCICES

Exercice 12.1 Transfert de fichiers

Le transfert de fichiers FTP utilise deux ports, quels sont ces ports et leur utilité ?

Exercice 12.2 Serveurs DNS

Quels autres serveurs DNS doit connaître un serveur DNS ?

Exercice 12.3 RPC

À quoi correspond le terme RPC dans un environnement client/serveur ?

Exercice 12.4 Arbre de nommage

Proposez une arborescence sous le domaine « fr » qui permette de distinguer le Conservatoire national des Arts et Métiers (CNAM) de la Caisse nationale d'assurance maladie (CNAM).

Exercice 12.5 Commande Ping

La commande Ping sur Renault.fr, à partir de votre ordinateur connecté directement à Internet par un modem V.90, a donné la réponse suivante :

```
Envoi d'une requête 'ping' sur www.renault.fr [160.92.111.2] avec 32 octets de
données :

Réponse de 160.92.111.2 : octets=32 temps=2082 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=155 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=156 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=156 ms TTL=246

Statistiques Ping pour 160.92.111.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 155ms, Maximum = 2082ms, Moyenne = 637ms
```

1. Quelle est la classe de l'adresse attribuée par l'hébergeur du serveur de la régie Renault ?
2. Quels sont les protocoles utilisés par la commande Ping ?
3. Qu'est-ce qui peut justifier une valeur de RTT beaucoup plus importante pour la première réponse que pour les suivantes ?

Partie **III**

Mise en œuvre

13 Introduction aux réseaux de transport 363
13.1 Généralités 363
13.2 Le plan de transmission 364
13.3 Le plan de service 374
13.4 L'accès aux réseaux, la boucle locale 383
13.5 Conclusion 394
EXERCICES 395

14 Les protocoles de cœur de réseau 397
14.1 Le protocole X.25 397
14.2 Le relais de trame ou Frame relay 411
14.3 L'ATM (*Asynchronous Transfer Mode*) 421
14.4 Conclusion 438
EXERCICES 439

15 MPLS, *Multiprotocol Label Switching* 443
15.1 Généralités 443
15.2 Principe 443
15.3 Le réseau MPLS 444
15.4 MPLS et les infrastructures existantes 448
15.5 La construction des routes dans un réseau MPLS 451
15.6 MPLS et l'ingénierie de trafic 454

15.7 Les VPN MPLS 454
15.8 Conclusion 459
EXERCICE 460

16 Les réseaux locaux et métropolitains 461
16.1 Introduction 461
16.2 Étude succincte des différentes couches 466
16.3 Étude succincte des principales implémentations 477
16.4 Les réseaux locaux ATM 484
16.5 Les réseaux métropolitains 492
16.6 Les canaux hauts débits 496
16.7 Conclusion 498
EXERCICES 499

17 Ethernet et ses évolutions sans fil 501
17.1 Introduction 501
17.2 Les caractéristiques générales des réseaux Ethernet/802.3 501
17.3 Les différentes versions d'Ethernet 506
17.4 L'Ethernet sans fil 518
17.5 Conclusion 541
EXERCICES 542

18 Pontage, commutation et VLAN 545
18.1 Pont ou commutateur ? 545
18.2 Les ponts 546
18.3 La commutation dans les LAN 556
18.4 Les réseaux virtuels ou VLAN (*Virtual Local Area Network*) 562
18.5 Conclusion 567
EXERCICES 568

19 Interconnexion des réseaux et qualité de service 571
19.1 L'interconnexion des réseaux, généralités 571
19.2 Les éléments d'interconnexion (relais) 576
19.3 Les techniques de routage 582
19.4 Notions de qualité de service 597
19.5 Le *multicast* et le routage *multicast* 603
19.6 Les fonctions annexes des routeurs 607
19.7 Les passerelles applicatives 610
EXERCICES 611

Chapitre **13**

Introduction aux réseaux de transport

13.1 GÉNÉRALITÉS

Un réseau peut être vu comme étant la superposition de trois plans (figure 13.1) :

- Le **plan usager** qui correspond à l'installation privée de l'usager final.
- Le **plan service** qui correspond au point où le service requis par l'usager, service données ou voix, est mis à sa disposition. Ces réseaux peuvent être privés ou publics. L'usager est relié au plan service par une liaison d'abonné appelée aussi **boucle locale**. Les éléments actifs de ces réseaux (commutateurs, routeur...) ne sont pas reliés directement entre eux.
- Enfin, le **plan transmission** qui correspond au réseau réel de transport des données et de la voix. Ce sont les techniques de numérisation et de multiplexage qui ont autorisé le transport de manière banalisée de tout type de flux (voix, données, images). C'est à ce réseau que sont reliés les éléments actifs du réseau de transport.

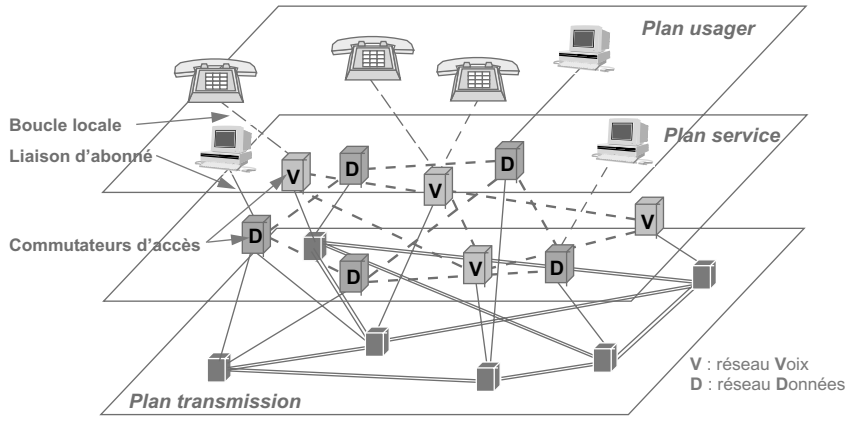


Figure 13.1 Les trois plans d'un réseau de transmission.

Ce chapitre concerne l'étude des plans de transmission, de service et des modes d'accès à ce dernier.

13.2 LE PLAN DE TRANSMISSION

13.2.1 Généralités

Jusqu'aux années 1960, les réseaux étaient fondamentalement distincts, il était même interdit d'effectuer des transferts de données sur le réseau téléphonique. Avec la numérisation de la voix, les infrastructures se sont banalisées (figure 13.2). Pour optimiser l'utilisation des supports de transmission, le CCITT (UIT-T) a normalisé, à partir des liaisons MIC (Modulation par impulsion et codage), différents niveaux de multiplexage. Cette hiérarchie appelée **PDH** (*Plesiochronous Digital Hierarchy*), différente en Amérique du Nord et au Japon, a constitué la base de tous les réseaux de transmission jusqu'aux années 1990.

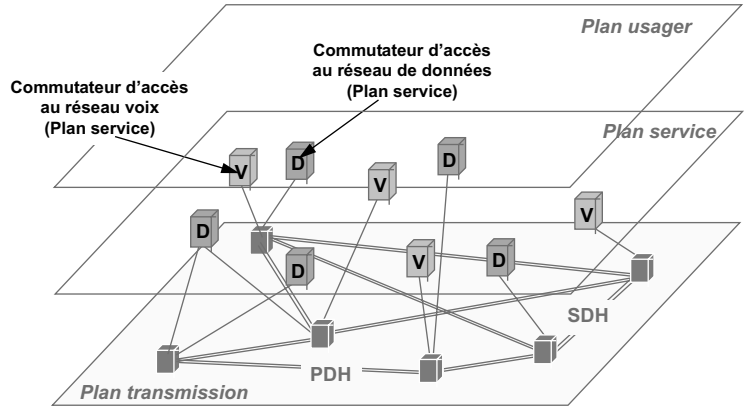


Figure 13.2 Le plan de transmission.

Outre la rationalisation de l'utilisation des supports, la hiérarchie PDH a eu le mérite de résoudre les difficultés de synchronisation des flux provenant de sources différentes aux horloges proches (plésio) mais non identiques. Fondée sur un réseau de distribution d'horloge, la hiérarchie synchrone (**SDH**, *Synchronous Digital Hierarchy*) garantit la délivrance des bits en synchronisme d'une horloge de référence. Elle autorise des débits plus élevés, apporte des solutions d'administration et de contrôle et enfin répond à un besoin de normalisation des interfaces optiques.

Si les cœurs des réseaux sont aujourd'hui SDH, pour des raisons historiques, la distribution des débits chez l'utilisateur repose toujours sur la hiérarchie plésiochrone. L'adage qu'une technologie ne supplante jamais une autre, mais vient la compléter prend ici toute sa valeur (figure 13.3).

13.2.2 La synchronisation des réseaux

Horloges et mécanismes associés

Les références temporelles dans un réseau sont fournies à partir d'oscillateurs. Indépendamment du fait qu'il n'est pas possible de réaliser des oscillateurs de fréquences strictement identiques,

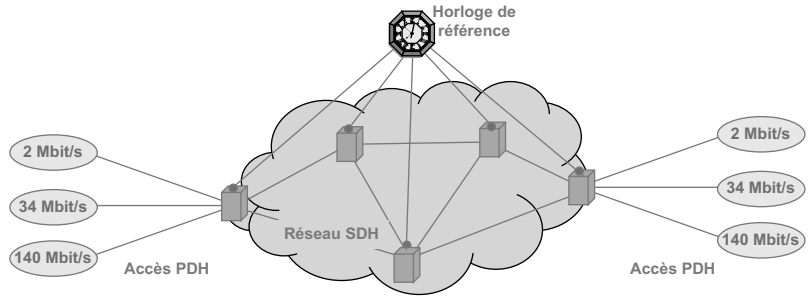


Figure 13.3 La cohabitation des techniques PDH et SDH.

les signaux d'horloge déduits du signal binaire subissent les mêmes altérations que ce dernier. Même lorsque les différentes horloges du réseau sont asservies à une horloge de référence unique, des écarts subsistent. Les différences d'horloge provoquent des différences de débits (figure 13.4) et sont, aujourd'hui, la principale source d'erreur dans les réseaux (**saut de bits**).

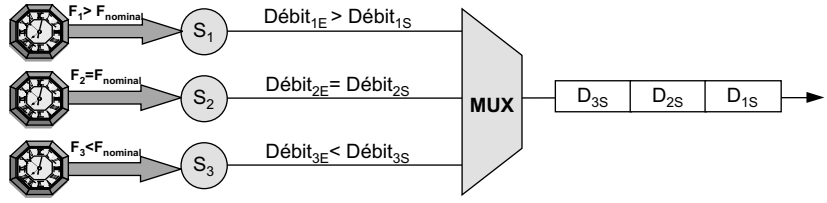


Figure 13.4 Les écarts d'horloge et de débit.

Les signaux d'horloge subissent deux types d'altération, l'une et l'autre correspondent à des variations de la fréquence d'horloge autour d'une valeur moyenne. La première est une variation rapide autour de la fréquence nominale, le cycle est répétitif plusieurs fois par seconde, il s'agit du phénomène connu sous le nom de **gigue**[1] ou *jitter*. La gigue s'exprime en amplitude de la variation autour de la fréquence moyenne, elle varie de 10^{-5} à 10^{-6}.

La seconde, beaucoup plus lente, s'appelle dérapage ou glissement, son cycle peut être très grand. C'est, par exemple, la variation de fréquence due aux variations de température durant la journée.

Pour remédier à ces écarts d'horloge et donc de débit, plusieurs solutions sont envisageables. La plus simple consiste à régénérer périodiquement le signal, les **répéteurs** ou **régénérateurs** non seulement restaurent le signal (forme et amplitude) mais peuvent aussi recalibrer le signal autour d'une fréquence moyenne (figure 13.5).

Cependant, les bits sont reçus par les éléments actifs au rythme de l'horloge source, ils sont réémis au rythme de l'horloge émission du système. Si le rythme de l'horloge source est supérieur

1. La gigue, dans les réseaux, a deux origines. Celle évoquée ici correspond aux fluctuations d'horloge, elle est quantifiable et engendre des décalages temporels entre les bits provoquant éventuellement des erreurs (saut de bits). L'autre dépend essentiellement de la charge du réseau et de ses variations, elle n'engendre pas d'erreur binaire mais peut rompre, éventuellement, l'isochronie des paquets de données.

© Dunod – La photocopie non autorisée est un délit

à celui de l'horloge émission, le système reçoit plus de bits qu'il ne peut en émettre. Il est alors nécessaire de mémoriser les bits excédentaires en attente d'une dérive inverse de l'horloge source. En principe, les variations d'horloge s'annulent ainsi, les bits reçus en excédant durant une période pourront être émis à la période suivante. Pour limiter la taille des mémoires tampons, l'UIT-T a fixé des limites aux dérives d'horloge, celles-ci devant être d'autant plus faibles que les débits sont importants.

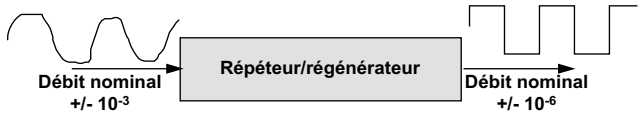


Figure 13.5 La régénération du signal par un répéteur.

La figure 13.6 représente un système de correction de gigue. La mémoire tampon (*buffer*) de réception est constituée par un registre à décalage « élastique ». Le *buffer* est plus ou moins rempli selon les écarts de rythme entre l'horloge de réception (Hr) et l'horloge d'émission (He). Ce dispositif est efficace, mais il introduit un retard (temps de rétention des bits).

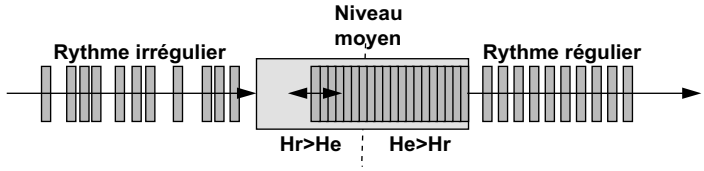


Figure 13.6 Principe de la correction de gigue d'horloge.

Quelle que soit la technique utilisée pour asservir les horloges, on ne peut garantir un synchronisme parfait de toutes les horloges d'un réseau. Ainsi, lors des opérations de multiplexage, les différentes voies incidentes peuvent avoir des rythmes d'horloge différents. Les dispositifs précédents ne suffisent plus. La seule solution envisageable consiste à organiser dans le train d'émission une position variable des débits affluents (cadrage). Ce principe, illustré par la figure 13.7, est utilisé aussi bien dans la hiérarchie plésiochrone (justification au niveau bit) que dans la hiérarchie synchrone (justification au niveau octet). Un pointeur permet de déterminer où débutent les données.

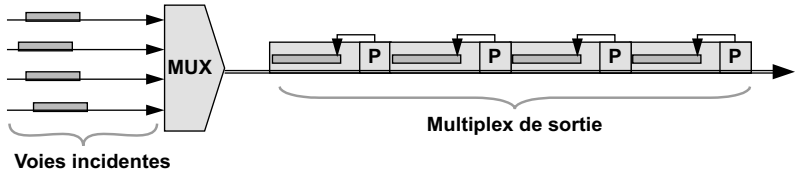


Figure 13.7 Principe de la justification.

Afin de permettre le cadrage des données, le débit du multiplex de sortie est nécessairement plus élevé que la somme des débits des voies incidentes, ce surdébit est dit surdébit de justification. Seule l'utilisation conjuguée de surdébit et de pointeurs associés autorise une compensation dynamique non seulement des différences d'horloge mais aussi des écarts de phase introduits par les différences de trajet (temps de propagation) des différents affluents. La figure 13.8 illustre le principe de la justification au niveau bit par bit de cadrage.

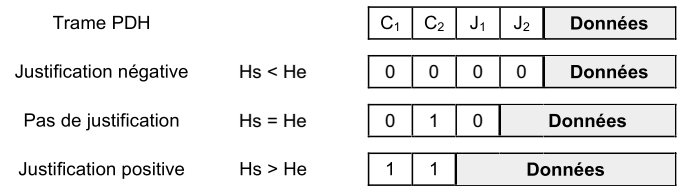


Figure 13.8 Principe de la justification dans les trames PDH.

La justification est nulle quand la fréquence d'horloge du train incident (Hs) est identique à celle du train d'émission (He), c'est-à-dire que le débit binaire incident correspond exactement au débit binaire nominal d'émission. Si le train de bits incident est supérieur à la capacité nominale d'émission, elle est dite positive et négative dans le cas inverse. Dans l'exemple de la figure 13.8, l'écart maximal des horloges a été supposé limité à 1 bit. La position des données dans la trame varie donc de ± 1 bit, par rapport à une position de référence. Les bits C_1 et C_2 indiquent, lorsqu'ils sont positionnés à 1, que le bit de justification correspondant (C_1 pour J_1 et C_2 pour J_2) contient un bit de donnée. Lorsqu'ils ne sont pas utilisés, les bits de justification J_1 et J_2 et d'indication (C_1 et C_2) sont à 0.

La distribution d'horloge dans un réseau SDH

Il existe deux modes de synchronisation des réseaux. Le mode synchronisation mutuelle et le mode maître-esclave ou mode hiérarchique. Dans le mode synchronisation mutuelle, tous les nœuds du réseau sont considérés au même niveau. Chaque nœud détermine, à partir des signaux incidents, une horloge moyenne et y aligne la sienne. Cette méthode est peu utilisée, on lui préfère une synchronisation de type hiérarchique. Le réseau de distribution d'horloge[2] est organisé sur trois niveaux (figure 13.9).

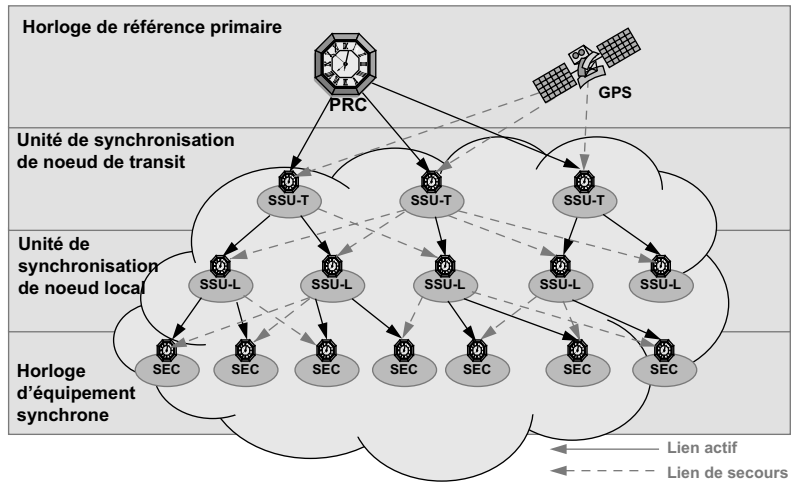


Figure 13.9 La synchronisation maître-esclave dans un réseau SDH.

2. La distribution d'horloge n'est pas réservée aux réseaux SDH, elle peut aussi être utilisée dans les réseaux PDH.

© Dunod – La photocopie non autorisée est un délit

Le rythme de référence primaire (**PRC**, *Primary Reference Clock*, horloge primaire de référence) est fourni par une horloge au césium[3] de grande stabilité (10^{-11}). À des fins de sécurité, cette horloge est doublée. Certains opérateurs utilisent des récepteurs **GPS** (*Global Positionning System*). Cette dernière approche, bien qu'elle soit sous le contrôle du ministère de la Défense américain (DoD), tend à se répandre. Le GPS peut être utilisé comme horloge principale mais, le plus souvent, il est employé comme horloge de secours.

Afin de rétablir un lien de synchronisation, en cas de défaillance d'un nœud de niveau supérieur, le réseau de distribution d'horloge assure une redondance des liens. Le tableau de la figure 13.10 détaille les différents niveaux de distribution d'horloge, il indique les normes de référence et la stabilité des horloges de chaque niveau.

Abréviation	Appellation	Avis UIT-T	Stabilité
PRC	*Primary Reference Clock* Horloge primaire de référence	G.811	10^{-11} sur le long terme
SSU-T	*Synchronisation Supply Unit Transit* Unité de synchronisation de nœud de transit	G.812T	50•10⁻ Dérive maxi. sur 24 h. •10^{-9}
SSU-L	*Synchronisation Supply Unit Local* Unité de synchronisation de nœud de transit	G.812L	10^{-8} Dérive maxi. sur 24 h. 2•10^{-8}
SEC	*Synchronous Equipement Clock* Horloge d'équipement synchrone	G.813	5•10^{-8} Dérive sur 24 h. 2•10^{-7}

Figure 13.10 Les références normatives.

Dans les réseaux SDH, l'octet **SSM** (*StatuS Message byte*, message d'état de la synchronisation) permet à chaque instant d'être informé de l'état de la source de synchronisation. Enfin, remarquons que, pour garantir son indépendance, chaque opérateur dispose de sa propre horloge de référence. Par conséquent, si les réseaux d'opérateur sont des réseaux synchrones (SDH), le réseau qui résulte de leur interconnexion est un réseau du type plésiochrone.

13.2.3 La hiérarchie plésiochrone (PDH)

Généralités

La hiérarchie PDH est apparue avec la numérisation de la voix et la nécessité de transporter simultanément plusieurs canaux téléphoniques sur un même support (multiplexage temporel). Le multiplex de base est constitué du regroupement de plusieurs canaux téléphoniques de 64 kbit/s. Ces regroupements sont différents en Europe, au Japon et en Amérique du nord, ce qui conduit à la définition de différentes hiérarchies plésiochrones illustrées par la figure 13.11.

3. Lorsque l'on fournit une énergie suffisante, un électron passe d'un niveau d'énergie à un autre. C'est sur ce principe que reposent les horloges atomiques, il consiste à irradier des atomes de césium 133 à l'aide d'une source rayonnante afin de provoquer une transition de niveau. Pour maintenir ces transitions, la source de fréquence est asservie par les transitions elles-mêmes, on obtient ainsi un générateur de référence horaire très stable : 9 162 631 770 Hz avec une stabilité de 10^{-14} soit d'une seconde de dérive pour 3 millions d'années ! Rappelons que, depuis 1967, la seconde a été définie comme correspondant à 9 162 631 770 périodes de radiation correspondant à la transition entre deux niveaux de l'atome de césium 133.

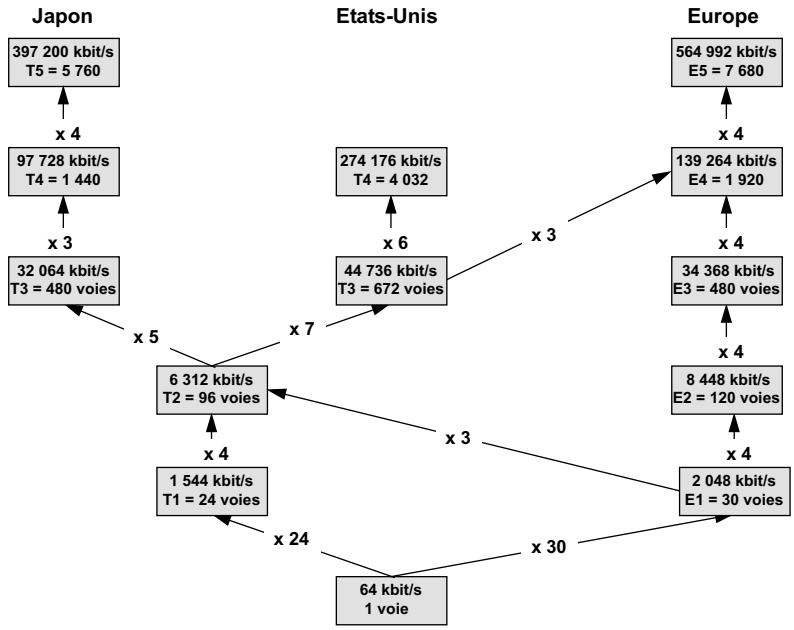


Figure 13.11 Les différents regroupements en hiérarchie PDH.

Chaque intervalle de temps ou IT peut transporter un échantillon de voix ou toute autre information numérique. La concaténation de plusieurs voies permet une granularité des débits modulo 64 kbit/s. Les surdébits entre les différents niveaux de regroupement sont dus aux signaux d'alignement, de supervision et de justification binaire. Les niveaux 5 ne sont pas normalisés par l'UIT-T.

La trame de base du système européen

La trame de base regroupe 30 voies de communication (Intervalles de temps, IT ou *Slot time*) et deux voies de service de 8 bits. La position de chaque voie est déterminée en comptant un certain nombre de temps d'horloge à partir d'une combinaison particulière de bits appelée **mot de verrouillage de trame** (**MVT**) qui balise le début de la trame de 32 voies (IT). L'organisation de base de la trame (G.704) est illustrée par la figure 13.12.

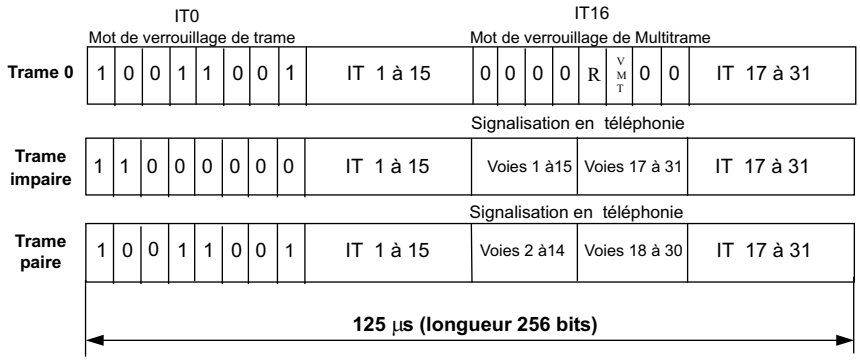


Figure 13.12 L'organisation de la trame G.704 ou G.732 (téléphonie).

© Dunod – La photocopie non autorisée est un délit

Les trames sont regroupées selon une structure dite de **multitrame**, cette structure regroupe deux sous-groupes de 16 trames numérotées globalement de 0 à 31. Ce regroupement permet le transport d'informations spécifiques notamment de contrôle d'erreur sur 4 bits émis bit par bit dans le premier bit de chaque IT0 (bit X de la figure 13.12). L'IT0 des trames paires transporte une information de synchronisation dite mot de verrouillage de trame ou MVT (X0011011). Les bits P et D des trames impaires transportent une information d'alarme (P, alarme urgente ; D, alarme non urgente). Enfin, les bits YYYY sont laissés à disposition pour un usage national. L'IT16 de la trame 0 sert de fanion pour indiquer le début d'une séquence de 16 trames (**mot de verrouillage multitrame**). Le bit A est utilisé pour signaler une perte d'alignement de la multitrame.

La trame de base du système américain

La trame nord-américaine (utilisée aussi au Japon) ou T1 comporte 24 IT de 64 kbit/s donnant un débit total de 1 544 kbit/s et un débit utile de 1 536 kbit/s.

À l'instar de la trame G.704, la signalisation comporte deux types d'information, celles relatives à la structure de la trame (ou **signalisation de supervision**) et celles en rapport avec l'état de chaque canal téléphonique (**signalisation voie par voie** ou CAS).

La trame de base T1[4] (trame G.733, aussi notée DS1 à DS12), représentée figure 13.13, comprend 24 IT (DS0) de 8 bits (192 bits). La multitrame de premier niveau regroupe 12 trames de base. Chaque trame de base est précédée d'un bit (bit de tramage constituant la signalisation de supervision). Ces 12 bits forment un mot (mot **SF**, *SuperFrame*) représentant la séquence binaire 100011001100 et identifiant la trame.

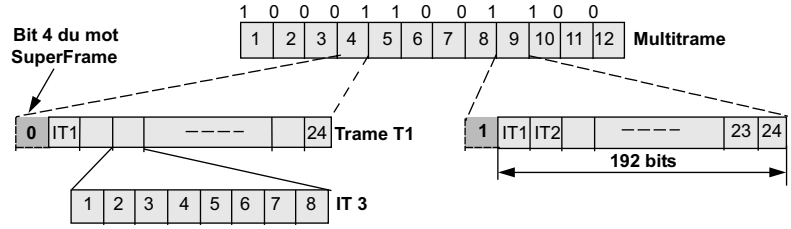


Figure 13.13 L'organisation de la multitrame T1.

La signalisation téléphonique de chacune des voies est réalisée par vol, toutes les six trames, du bit de poids faible dans l'IT (un bit de signalisation est substitué au bit d'information, c'est une signalisation dans la bande). Remarquons que, si en téléphonie, ce mode de signalisation est efficace puisqu'il économise l'IT de signalisation de la trame E1, en transmission de données, il pénalise fortement le système, la bande utile n'étant plus que de 56 kbit/s par IT (7 bits, toutes les 125 μs).

13.2.4 La hiérarchie synchrone (SDH)

Généralités

La hiérarchie numérique synchrone conserve une structure de multiplexage, elle améliore les fonctions de maintenance et d'exploitation du réseau, elle simplifie la mise en œuvre et l'interconnexion des réseaux.

4. T1 désigne le canal de transmission, DSx le format des données.

Outre l'utilisation de surdébits (justification et bourrage) qui consomme inutilement de la bande passante, l'inconvénient majeur de la hiérarchie PDH réside dans l'obligation de démultiplexer complètement le train à haut débit pour reconstituer un lien à 2 Mbit/s. La figure 13.14 illustre l'extraction d'un conduit à 2 Mbit/s d'un lien à 140 Mbit/s.

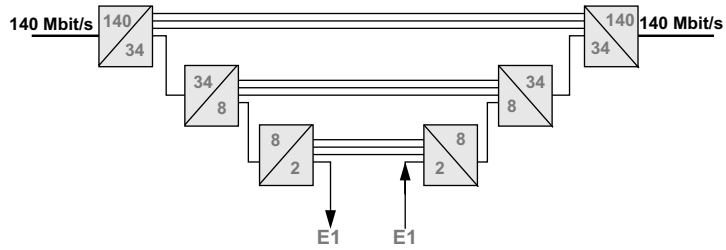


Figure 13.14 La constitution d'une liaison à 2 Mbit/s entre A et B en PDH.

La hiérarchie synchrone se distingue essentiellement de la hiérarchie plésiochrone par la distribution d'horloge à tous les niveaux du réseau réduisant ainsi les écarts d'horloge. Les données sont encapsulées dans un « *container* ». À chaque *container* est associé un surdébit destiné à l'exploitation de celui-ci. Le *container* et le surdébit constituent un *container* virtuel (**VC**, *Virtual Container*). Un pointeur (surdébit) pointe sur la charge utile de la trame. Lorsque l'horloge source n'est pas en phase avec l'horloge locale, la valeur du pointeur est incrémentée ou décrémentée. L'utilisation de ces pointeurs permet d'insérer ou d'extraire un train numérique de différents débits sans être contraint de reconstituer toute la hiérarchie de multiplexeurs (figure 13.15). Ce dernier point constitue l'un des principaux avantages de la hiérarchie SDH par rapport à la hiérarchie PDH.

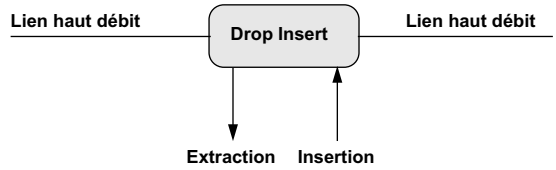


Figure 13.15 L'insertion et l'extraction d'un niveau inférieur.

On distingue deux types de hiérarchie synchrone : la hiérarchie SDH en Europe et la hiérarchie **SONET**[5] (*Synchronous Optical NETwork*) aux États-Unis. Pour garantir la connectivité des différentes hiérarchies, des niveaux identiques ont été définis. Le premier niveau de la hiérarchie SONET : **STS-1** (*Synchronous Transport Signal – level 1*) ou **OC1** (*Optical Carrier-1*) est défini à 51,84 Mbit/s. La hiérarchie SDH fixe un premier niveau (ou trame de base) à 155,52 Mbit/s (**STM-1,** *Synchronous Transport Module – level 1*). La figure 13.16 donne la correspondance entre les deux hiérarchies.

La trame de base SDH (figure 13.17) comporte 2 430 octets émis avec une période de récurrence de 125 μs soit un débit de 155,20 Mbit/s. Elle est divisée en neuf éléments ou rangées de 270 octets, chaque élément est divisé en deux champs. Un champ de surdébit de 9 octets par rangée (**SOH**,

5. C'est la hiérarchie SONET qui, issue des travaux de Bellcore en 1985 (BELL COmmunication REsearch), est à l'origine de la hiérarchie SDH.

© Dunod – La photocopie non autorisée est un délit

SONET	SDH	Débit en Mbit/s	Accès ATM
OC1		51,84	
OC3	**STM-1**	**155,52**	Oui
OC9		466,56	
OC12	**STM-4**	**622,08**	Oui
OC18		933,12	
OC24		1 244,16	
OC36		1 866,24	
OC48	**STM-16**	**2 488,32**	Oui

Figure 13.16 Correspondance entre SONET et SDH.

Section OverHead) contient les informations de supervision, notamment les pointeurs. Les données sont déposées dans les champs utiles (261 octets) de chacune des rangées (**AU**, *Administrative Unit*). L'ensemble des données déposées forme un *container*.

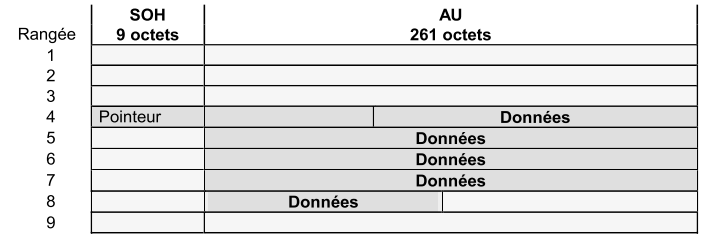


Figure 13.17 La structure simplifiée de la trame SDH.

Les équipements SDH

La hiérarchie synchrone met en œuvre trois types d'équipements (figure 13.18) :

- Les **multiplexeurs d'accès** permettent le multiplexage et le démultiplexage de plusieurs affluents plésiochrones et/ou synchrones.
- Les **multiplexeurs à insertion/extraction** (**ADM**, *Add Drop Mux*) assurent le transfert des données d'Est en Ouest (E ↔ W) tout en autorisant l'extraction et/ou l'insertion de sous-débit.
- Les **brasseurs numériques** (**DXC**, *Digital Cross Connect*) modifient l'affectation des flux d'information entre un affluent d'entrée et un affluent de sortie. Le croisement de flux est défini par l'opérateur, il est permanent.

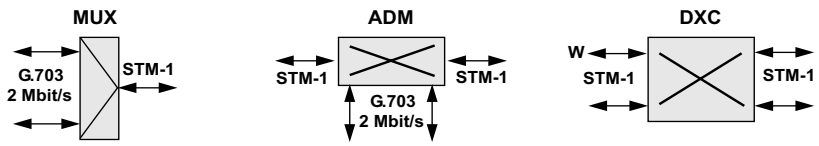


Figure 13.18 Les équipements SDH.

Le multiplexage des différents affluents d'ordre *N* vers un affluent d'ordre *N+1* est réalisé par entrelacement d'octets (figure 13.19).

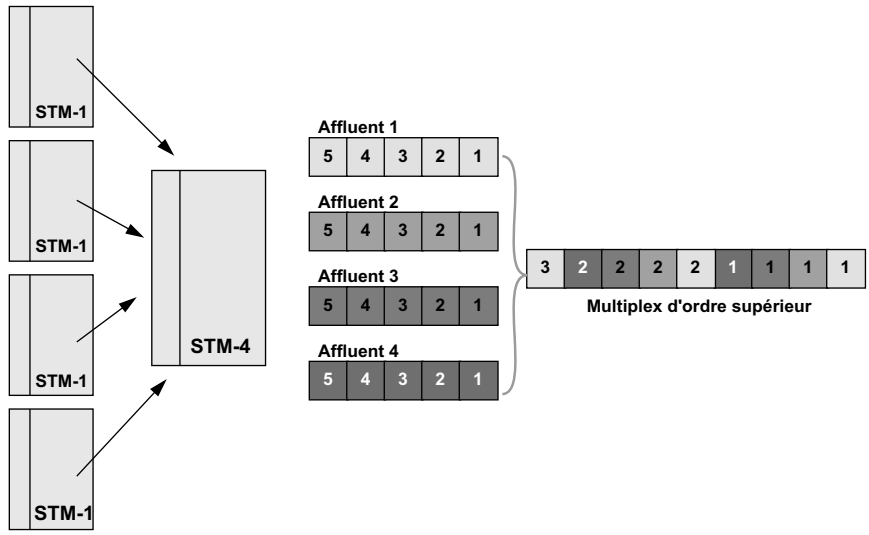


Figure 13.19 Principe du multiplexage d'octets.

L'entrelacement temporel d'octets permet d'une part, en répartissant les erreurs, d'en améliorer la détection et, d'autre part de faciliter l'extraction/insertion, il n'est pas nécessaire d'attendre la réception complète de l'affluent pour débuter son insertion/extraction dans le multiplex d'ordre supérieur/inférieur.

La topologie d'un réseau SDH

La technologie SDH peut être mise en œuvre sur toutes les formes de topologie : point à point, arborescente, bus, anneau et maillée[6]. Généralement, les réseaux dorsaux utilisent une topologie maillée alors que les réseaux de desserte (métropolitain) sont constitués d'une hiérarchie d'anneaux (figure 13.20).

Un autre avantage des infrastructures SDH concerne les mécanismes de sécurisation automatique qui permettent le rétablissement du trafic dans des délais d'environ 50 ms. Ce mécanisme, dit d'**autocicatrisation** (**APS**, *Automatic Protection Swiching*), est basé sur l'utilisation d'informations de supervision contenues directement dans l'en-tête SDH (surdébit de section, SOH).

13.2.5 La transmission optique

Si la hiérarchie synchrone se préoccupe de la structuration des données, la transmission physique est aujourd'hui optique. L'apparition des systèmes WDM/DWDM *(Wavelength Division Multiplexing, Dense WDM*) illustré figure 13.21 permet sur une seule fibre de disposer jusqu'à 128 canaux de communication. Les amplificateurs optiques dopés à l'erbium (EDFA, *Erbium Doped Fiber Amplifier*) compensent les pertes d'insertion dues aux opérations de multiplexage et de démultiplexage.

6. La tendance actuelle est plutôt au développement de réseau « marguerite » : ensemble d'anneaux autour d'un cœur de réseau, lui-même une boucle (boucle nationale, boucle régionale, boucle métropolitaine).

© Dunod – La photocopie non autorisée est un délit

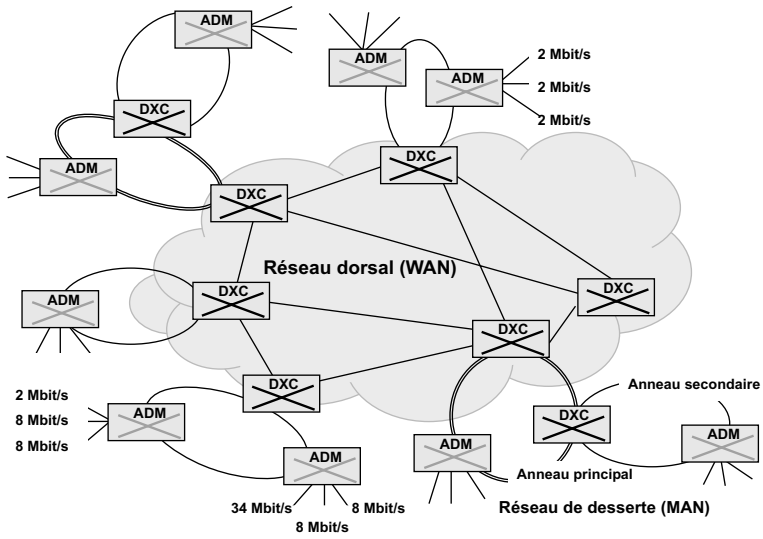


Figure 13.20 Principe d'un réseau SDH.

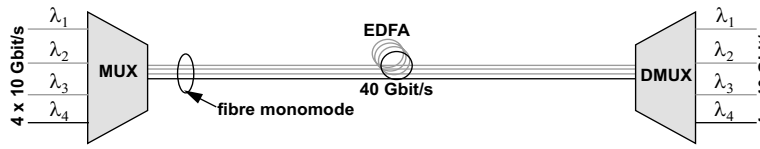


Figure 13.21 Principe d'une liaison DWDM.

13.3 LE PLAN DE SERVICE

13.3.1 Généralités

Le plan de service (figure 13.22) correspond au réseau de transport de données. L'interconnexion des installations locales de l'usager est réalisée par le plan service.

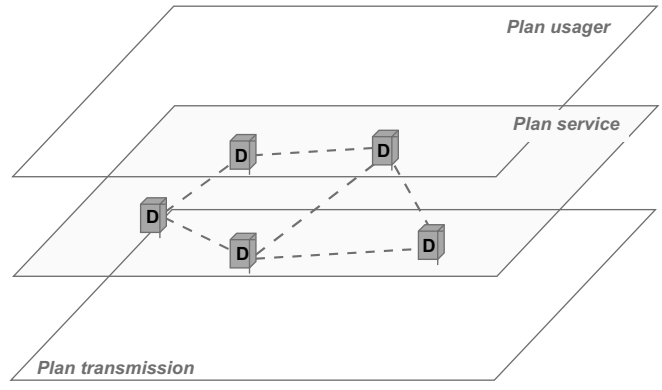


Figure 13.22 Le plan de service.

La figure 13.23 représente le réseau de transport tel que le voit l'usager.

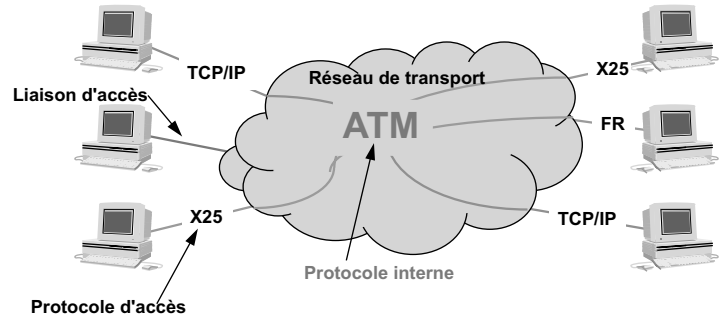


Figure 13.23 Les protocoles d'accès et protocole interne.

Au cours des années 1970, la recherche de la performance a orienté les concepteurs de réseaux vers la réalisation de réseaux à commutation de paquets (*Packet switching*) en mode orienté connexion (**CONS**, *Connection Oriented Network Service*) avec le protocole X.25. À l'origine, défini comme protocole d'accès aux réseaux de transport, X.25 a très vite évolué vers un protocole de cœur de réseau. Le besoin croissant de bande passante a rapidement conduit les opérateurs à rechercher des protocoles internes plus efficaces : d'abord le relais de trames (**FR**, *Frame Relay*), puis l'**ATM** (*Asynchronous Transfer Mode*).

Cependant, afin de garantir la pérennité des services et de faire bénéficier les usagers des progrès technologiques, les accès X.25 ont été maintenus et des accès FR et TCP/IP ont été offerts (figure 13.24). Deux modes d'accès aux réseaux publics sont définis :

– Les modes d'accès permanent (*On-line*), l'utilisateur est alors relié au réseau *via* une ligne dédiée (liaison spécialisée).
– Les modes d'accès temporaire (*Dial-up*), l'utilisateur accède alors au réseau *via* le réseau téléphonique (RTC ou RNIS).

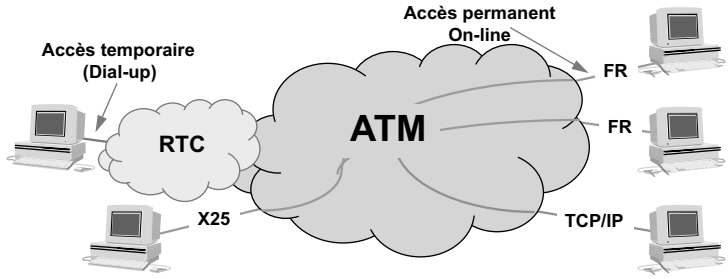


Figure 13.24 Les différents modes d'accès au réseau de transport.

13.3.2 Introduction aux protocoles réseaux

Le protocole X.25

Conçu par les PTT français et britanniques, TCTS (*Trans Canada Telephon System*) et Telnet (États-Unis), le protocole X.25 a été le premier protocole utilisé dans les réseaux publics de

© Dunod – La photocopie non autorisée est un délit

données. C'est en décembre 1978 que Transpac (*Transmission by packet*, filiale de France Télécom) a ouvert le premier réseau mondial public de transmission en mode paquet X.25 (**PSPDN**, *Packet Switched Public Data Network*). L'avis **X.25,** adopté en septembre 1976 par le CCITT (UIT-T), définit les protocoles d'accès au réseau, c'est-à-dire le protocole entre l'ETTD (DTE) et le réseau (ETCD ou DCE dans la norme X.25).

Le protocole X.25[7] couvre les trois premières couches du modèle OSI[8] (figure 13.25) :

– La couche physique, niveau bit ou X.25-1 définit l'interface ETTD/ETCD. Elle est conforme à l'avis X.21 et X.21 bis de l'UIT-T.
– La couche liaison, niveau trame ou X.25-2, met en œuvre un sous-ensemble d'HDLC appelé LAP-B (*High Level Data Link Control*, *Link Access Protocol Balenced*).
– La couche réseau, niveau paquet ou X.25-3, gère les circuits virtuels (permanents ou commutés). Si un ETTD peut communiquer simultanément, sur une même liaison d'abonné, avec plusieurs sites distants, l'accès au réseau est dit multivoie, dans le cas contraire, l'accès est dit **univoie** ou **monovoie**.

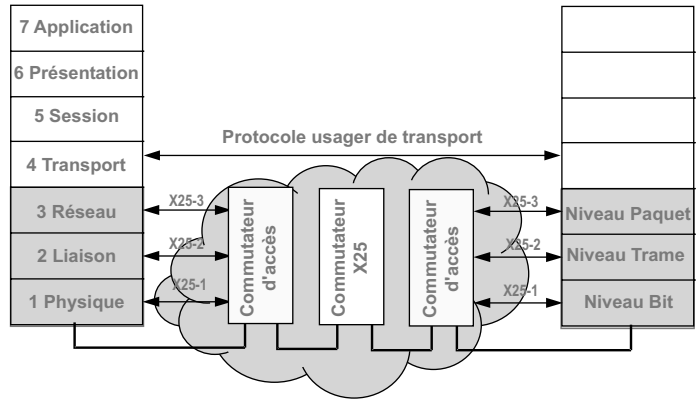


Figure 13.25 L'architecture du protocole X.25.

Dans le protocole X.25, la signalisation est du type dans la bande, ce qui signifie que les données et les informations de signalisation sont transportées par des unités de données similaires. Indépendamment de la pauvreté d'un tel système de signalisation, l'établissement de la route et la commutation sont réalisées au même niveau et traitées par une même instance de programme, ceci a pour conséquence immédiate non seulement de multiplier les opérations d'encapsulation et de décapsulation mais surtout de pénaliser les performances.

La décentralisation des traitements vers une architecture largement distribuée de type client/serveur a modifié l'amplitude et la nature des trafics sur les liens d'interconnexion. L'accroissement des débits nécessaires et la sporadicité des échanges caractérisent essentiellement cette évolution, rendant obsolète les offres de débit figées telles que celles d'X.25.

7. Le protocole X.25 est étudié en détail au chapitre suivant.
8. Le modèle OSI a été décrit au chapitre 7.

Le développement d'applications multimédias (données, son, vidéo) a, non seulement, engendré un besoin de débit plus important, mais a introduit également des contraintes temporelles strictes dans les échanges (trafic isochrone). X.25 ne peut répondre à cette demande.

Introduction à l'évolution des protocoles réseaux

L'évolution des protocoles réseaux s'est réalisée selon deux approches (figure 13.26) :

- Le relais de trames ou *Frame Relay* qui correspond à un allégement du protocole HDLC version LAP-D. Ce protocole répond aux besoins de haut débit ; ne traitant pas les flux isochrones à l'origine, il a été perçu comme un protocole de transition entre X.25 et ATM ;
- Le relais de cellules ou *Cell Relay*, plus connu sous le nom d'**ATM** (*Asynchronous Transfer Mode*) qui utilise une technique de commutation rapide de cellules de taille fixe. ATM met en œuvre des mécanismes spécifiques pour assurer les transferts isochrones (émulation de circuits pour la voix et la vidéo).

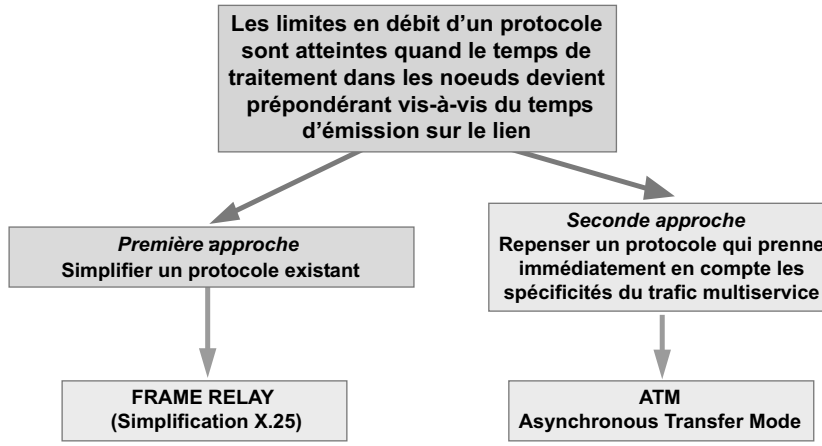


Figure 13.26 Les différentes approches des nouveaux protocoles.

C'est dans le cadre de l'évolution du RNIS (**RNIS-LB**, RNIS large bande ou **B-ISDN**, *Broadband-ISDN*) qu'ont été développés le Frame Relay et l'ATM.

L'augmentation du débit réel de ces protocoles ne peut résulter que de l'allégement des traitements intermédiaires, ce qui a conduit à :

- reporter sur les organes d'extrémité (les calculateurs) les tâches de détection et de reprise sur erreur ;
- diminuer les opérations de couches en effectuant les opérations d'acheminement le plus bas possible, sans avoir à remonter au niveau 3 ;
- formuler des hypothèses optimistes sur le comportement du réseau en n'effectuant pas de contrôle de flux entre les nœuds ;
- supprimer les acquittements intermédiaires, ceux-ci n'étant réalisés que par les organes d'extrémité (acquittement de bout en bout) ;

© Dunod – La photocopie non autorisée est un délit

– simplifier le traitement dans les nœuds en n'utilisant qu'un seul type de données et en mettant en œuvre une signalisation par **canal sémaphore** pour l'établissement des circuits et la gestion du réseau.

C'est notamment, l'introduction de la fibre optique dans les réseaux qui, en fiabilisant la transmission, a autorisé cette simplification des protocoles. La figure 13.27 représente l'architecture générale de ces nouveaux protocoles :

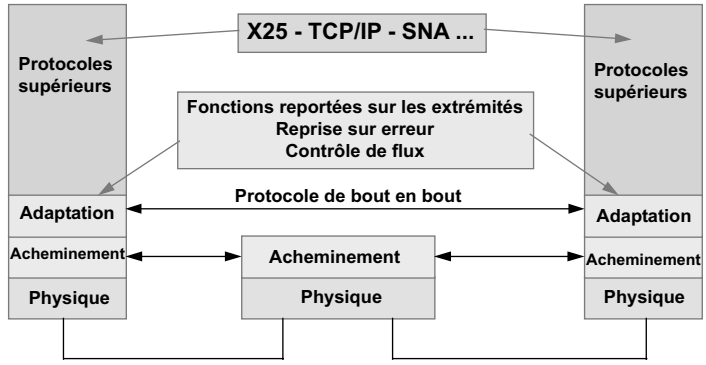


Figure 13.27 L'architecture générale des réseaux haut débit.

Dans ce type d'architecture, la couche 2 est scindée en deux sous-couches : un noyau assurant les fonctions élémentaires d'acheminement, de détection d'erreur et de signalisation de la congestion, et une couche d'adaptation entre les protocoles supérieurs et le noyau. Cette dernière, facultative, n'est présente que sur les organes d'extrémité. L'ensemble assure la transparence aux protocoles supérieurs.

Introduction au Frame Relay

La première approche d'allégement des tâches X.25 a concerné l'acheminement. Le champ Adresse de la trame LAP-B étant inutilisé, il était possible d'y inscrire l'information d'indication du numéro de voie logique et de réaliser ainsi la commutation au niveau 2 (*Frame switching* ou commutation de trames). Ce principe est illustré figure 13.28.

Par la suite, toutes les fonctions non liées directement à l'acheminement furent abandonnées pour donner naissance au **relais de trames** (*Frame Relay*) ou encore **LAP-F**. Initialement prévue pour une utilisation sur le RNIS (Canal D ou sur un ou plusieurs canaux B), la technologie Frame Relay[9] a rapidement évolué, sous l'égide du Frame Relay Forum[10], vers un service de liaisons virtuelles permanentes, puis commutées utilisables sur tout support numérique, hors RNIS.

Le relais de trames offre un service réseau en mode connecté conforme à l'avis Q.922 de l'UIT-T. La signalisation est du type canal sémaphore conforme à l'avis Q.933 (évolution de l'avis Q.931, protocole D du RNIS). Elle établit un service de liaison virtuelle entre les deux extrémités, qui peut

9. Le protocole *Frame Relay* est étudié en détail au chapitre suivant.

10. Afin d'harmoniser les solutions, de combler les vides des normes et de proposer rapidement des solutions techniques cohérentes, les constructeurs se regroupent autour d'une technologie pour édicter leurs propres règles : ce sont les forums constructeurs.

être permanent (PVC, *Permanent Virtual Circuit*) ou établi à la demande (SVC, *Switched Virtual Circuit*). Compte tenu de la complexité d'établissement d'un SVC, les opérateurs n'offrent qu'un service de circuits virtuels permanents.

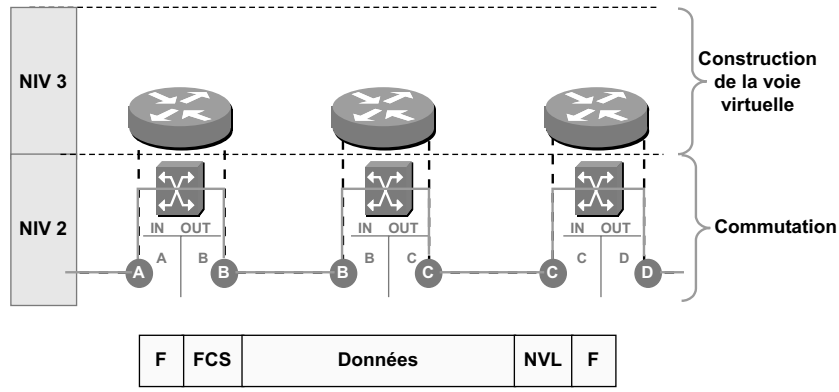


Figure 13.28 Première approche du Frame Relay.

Le relais de trames couvre les couches 1 et 2 du modèle OSI, mais n'est pas conforme à ce dernier. La couche physique émet un train de bits sur le support en assurant la transparence binaire (technique dite du *Bit stuffing* ou de transparence binaire)

La couche 2 est subdivisée en deux sous-couches : le noyau (*Core*) et une sous-couche (**EOP**, *Element of Procedure*) complémentaire mais facultative. Non normalisées, ces fonctionnalités sont laissées à la discrétion de l'utilisateur. Cette sous-couche 2 supérieure peut, par exemple, être HDLC LAP-B. La répartition des fonctions essentielles est schématisée par la figure 13.29.

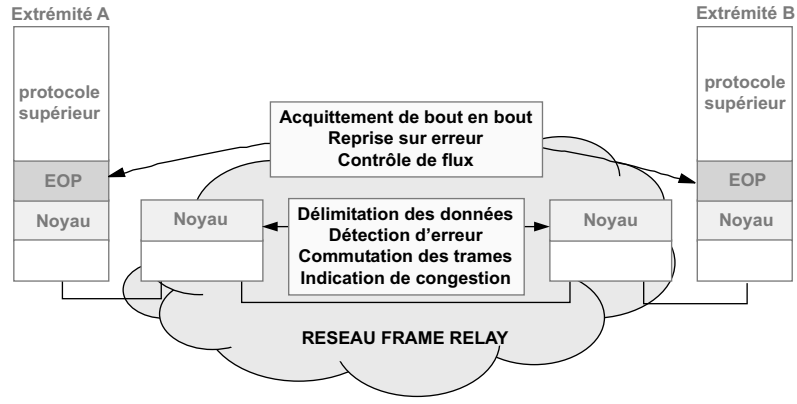


Figure 13.29 L'architecture du relais de trames.

Introduction à l'ATM (Asynchronous Transfer Mode)

Le relais de trames n'est qu'une évolution d'HDLC (LAP-D). Peu adapté, en natif, au transfert des flux isochrones, il n'est parfois perçu que comme une solution temporaire au besoin de haut débit. Ses limitations sont essentiellement dues au traitement d'unités de données de taille variable.

© Dunod – La photocopie non autorisée est un délit

Pour pallier cet inconvénient, la recommandation FR11 (Frame Relay Forum 11) introduit, pour le traitement de la voix, la notion de trames de longueur fixe.

C'est l'approche initiale d'ATM[11] qui, en traitant des unités de données de taille réduite et fixe (cellules), a considérablement réduit les temps de traitements. La commutation est alors directement réalisée par des systèmes matériels (*hardware*) et non plus logiciels, ce qui autorise des débits de plusieurs centaines de mégabits par seconde.

C'est sur ces bases que le CNET (Centre nationale d'étude et de télécommunication) a décrit, en 1982, une technique de multiplexage asynchrone (**ATD**, *Asynchronous Time Division*) qui allait donner naissance à l'ATM. L'ATM supporte des liaisons point à point, ou point à multipoint, il comporte trois couches (figure 13.30) dont les fonctions essentielles sont :

– assurer l'adaptation des cellules au système de transport physique utilisé (couche physique),
– effectuer la commutation et le multiplexage des cellules (couche ATM à proprement parler),
– adapter les unités de données (segmentation et réassemblage) des protocoles supérieurs à la couche ATM (couche **AAL**, *ATM Adaptation Layer*) et mettre en place des mécanismes spécifiques à chaque type de données transportées.

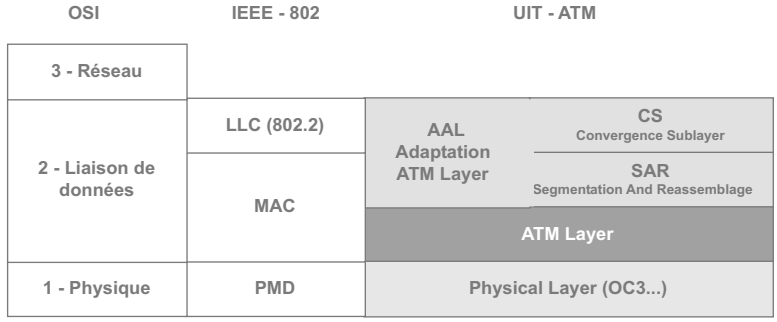


Figure 13.30 L'architecture ATM.

L'ATM est une technologie en mode connecté, les données ne sont acheminées dans le réseau qu'après l'établissement d'une voie virtuelle (**VCC**, *Virtual Channel Connection*). Le circuit établi peut-être :

– bidirectionnel en mode point à point (*unicast*),
– unidirectionnel en mode point à multipoint (*multicast*).

Technologie orientée connexion, l'ATM peut, toutefois, émuler un mode de fonctionnement non connecté.

Conclusion

Autorisant un partage optimal de la bande passante, l'ATM est aujourd'hui le protocole de cœur de réseau utilisé par la majorité des opérateurs. Outre l'aspect performance, l'ATM permet de garantir aux utilisateurs une certaine qualité de service de bout en bout.

11. Le protocole ATM est étudié en détail au chapitre suivant.

L'ATM n'est pas un protocole de bout en bout comme l'est TCP/IP, ce n'est qu'un protocole de transport. Les données utilisateurs doivent donc être encapsulées, ceci conduit à des empilements protocolaires fortement pénalisants. Aussi, la tendance actuelle consiste à appuyer les protocoles utilisateurs (TCP/IP) sur la couche transmission (**POS**, *Packet Over SDH/Sonet*) voire directement sur la couche optique. Cependant, afin d'apporter au monde IP les avantages de la commutation, une couche supplémentaire a été introduite afin de labéliser les datagrammes IP et de substituer au routage IP la commutation. MPLS (*MultiProtocol Label Switching*) associé à PPP permet le transport des flux IP sur SDH (figure 13.31), voire directement sur un canal optique (**WDM**, *Wavelength Division Multiplexing* ou multiplexage de longueur d'onde).

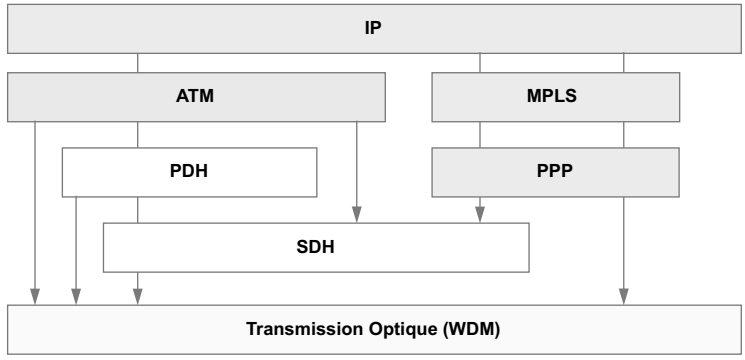


Figure 13.31 L'évolution de l'architecture protocolaire des réseaux.

13.3.3 Les réseaux d'opérateurs

Généralités

Les réseaux d'opérateurs assurent deux fonctions essentielles, la collecte des flux des différentes sources par un ensemble de liens formant le réseau d'accès, et l'acheminement de ce trafic par leurs réseaux dits de transit. Certains opérateurs n'assurent que l'une des deux fonctions, on distingue alors les opérateurs de boucle locale et les opérateurs de transit. On appelle point de présence (**PoP**, *Point of Presence*) l'interface d'interconnexion entre le réseau d'accès et le réseau de transit (figure 13.32).

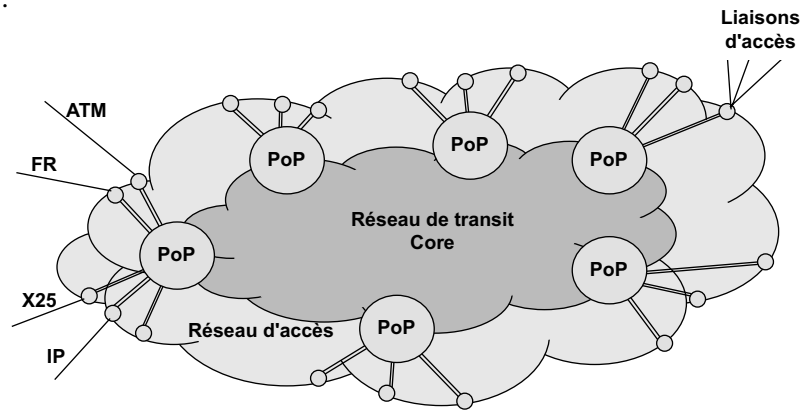


Figure 13.32 L'architecture du plan de service.

© Dunod – La photocopie non autorisée est un délit

La conception d'un réseau d'opérateur doit répondre à trois critères :

– performance pour le cœur de réseau (réseau de transit) ;
– flexibilité à la périphérie (PoP) ;
– enfin, capacité d'irrigation pour le réseau de desserte (réseau d'accès).

Les réseaux IP

La plupart des réseaux d'opérateurs mettent en œuvre le protocole ATM, alors que la majorité des utilisateurs utilisent le protocole TCP/IP. On désigne sous le nom de réseau IP, l'infrastructure de l'opérateur destinée à acheminer le trafic IP. Le trafic IP peut être tout simplement encapsulé dans l'ATM sans apport de qualité de service (figure 13.33).

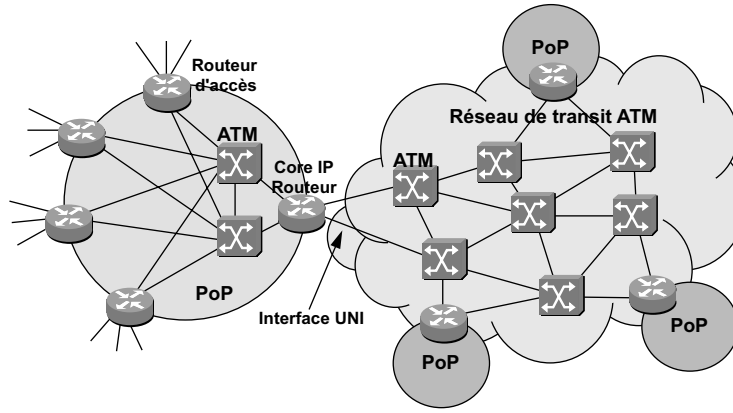


Figure 13.33 Les réseaux IP/ATM.

Cependant l'utilisation du protocole MPLS[12] (*MultiProtocol Label Switching*) permet d'assurer un trafic différencié (DiffServ) par distribution des labels et mappage de ceux-ci sur une voie ATM (figure 13.34).

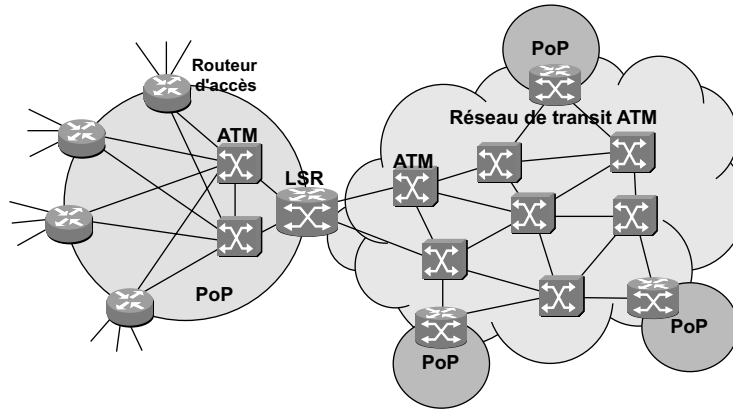


Figure 13.34 Les réseaux IP/MPLS sur ATM.

12. Le protocole MPLS est étudié en détail au chapitre 15.

Les routeurs d'interface (*Core IP Router*) sont remplacés par des commutateurs/routeurs qui attribuent un label MPLS aux datagrammes IP (**LSR**, *Label Switching Router*). Remarquons que chaque routeur d'accès et LSR disposent, pour des raisons de sécurité, d'un double attachement aux commutateurs ATM (voir § 13.4.3).

13.4 L'ACCÈS AUX RÉSEAUX, LA BOUCLE LOCALE

13.4.1 Définition

La boucle locale correspond à l'ensemble des moyens mis en œuvre par un opérateur pour collecter le trafic des utilisateurs. Une définition plus restrictive limite l'utilisation du terme boucle locale au seul câble de raccordement usager/réseau. Pour des raisons historiques, l'infrastructure du réseau de boucle locale correspond à celle de la distribution des services voix. Cette infrastructure est aujourd'hui partagée entre les accès aux réseaux voix et les accès aux réseaux de données.

13.4.2 Organisation de la distribution des accès

Les moyens d'accès se répartissent en deux catégories, les accès aux réseaux d'opérateurs (opérateurs de boucle locale) et les moyens fournis à l'usager pour raccorder ses propres sites informatiques et réaliser ainsi un réseau privé (opérateur de liaisons louées). La figure 13.35 illustre cette approche.

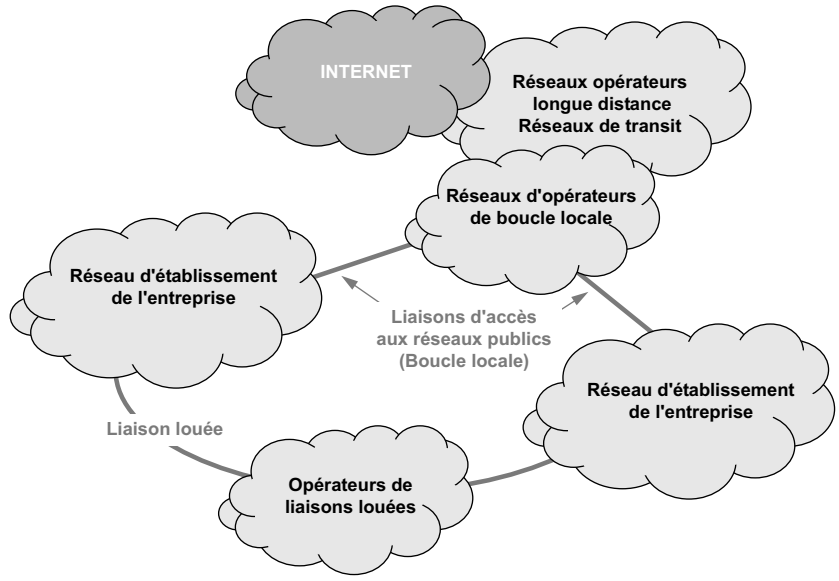


Figure 13.35 Principe du raccordement des usagers.

La réalisation d'un réseau de distribution (collecte) nécessite des investissements importants. Dans la plupart des pays, ces réseaux ont été financés par des ressources publiques. La mise en concurrence des télécommunications a donc posé le problème du partage de cette ressource.

© Dunod – La photocopie non autorisée est un délit

C'est sous le terme de dégroupage de la boucle locale que l'**ART** (Autorité de régulation des télécommunications[13]) a organisé ce partage, en instituant la colocalisation des équipements actifs (figure 13.36).

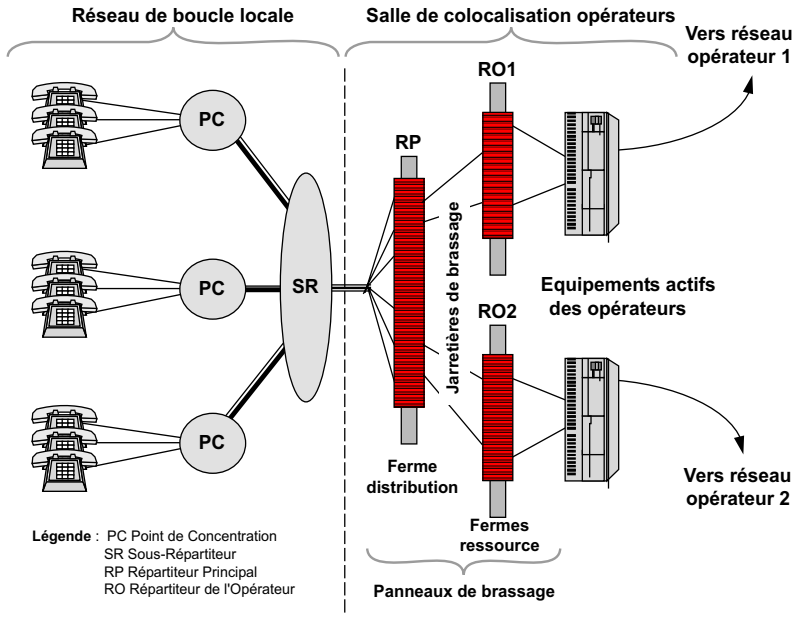


Figure 13.36 Dégroupage total selon l'ART.

La notion de dégroupage se décline selon 2 modes accès à la boucle locale. Le dégroupage total donne, à un opérateur autre que France Télécom, l'accès à toute la bande de fréquences de la paire de cuivre. L'ensemble des services, téléphonie et accès Internet est alors complètement géré par l'opérateur alternatif. Dans le dégroupage partiel, l'opérateur alternatif n'a accès qu'aux fréquences hautes de la paire de cuivre, les services téléphoniques (fréquences basses) restent gérés par France Télécom.

13.4.3 L'accès aux réseaux par liaison dédiée (ligne spécialisée)

Principe

Les liaisons louées peuvent être utilisées pour réaliser des réseaux privés, mais elles constituent aussi le principal moyen d'accès permanent au réseau d'un opérateur réseau de transport qui les loue à un opérateur de liaisons louées. L'opérateur de service réseau fournit alors les moyens d'extrémités, modems voire l'équipement d'accès appelé **CPE** (*Customer Premises Equipment*) pouvant être un routeur, un FRAD *(Frame Relay Access Device*), un commutateur...). La figure 13.37 illustre le principe d'un tel accès.

13. Depuis le 20 avril 2005, l'ART est devenu l'ARCEP (Autorité de régulation des communications électroniques et des postes).

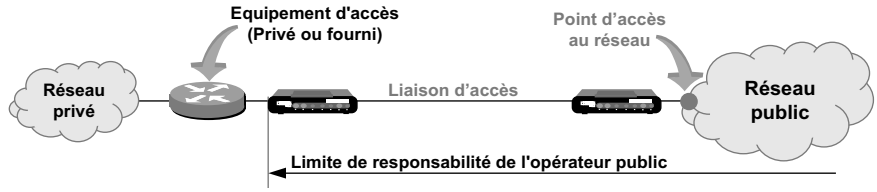


Figure 13.37 Principe de l'accès permanent à un réseau.

Sécurisation des accès

La permanence de l'accès au système d'information est devenue un enjeu stratégique pour les entreprises. Aussi de nombreuses mesures sont prises pour la garantir et, en particulier, la sécurisation des liens vers l'extérieur. La figure 13.38 illustre l'un de ces moyens. Le réseau final est relié par deux liens en deux points d'accès différents au réseau de l'opérateur. Le protocole de routage externe **eBGP** (*Border Gateway Protocol*) est utilisé pour annoncer, au réseau public, les liens et les coûts vers le réseau privé. Dans le mode actif/passif, le plus fréquemment utilisé, chaque routeur annonce cette accessibilité avec un coût différent. Le routeur R1, annonçant le moindre coût sera élu comme étant le routeur d'accès au réseau (routeur actif). En cas de défaillance du routeur actif, ou de coupure du lien, aucune annonce en provenance de R1 n'est reçue, la route annoncée par le routeur R2 devient alors la route de moindre coût (c'est la seule !), R2 bascule en mode actif. Lorsque la défaillance sera résolue, R1 annonçant un moindre coût redevient actif et R2 passif.

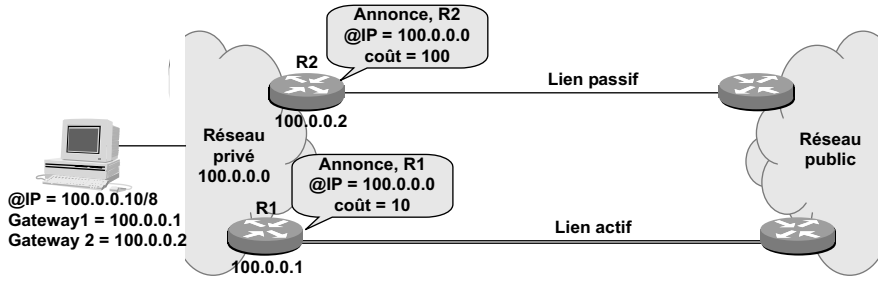


Figure 13.38 Principe de la redondance d'accès mode actif/passif.

Si l'architecture d'accès en mode actif/passif augmente la disponibilité d'un site, elle est coûteuse car l'une des liaisons est inutilisée alors que son coût n'est généralement pas négligeable. La solution consiste alors à scinder le réseau du site en deux sous-réseaux et de croiser les annonces. Le routeur R1 annonce le sous-réseau 1 avec un coût A et le sous-réseau 2 avec un coût B (avec par exemple A < B), alors que le routeur 2 annonce le sous-réseau 1 avec un coût de B et le sous-réseau 2 avec un coût de A (A > B). Ce mode de fonctionnement est dénommé Actif/Actif (figure 13.39).

Cependant, dans ces configurations, les deux routeurs de bordures du réseau privé sont connus du réseau par deux adresses différentes. Les stations du réseau doivent donc être capables d'adresser ces deux routeurs, ce qui peut poser un problème de configuration ou d'architecture du réseau. Le protocole **VRRP** (*Virtual Router Redundancy Protocol,* RFC 2338) résout ce problème en permettant à un ensemble de routeurs situé dans un même domaine de diffusion d'être vus par une

© Dunod – La photocopie non autorisée est un délit

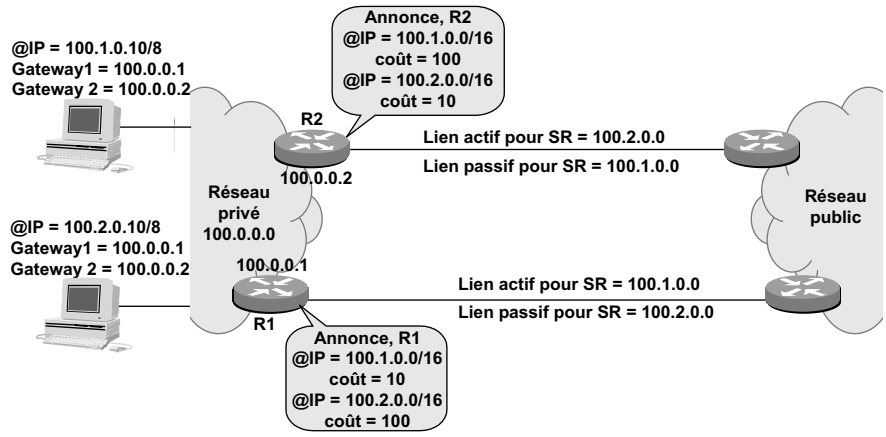


Figure 13.39 Principe de la redondance d'accès mode actif/actif.

seule et même adresse IP (IP virtuelle) et une seule et même adresse MAC (MAC virtuelle). Un seul routeur est actif à la fois. La figure 13.40 illustre le principe du protocole VRRP

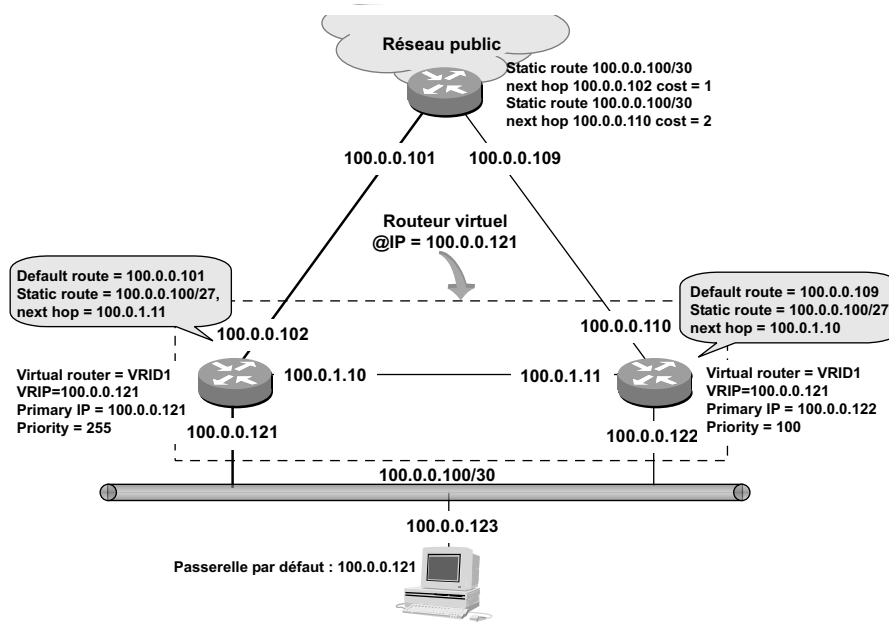


Figure 13.40 Principe du protocole VRRP.

Un domaine VRRP comprend :

– un ensemble de routeurs identifiés par un même **VRID** (*Virtual Router ID*) ;
– un routeur maître, seul actif à un moment donné (*Master Virtual Router*) ;

– un routeur propriétaire de l'adresse IP du groupe VRRP, le « *Owner Virtual Router* », c'est sur cette adresse que sont réalisées les opérations de routage, alors que tous les autres routeurs du groupe restent identifiés par une adresse IP propre ;
– un ou plusieurs routeurs « *Backup Virtual Router* » capable de prendre le relais du routeur primaire en cas de défaillance de celui-ci ou de la chute d'un lien de ce dernier.

Différentes priorités sont affectées aux routeurs du groupe VRRP qui déterminent l'ordre d'élection du routeur actif en cas de défaillance du routeur principal. Le routeur actif par défaut se voit attribuer la plus haute priorité, soit 255. En permanence le système émet des trames de contrôle VRRP (*Hello*) à l'adresse *multicast* 224.0.0.18 et à l'adresse MAC associée 01:00:5E:00:00:*xx* où *xx* représente l'identifiant du groupe de routeur (VRID). La défaillance du routeur actif est détectée par l'arrêt de ces diffusions. La figure 13.41 illustre les différents cas de dysfonctionnement, dans une configuration spécifique où un lien de secours supplémentaire a été réalisé entre les deux routeurs du groupe VRRP.

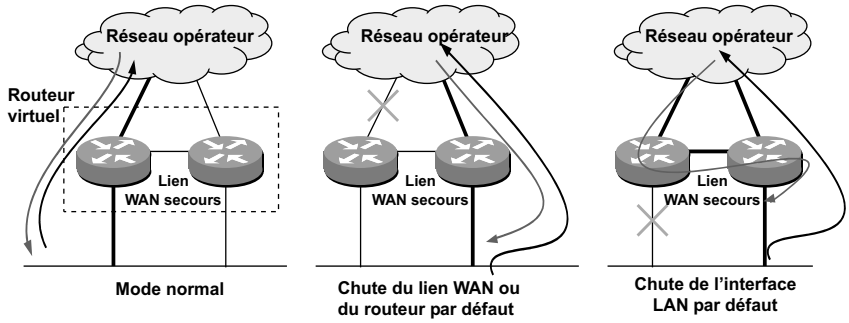


Figure 13.41 Principe du protocole VRRP.

Le protocole VRRP fonctionne en mode Actif/Passif, des implémentations propriétaires autorisent un mode Actif/Actif.

13.4.4 La Boucle locale radio (BLR)

Compte tenu des coûts d'accès à l'infrastructure cuivre et/ou du coût de réalisation d'une telle infrastructure, certains opérateurs se sont tournés vers la mise en œuvre de liaisons radios (**WLL**, *Wireless Local Loop* ou Boucle locale radio, BLR). La BLR permet de proposer l'accès à un grand nombre d'abonnés pour un coût relativement faible, elle est particulièrement bien adaptée aux zones semi-urbaines à densité de population intermédiaire. En fait la BLR présente de nombreux avantages :

– coût de déploiement faible,
– capacité d'innerver des zones à accès difficile,
– éventuellement de proposer des services de mobilité...

La technologie cellulaire mise en œuvre collecte les flux et permet la diffusion. La figure 13.42 décrit un système de BLR.

© Dunod – La photocopie non autorisée est un délit

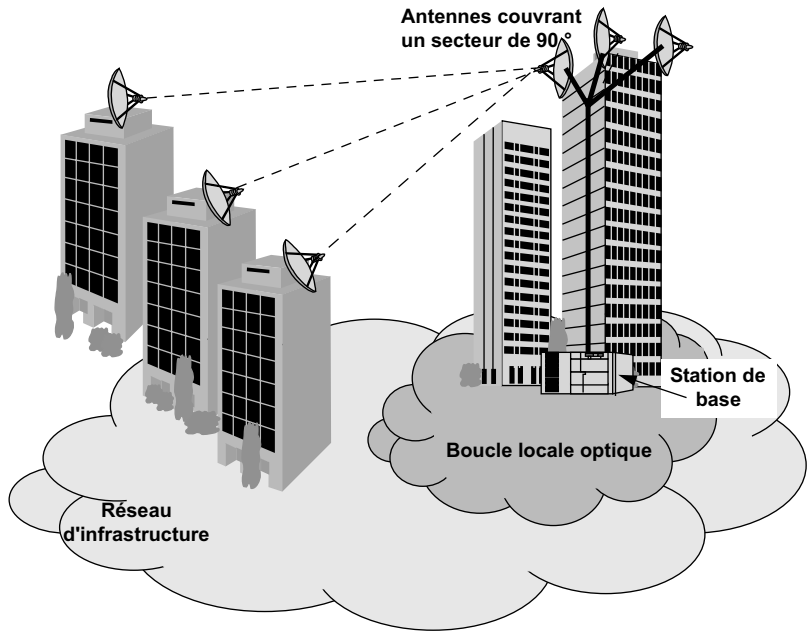


Figure 13.42 Principe de la BLR.

Utilisant une bande de fréquence de 3,5 GHz et 26 GHz, la technologie LMDS (*Local Multipoint Distribution System*) autorise :

– en mode point à point, dans la bande des 26 GHz, des débits pouvant atteindre, dans un rayon de 3 à 5 km autour de la base, des débits de 155 Mbit/s ;
– toujours dans la bande des 26 MHz, mais en mode point-multipoint (bande partagée par plusieurs utilisateurs) les débits partagés de 256 kbit/s à 10 Mbit/s ;
– enfin en mode point-multipoint dans la bande des 3,5 GHz des débits partagés de 64 kbit/s à 2 Mbit/s avec une portée d'environ 10 à 20 km.

Se présentant comme un concurrent aux accès filaires à Internet et aux réseaux téléphoniques des opérateurs, la BLR n'a pas connu le succès espéré. La définition de nouvelles normes par l'IEEE : 802.16 (**WiMax**, *Worldwide Interoperability for MicroWave Access*) ou Ethernet sans fil dans les réseaux métropolitains relance l'intérêt des interfaces radio dans les réseaux d'accès.

À l'instar de la BLR à 26 GHz en mode point à point, le WiMax offre des débits symétriques pouvant atteindre, en théorie, 72 Mbit/s avec une portée de 50 km. En pratique le débit est d'environ 12 Mbit/s avec une portée réelle maximale de 20 km. En mode point-multipoint le WiMax est une alternative à l'accès ADSL avec un débit partagé de 12 Mbit/s.

13.4.5 Les accès hauts débits

Généralités

Dans les grandes métropoles, la diffusion de programmes vidéo a largement fait appel à la fibre optique qui constitue le support idéal pour les transmissions large bande (**PON**, *Passive Optical*

Network). Amener la fibre optique chez l'abonné (**FTTH**, *Fiber To The Home*) semble la solution idéale mais elle est trop coûteuse (figure 13.43). Aussi, la distribution chez l'abonné final est généralement réalisée par un câble cuivre à partir d'un point de distribution commun situé dans l'immeuble (**FTTB**, *Fiber To The Basement*) ou au plus près d'un groupe d'habitations (**FTTC**, *Fiber To The Curve*).

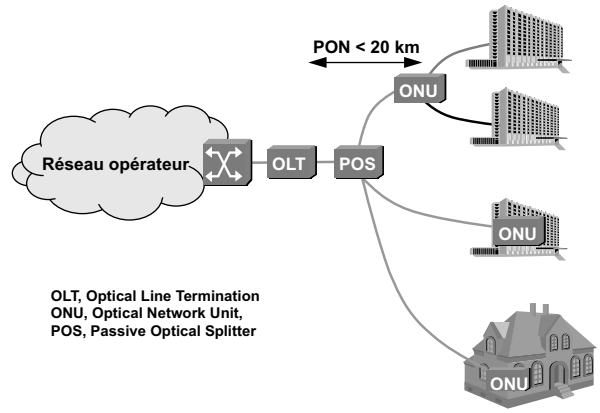


Figure 13.43 Principe de la boucle locale optique.

Selon l'équipement terminal (**CPE***, Customer Premises Equipment*) le protocole mis en œuvre s'appuie directement sur ATM (**APON**, *ATM over PON*) ou sur **EPON** *(Ethernet over PON*). Les réseaux de distribution vidéo des câblo-opérateurs utilisent largement ces techniques, la figure 13.44 illustre le principe de ces réseaux qui mixent des solutions optiques et coaxiales (réseaux **HFC**, *Hybrid Fiber Coaxial*). Le modem câble offre un débit de 10 Mbit/s dans le sens descendant et 768 kbit/s dans le sens montant.

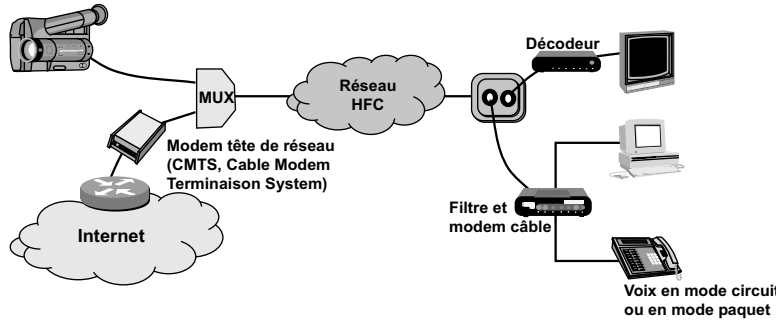


Figure 13.44 Principe des réseaux CATV (*Cable Television*).

La figure 13.45 présente l'aspect protocolaire de l'accès Internet *via* les réseaux CATV. Cependant, cette approche nécessite des travaux d'infrastructure qui ne peuvent être rentabilisés que dans les grandes métropoles. Aussi, compte tenu de la base installée, l'idée de réutiliser l'ensemble de la distribution téléphonique pour offrir, à tout abonné du réseau téléphonique commuté résidentiel ou entreprise, un accès haut débit sur une simple ligne téléphonique a conduit à rechercher de nouvelles technologies permettant d'exploiter au mieux cette infrastructure.

© Dunod – La photocopie non autorisée est un délit

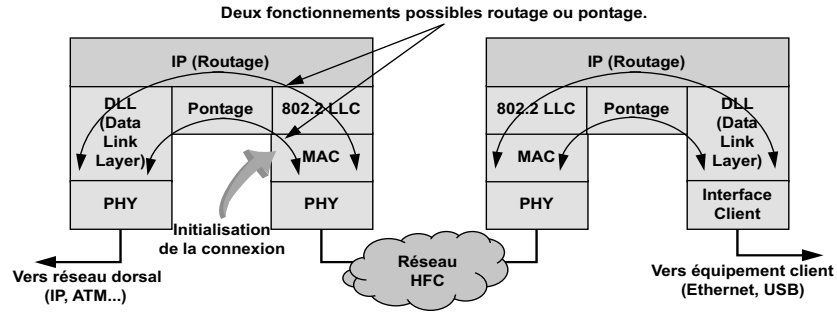


Figure 13.45 Principe de l'accès Internet *via* un réseau CATV.

Les techniques DSL

La bande passante du service voix est limitée à 4 kHz, cependant la bande passante réelle de la paire torsadée est supérieure au MHz. La technologie **ADSL** (*Asymmetric data rate Digital Subscriber Line*) tout en préservant la bande nécessaire au service téléphonique offre un accès haut débit à l'utilisateur final. ADSL partage la bande disponible entre le service voix (0 à 4 kHz) et deux canaux données simplex, l'un dit montant (*Up*) offre une bande passante de 32 à 640 kbit/s, le second (*Down*) un débit de 1,5 à 8,2 Mbit/s.

Les données sont transposées en fréquence selon un codage spécifique dit **DMT**[14] (*Discrete MultiTone*) dans la bande de 25 kHz à 1,1 MHz. Le codage DMT divise chacun des spectres haut débit en sous-canaux (porteuses ou tonalités) espacés de 4,312 5 kHz. Chaque sous-canal, modulé en phase et en amplitude (MAQ) codant, en principe, 8 bits dans un temps d'horloge, constitue un symbole DMT. Le nombre de bits codés par symbole dépend de l'état de la ligne. Le canal ascendant comporte 20 tonalités ou symboles DMT soit, à une rapidité de modulation de 4 kBaud (4 000 symboles DMT par unité de temps), une bande passante maximale de 640 kbit/s ($20 \times 8 \times 4\,000$). Le canal descendant est constitué de 256 sous-canaux, soit un débit maximal de 8,192 Mbit/s ($256 \times 8 \times 4\,000$). Selon les conditions de transmission sur la ligne, certains sous-canaux, dont le rapport signal sur bruit et/ou le niveau du signal sont insuffisants, peuvent être inhibés. En adaptant le nombre de bits par symbole et le nombre de sous-canaux utilisés, DMT optimise en permanence le débit en fonction de la qualité du canal de transmission par pas de 32 kbit/s (figure 13.46).

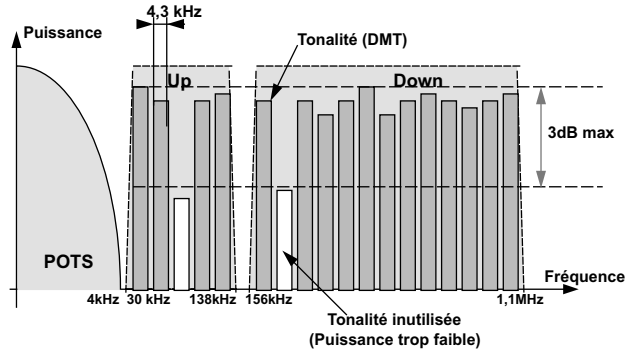


Figure 13.46 Le spectre DMT utilisé dans l'ADSL.

14. La modulation DMT est aussi appelée OFDM (*Orthogonal Frequency Division Multiplexing*).

L'accès au réseau haut débit de l'opérateur *via* la ligne téléphonique nécessite l'installation d'un équipement spécifique chez l'utilisateur final qui assure la séparation des canaux : le *splitter* (séparateur vocal), ou coupleur **POTS** (*Plain Old Telephon Service*, service téléphonique traditionnel) et le modem ADSL. Le *splitter* est généralement intégré au modem. Le modem offre un accès de type Ethernet, USB ou Wi-Fi. Du côté opérateur, le **DSLAM** (*Digital Subscriber Line Access Multiplex*) est un multiplexeur fréquentiel assurant la séparation des bandes de fréquences téléphoniques et de données, modem ADSL, il assure aussi l'interface entre les connexions utilisateurs et le réseau haut débit de l'opérateur (figure 13.47). Cependant, la connexion IP doit être prolongée jusque chez le fournisseur de service Internet (**FAI**), ce rôle est dévolu au **BAS** (*Broadband Access Server*), la figure 13.48 illustre l'architecture protocolaire d'un accès ADSL.

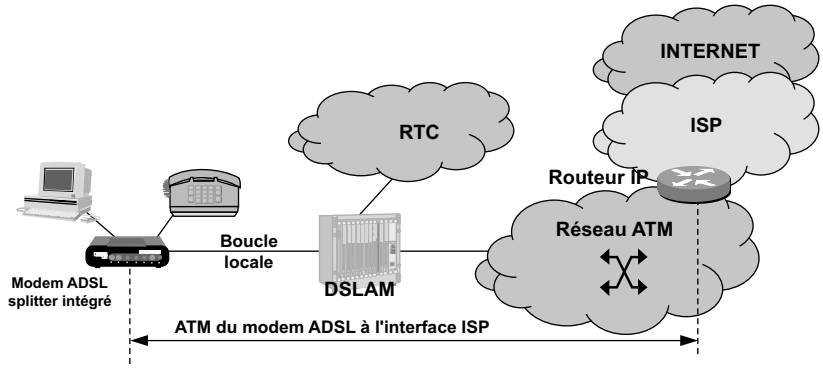


Figure 13.47 L'architecture d'un réseau ADSL.

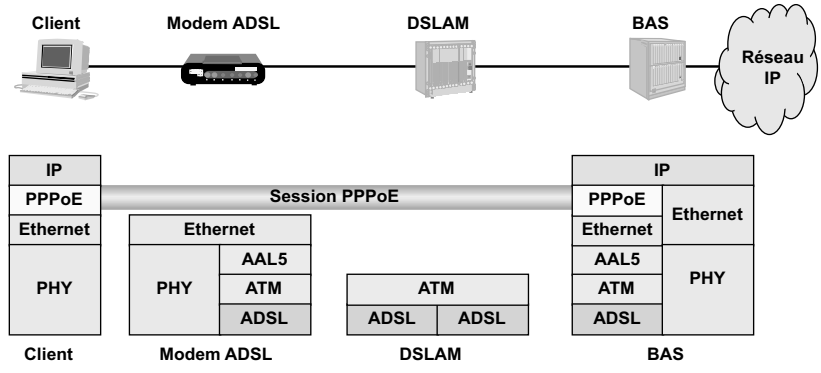


Figure 13.48 L'architecture protocolaire d'accès ADSL.

C'est le BAS qui réalise les fonctions d'authentification du client et l'acheminement des données vers les différents fournisseurs d'accès. Cette authentification est réalisée par le protocole PPP adapté à une interface Ethernet (**PPPoE**, *PPP over Ethernet*) ou à une interface USB (**PPPoA**, *PPP over ATM*). La figure 13.49 illustre l'acheminement des données lorsque le FAI a accès à la boucle locale.

© Dunod – La photocopie non autorisée est un délit

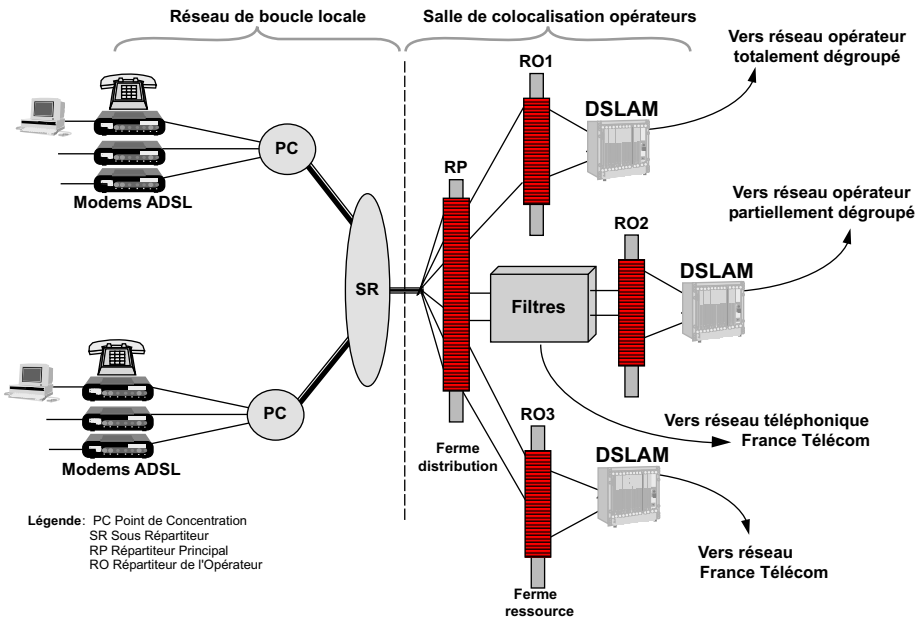


Figure 13.49 L'accès ADSL et le dégroupage de la boucle locale.

Compte tenu de l'intérêt économique des techniques DSL, d'autres solutions ont été développées pour raccorder à moindres frais les usagers aux réseaux des opérateurs. La figure 13.50 présente succinctement ces différentes versions.

Appellation	Débit descendant	Débit montant	Distance	Utilisation
ADSL	32 kbit/s à 8 Mbit/s	32 kbit/s à 1,1 Mbit/s	5,5 km	Accès professionnel à Internet Interconnexion de LAN Vidéo à la demande (VoD)
UADSL G.Lite	64 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	5,5 km	Accès résidentiel à Internet
SDSL	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	1,54 Mbit/s (T1) 2,048 Mbit/s (E1)	6,5 km	Interconnexion de LAN Serveur Internet Vidéoconférence
IDSL	144 kbit/s à 1,5 Mbit/s	32 kbit/s à 512 kbit/s	11 km	Accès RNIS
VDSL	13 à 52 Mbit/s	1,5 à 2,3 Mbit/s	1,2 km	Accès Internet, VoD TV haute définition
HDSL	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	1,5 Mbit/s (T1) 2,048 Mbit/s (E1)	4,5 km	Accès professionnel E1 Raccordement PABX Interconnexion de LAN

Figure 13.50 Les différentes technologies xDSL.

En utilisant une bande de fréquence étendue jusqu'à 2,2 MHz, l'ADSL2+ autorise un débit théorique pouvant atteindre, dans les conditions optimales (proximité du point de raccordement, diamètre de la paire cuivre, bruit faible et qualité des connecteurs), un débit descendant théorique

de 25 Mbit/s et un débit montant de 1 Mbit/s. En implémentant une technique de répartition des voies proche du TDMA (**CVoDSL**, *Channel Voice over DLS*) le débit montant peut être porté à 1,2 Mbit/s, mais l'accès téléphonique traditionnel simultané n'est alors plus permis.

En terme de services, l'ADLS standard à 8 Mbit/s autorise la diffusion de télévision 4/3 codée en MPG2 à un débit d'environ 3,5 Mbit/s, l'ADLS2+ autorisera avec une liaison à 16 Mbit/s la télévision 16/9HD codée en MPEG4 avec un débit de 10 Mbit/s. Cependant, en positionnant les équipements actifs au niveau des sous-répartiteurs et non plus au répartiteur principal, diminuant ainsi la distance abonné élément actif, le **VDSL** (*Very High Rate DSL*) devrait offrir des débits de l'ordre de 50 Mbit/s.

13.4.6 Les courants porteurs

Utilisée depuis longtemps par EDF pour faire transiter des commandes spécifiques au pilotage du réseau électrique, la technique des courants porteurs en ligne (**CPL**, ou *Power Line Carrier* **PLC**) consiste à superposer au courant électrique à 50 Hz un courant porteur (multiplexage fréquentiel) véhiculant tout type d'information. Devant le développement anarchique de nombreux systèmes à courant porteur (interphone, signaux de commandes divers...), la norme EN 50065-1 a délimité les espaces de fréquences utilisables :

– de 9 à 95 kHz, bande réservée aux fournisseurs d'énergie électrique ;

– de 95 à 125 kHz, bande libre ;

– de 125 à 140 kHz, bande libre mais réservée aux applications de type domotique ;

– de 140 à 148,5 kHz, bande libre.

Le pilotage d'appareillage électrique par la technique des courants porteurs est défini par la norme X.10. Celle-ci consiste à représenter les différentes commandes par des bits à 1 matérialisé par une rafale d'une milliseconde à 120 kHz et les bits à 0 par l'absence de signaux à 120 kHz. Cette technique est aujourd'hui largement dépassée, la norme HomePlug 1.0 permet la réalisation dans un site (*in-door*) de véritables réseaux locaux. Le débit offert est de 14 Mbit/s avec repli jusqu'à 1 Mbit/s, le protocole d'accès est du type **CSMA/CA** (*Carrier Send Multiple Access/Collision Avoidance*). HomePlug 1.0 distingue quatre classes de service, l'accès étant réalisé par des modems CPL branchés /CA directement sur une prise de courant 220 V et offrant une interface Ethernet ou USB.

En étendant cette technique hors du domicile (*out-door*) la technique des courants porteurs se présente comme une alternative à l'ADSL pour l'accès au réseau Internet. Utilisant une bande de fréquence de 4,3 à 20,9 MHz, cette technique autorise des débits de l'ordre du Mbit/s. La figure 13.51 décrit le principe d'un accès Internet *via* les courants porteurs.

L'adaptateur CPL (Modem et interface d'accès) est directement raccordé à une prise de courant traditionnelle. Le réseau électrique du domicile sert de support de transmission. Pour éviter que les courants porteurs ne soient très fortement altérés par les circuits du compteur électrique, une dérivation établit un lien direct entre le réseau interne et les câbles EDF. À l'extérieur du domicile les informations sont transportées sur les lignes de distribution de l'EDF jusqu'à un centre de transformation où le réseau fibre optique de l'EDF prend le relais et assure l'interconnexion avec Internet.

© Dunod – La photocopie non autorisée est un délit

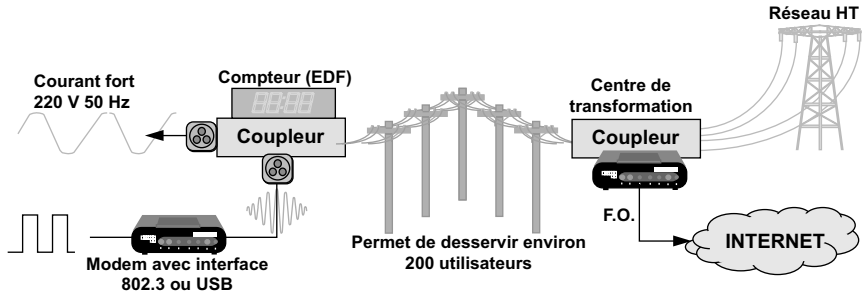


Figure 13.51 Principe de l'accès CPL.

13.5 CONCLUSION

L'évolution rapide des besoins, non seulement, en terme de débit mais essentiellement en terme de qualité de service, contraint les opérateurs de télécommunication a rechercher des techniques de plus en plus efficaces et en particulier à appuyer directement les protocoles utilisateur sur les réseaux WAN optiques en supprimant les protocoles intermédiaires traditionnels et à multiplier les techniques d'accès tant en terme de nombre de points d'accès que d'offre de débit et de diversité de techniques.

EXERCICES

Exercice 13.1 SDH/PDH

Quels sont les principaux avantages de la hiérarchie SDH vis-à-vis de la hiérarchie PDH ?

Exercice 13.2 Rendement protocolaire

Sur votre réseau, vous désirez accueillir des stations nomades. À des fins de sécurité absolue, vous avez décidé de développer un modem propriétaire. Sachant que la bande passante téléphonique pratique est plus grande que la bande passante théorique, vous comptez utiliser la bande de 200 à 3 800 Hz. Cependant, ces caractéristiques n'étant pas garanties en tout point du réseau téléphonique, vous décidez de développer votre modem sur le même modèle qu'ADSL. C'est-à-dire utiliser un ensemble de sous-porteuses, chacune transportant 128 symboles par seconde (1 symbole = 1 octet) et appelée tonalité.

Sachant que chaque tonalité occupera un spectre de fréquence de largeur 100 Hz et que, pour éviter les interférences, les spectres de chaque tonalité seront écartés de 20 Hz (bande de garde) :

1. Quelle est la largeur de bande occupée par une tonalité ?
2. Combien de tonalités pourront être utilisées simultanément ?
3. Dans cette hypothèse quel est le débit maximal du système ?

À l'instar d'ADSL, pour assurer l'adaptation à la ligne le système n'utilisera pas les tonalités dont le niveau sera atténué de 3 dB et plus par rapport à la tonalité la mieux transmise. Pour tester votre modem, vous relevez la bande passante de votre ligne test. Le résultat des mesures est donné par le tableau suivant (figure 13.52).

Tonalité	Niveau en mW	Tonalité	Niveau en mW
1	8	16	8
2	7	17	8
3	9	18	8
4	8	19	9
5	4	20	8
6	3	21	8
7	6	22	9
8	6	23	9
9	6	24	9
10	7	25	8
11	8	26	8
12	6	27	7
13	5	28	6
14	4	29	5
15	4	30	4

Figure 13.52 Bande passante (Puissance/Fréquence) de la ligne.

4. Quelle est la puissance de la tonalité la mieux reçue ?
5. Quelle est la puissance minimale des tonalités susceptibles d'être validées par le système ?
6. Dans ces conditions, quel est le nombre de tonalités qui seront validées par le système ?
7. Quel sera alors le débit binaire réel du modem ?

   Sachant que :

   – les messages sont issus d'une trame Ethernet remplie au maximum de sa capacité de transport (MTU d'Ethernet),
   – le protocole réseau est TCP/IP (aucune option n'est invoquée),
   – le transfert se fait en mode cellules ATM (nous supposerons que le datagramme IP est directement encapsulé dans la couche d'adaptation AAL5),
   – l'AAL5 fait du bourrage pour que les données soient segmentées en un nombre entier de cellules complètes et utilise 8 octets pour gérer le protocole.
8. Quel est le nombre minimal et maximal d'octets de bourrage que la couche AAL5 est susceptible d'introduire ?
9. Quel est le nombre de cellules ATM qui seront constituées ?
10. Complétez la figure 13.53 en remplaçant les X par la valeur en octets du champ.
11. Quel est le rendement du protocole (rapport entre le nombre de bits utiles et le nombre de bits transmis) ?
12. Quel est alors le taux de transfert d'information (bit/s) ?
13. En supposant un taux d'erreur de 10^{-6} quel est le taux de transfert d'information réel (bit/s) ?
14. Quel est le rendement global du système (TTI/Possibilité du modem)

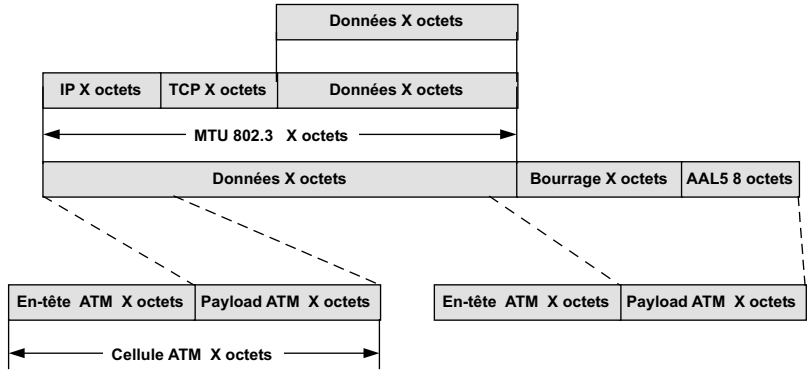


Figure 13.53 L'encapsulation de données dans ATM.

Chapitre **14**

Les protocoles de cœur de réseau

Le chapitre 13 a introduit les différents protocoles mis en œuvre dans les réseaux, ce chapitre se propose de les étudier en détail.

14.1 LE PROTOCOLE X.25[1]

14.1.1 Généralités

Rappelons que le protocole X.25 couvre les trois premières couches du modèle OSI (figure 14.1) :

- La couche physique, niveau bit ou X.25-1 définit l'interface ETTD/ETCD. Elle est conforme à l'avis X.21 et X.21 bis de l'UIT-T.
- La couche liaison, niveau trame ou X.25-2, met en œuvre un sous-ensemble d'HDLC appelé LAP-B (*High Level Data Link Control*, *Link Access Protocol Balanced*).
- La couche réseau, niveau paquet ou X.25-3, gère les circuits virtuels (permanents ou commutés).

14.1.2 Le niveau X.25-1

La recommandation X.25 spécifie que l'accès au réseau X.25 doit être conforme à l'une des recommandations X.21 (transmission numérique), X.21 bis (transmission analogique) ou X.31 (accès *via* le réseau RNIS). L'avis X.21 définit l'interface d'accès entre un ETTD et un réseau public de transmission de données (figure 14.2), il fixe les règles d'échange pour :

- L'établissement de la connexion avec un ETTD distant à travers un ou plusieurs réseaux.

1. Nous avons pris le parti de maintenir une étude détaillée de X.25. En effet, le protocole X.25 est l'archétype des protocoles réseau, il permet d'expliquer simplement tous les mécanismes. Conçu dans les années 1980, X.25 reste et restera longtemps encore un protocole très utilisé. Il est aux protocoles de télécommunications ce que Cobol est aux langages de programmation.

– L'échange des données en mode duplex intégral.
– La libération de la connexion.

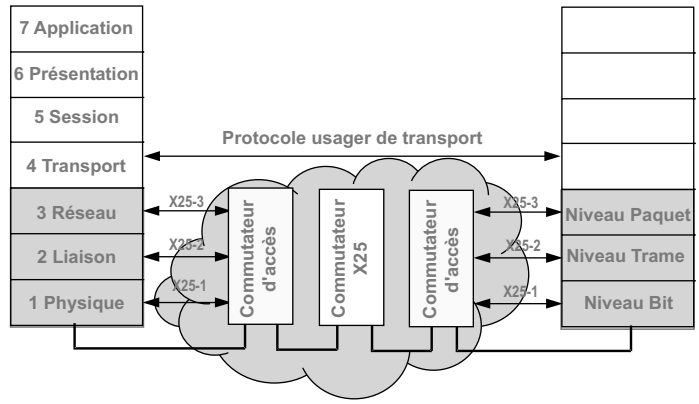


Figure 14.1 Architecture du protocole X.25.

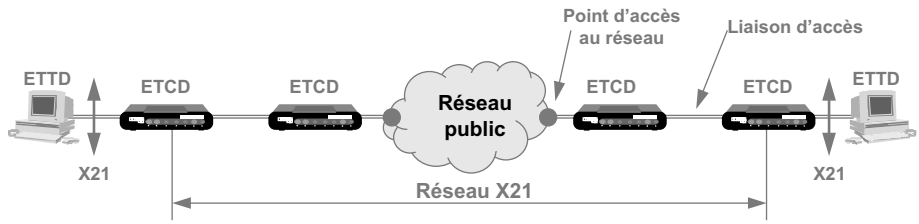


Figure 14.2 Le réseau X.21.

Ces interfaces ont été étudiées au chapitre 3, le lecteur pourra s'y reporter.

14.1.3 Le niveau X.25-2

Généralités[2]

Le niveau 2 du modèle OSI, ou couche liaison, garantit un transfert fiable de données sur une liaison physique non fiable (perturbations électromagnétiques). Au niveau trame, X.25-2 met en œuvre le protocole HDLC version LAP-B (*Link Access Protocol Balanced*). LAP-B est un protocole point à point en duplex intégral (*full duplex*), dans lequel les deux stations communicantes ont une responsabilité égale vis-à-vis de la liaison : chacune des extrémités peut émettre une commande. L'une des stations est l'ETTD (DTE), l'autre le nœud de rattachement au réseau ou ETCD (DCE) (en X.25, le réseau ou son point d'accès est assimilé au DCE). La figure 14.3 schématise le principe d'une liaison équilibrée.

L'accès au réseau peut utiliser un seul lien physique (**SLP**, *Simple Link Protocol*) ou, pour accroître le débit, une agrégation de plusieurs liens (**MLP**, *Multi Link Protocol*). L'utilisation de

2. Le protocole HDLC est étudié en détail au chapitre 4, *Notions de protocole*.

MLP est transparente pour le niveau réseau. L'évolution des débits physiques réalisables sur un seul lien a rendu obsolète l'utilisation du protocole MLP.

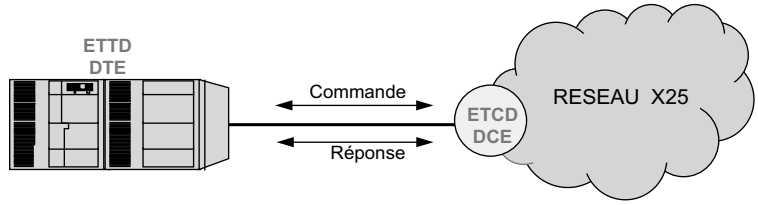


Figure 14.3 La liaison point à point en LAP-B.

HDLC LAP-B versus SLP

Le protocole HDLC LAP-B, étudié chapitre 4, utilise deux modes de fonctionnement : le fonctionnement normal (numérotation des trames sur 3 bits, modulo 8) et le mode étendu (numérotation des trames sur 7 bits, modulo 128). La structure générale de la trame HDLC est rappelée figure 14.4.

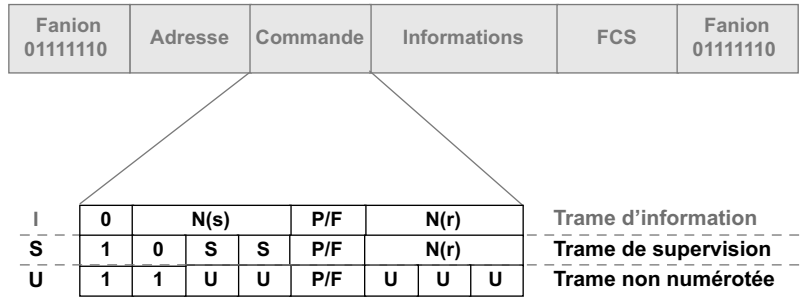


Figure 14.4 Rappel sur la structure de la trame HDLC.

HDLC utilise trois types de trames :

- Les trames d'information (**I**) contiennent un champ de données. Les champs $N_{(s)}$ et $N_{(r)}$ correspondent, pour chaque extrémité de la liaison, aux compteurs de trames d'information émises $V_{(s)}$ et reçues $V_{(r)}$.
- Les trames de supervision (**S**) permettent de contrôler l'échange de données. Le champ $N_{(r)}$ identifie la trame acceptée ou refusée ($N_{(r)} - 1$), il correspond au $N_{(s)}$ de la prochaine trame attendue.
- Les trames non numérotées (**U**, *unnumbered*) gèrent la liaison (établissement, libération...). Elles ne comportent aucun compteur (non numérotées).

Le contrôle et la reprise sur erreur sont réalisés entre chaque nœud du réseau, LAP-B est un protocole en point à point. Notons que pour se prémunir contre la perte d'un fanion, le calcul du FCS (*Frame Check Sequence*) diffère un peu. Le FCS est le complément à 1 de la division polynomiale du contenu de la trame par le polynôme générateur $G_{(x)} = x^{16}+x^{12}+x^5+1$ (avis V.41 de l'UIT-T). En émission, le registre de calcul du FCS est initialisé à 1. Sans erreur de transmission,

© Dunod – La photocopie non autorisée est un délit

ce mode de calcul donne comme résultat un reste qui est toujours égal à « 0001110100001111 » quel que soit le contenu de la trame. Ce nombre est dit **nombre magique**.

Pour ouvrir une connexion (figure 14.5), l'ETCD ou ETTD appelant émet une trame non-numérotée (trame U) SABM (ouverture en mode normal) ou SABME (ouverture en mode étendu). L'appelé l'acquitte avec la trame non numérotée UA. Sans réponse de l'appelé, l'appelant à échéance d'un *timer* (**T1**) renouvelle sa demande. Il abandonne la demande d'établissement après **N2** tentatives infructueuses, en principe le compteur N2 est initialisé à 10, il est décrémenté de 1 à chaque tentative.

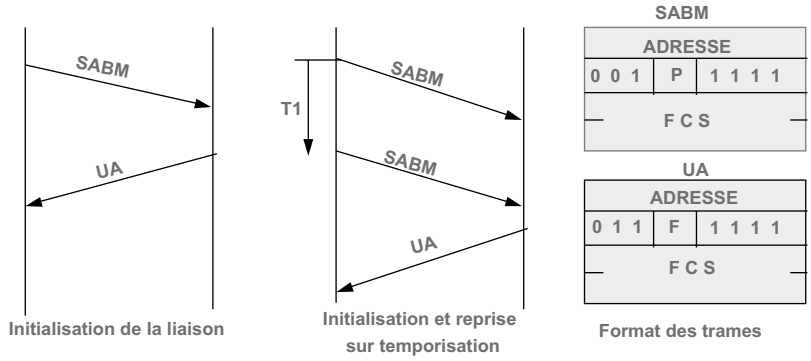


Figure 14.5 L'ouverture de connexion.

Lorsque la connexion est acceptée, l'appelant et l'appelé peuvent procéder à l'échange d'information (trames I), cet échange est contrôlé par des trames de supervision (trames S). Les trames d'information ($N_{(s)}$) sont numérotées modulo 8 (mode de base) ou modulo 128 (mode étendu).

L'accusé de réception (figure 14.6) peut être explicite, il est alors réalisé par une trame RR, ou implicite, ce sont alors les trames d'information du correspondant distant (échange *full duplex*) qui effectuent l'acquittement.

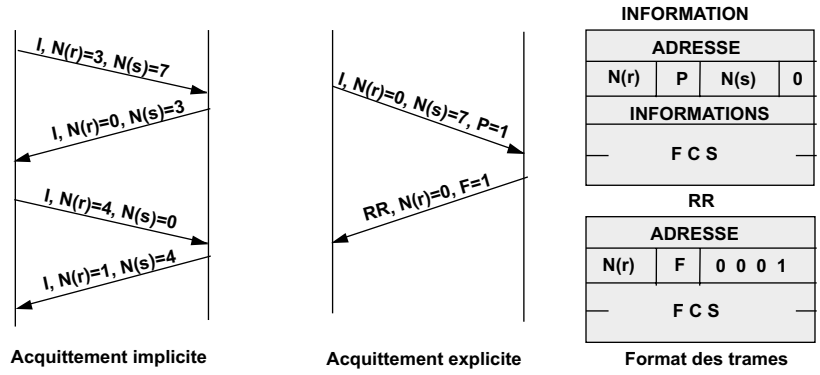


Figure 14.6 Le transfert de données.

Les trames S, RR, REJ et RNR supervisent l'échange. La trame RR sert à l'acquittement, la trame REJ indique la trame rejetée (trame erronée ou numéro de séquence invalide) et demande de

reprendre la transmission depuis la trame erronée (compteur $N_{(r)}$). La trame SREJ (rejet sélectif) ne demande la retransmission que de la trame rejetée. La trame RNR acquitte la trame $N_{(r)}-1$ et demande à l'émetteur d'arrêter provisoirement son émission, c'est le mécanisme du contrôle de flux (état bloqué ou occupé), les émissions ne reprendront qu'à réception d'une trame RR ou REJ (figure 14.7).

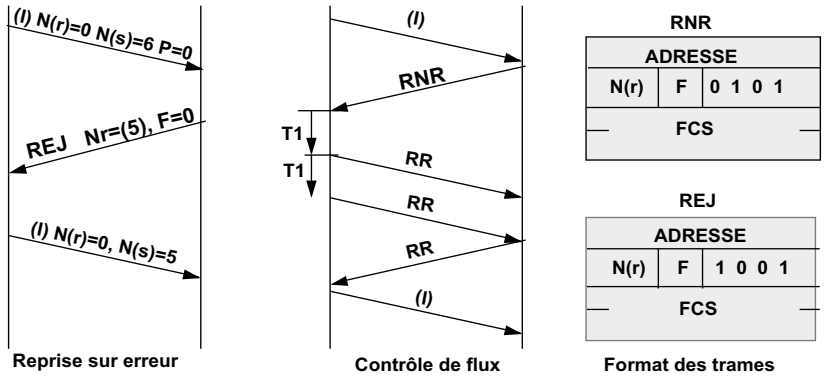


Figure 14.7 La reprise sur erreurs et contrôle de flux.

La déconnexion est demandée par l'ETTD ou ETCD par la trame DISC ; à réception d'une demande de déconnexion, le destinataire acquitte celle-ci (UA) et se déconnecte. L'émetteur de la demande de déconnexion n'exécute la procédure de déconnexion qu'après avoir reçu l'acquittement de sa demande.

La procédure de déconnexion est représentée figure 14.8. Le réseau (ETCD) peut signaler un incident de ligne (modem coupé par exemple) par l'émission de trames DM. Après **N2** retransmissions, il passe à l'état déconnecté.

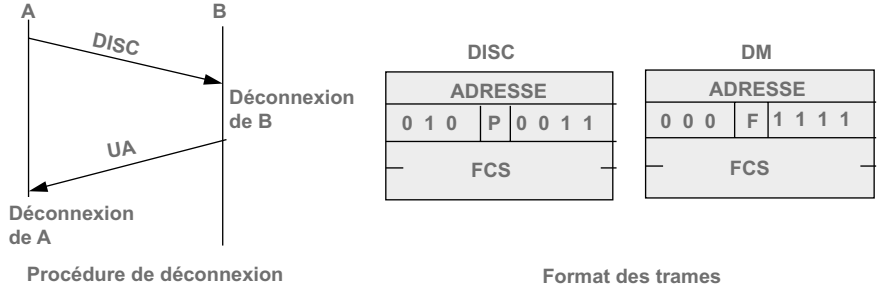


Figure 14.8 La rupture de la liaison.

Lorsque les erreurs ne peuvent être corrigées par une simple retransmission de la ou des trames litigieuses (nombre de retransmissions supérieur à N2, $N_{(r)}$ incorrect : valeur supérieure au nombre de trames réelles...), l'ETCD ou ETTD peut effectuer une déconnexion (DISC) ou réinitialiser la liaison (SABM). Certaines erreurs peuvent être signalées avant la réinitialisation de la liaison par la trame FRMR (figure 14.9). Les variables d'états $V_{(s)}$ et $V_{(r)}$ indiquent alors au destinataire l'état des compteurs de son correspondant. Le bit C/R à 1 indique que la trame rejetée est une trame de réponse, et à 0 que la trame rejetée est une trame de commande.

© Dunod – La photocopie non autorisée est un délit



Codage des bits Z	Y	X	W	Signification
0	0	0	1	Le champ commande de la trame reçue est incorrect
0	0	1	1	La longueur du champ information est incorrecte
1	0	0	0	La valeur de $N_{(r)}$ est incorrecte
0	1	0	0	La taille du champ d'information est excessive

Figure 14.9 La trame d'indication d'erreurs FRMR.

Le niveau X.25-3

➤ Généralités

La recommandation X.25-3 (**X.25 PLP**, *Packet Level Protocol*) gère l'établissement, le maintien et la libération des circuits virtuels (**CVC**, Circuit virtuel commuté ou **SVC**, *Switched Virtual Circuit*). Le protocole X.25-3 assure le transfert de données (acheminement), le séquencement[3], la détection des pertes, le contrôle de flux, la fragmentation et le réassemblage des paquets. Il résout les problèmes d'adressage et de multiplexage des connexions virtuelles sur la même liaison d'abonné.

La procédure d'établissement des CVC établit une relation entre un numéro de voie entrante et un numéro de voie sortante. Cette relation correspond à un lien virtuel entre les entités connectées (connexion virtuelle) similaire à la constitution d'un circuit en commutation de circuits. Le mode de mise en relation est dit orienté connexion. Ce procédé (figure 14.10) identifie une liaison logique, il autorise le multiplexage de connexions sur une même voie physique et, pour adresser les correspondants, l'utilisation d'un adressage abrégé : le numéro de voie logique (**NVL**).

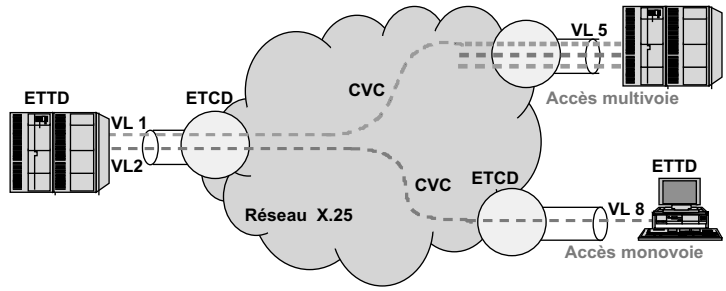


Figure 14.10 La mise en relation d'abonnés.

3. Les compteurs X.25-2 et X.25-3 diffèrent. En effet, X.25-3 décompte les données par circuit virtuel alors que le niveau 2 multiplexe sur la même connexion de liaison l'ensemble des circuits virtuels de l'entité de niveau 3.

➤ Format des unités de données

Les paquets X.25-3 comportent les informations relatives à l'adressage : le numéro de voie logique (adressage de convention), des informations de contrôle et éventuellement des données. Les paquets sont transmis à la couche trame qui les encapsule (figure 14.11).

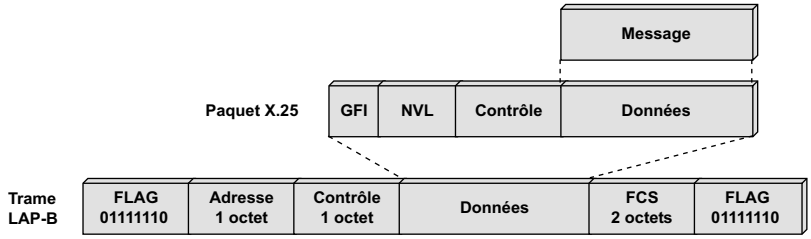


Figure 14.11 L'encapsulation des paquets X.25 dans les trames LAP-B.

Un paquet X.25, illustré figure 14.12, comporte au moins 3 octets. Le premier champ de 4 bits, dit champ **GFI** (*General Format Identifier*) définit certains paramètres de l'échange. Le premier bit a deux significations. Dans les paquets de données, il est dit bit **Q** (*Qualified*), dans les paquets d'établissement, bit **A** (*Address*). Le bit Q (bit à 1) est, par exemple, utilisé pour indiquer aux concentrateurs gérant les accès asynchrones (**PAD**, *Packet Assembler Disassembler*) que le paquet reçu est une commande à leur intention et non un paquet de données à transmettre à un ETTD caractère distant. Le bit A, dans un paquet d'établissement (ou d'appel) identifie le format du champ Adresse, à 0 il indique qu'une adresse est au format X.121 (valeur par défaut), à 1 il précise que le format de l'adresse est indiqué dans le champ adresse. Le bit **D** (*Delivery*) détermine la portée des acquittements. Si le bit D est à 1, l'acquittement a une signification de bout en bout, sinon il est local. La recommandation X.25, antérieure au modèle OSI, n'est, sur ce point pas conforme aux spécifications du modèle de référence qui ne prévoit un acquittement de bout en bout qu'au niveau de la couche transport, en principe ce bit est toujours à 0. Les deux bits suivants indiquent la taille des compteurs (01, modulo 8 ; 10, modulo 128).

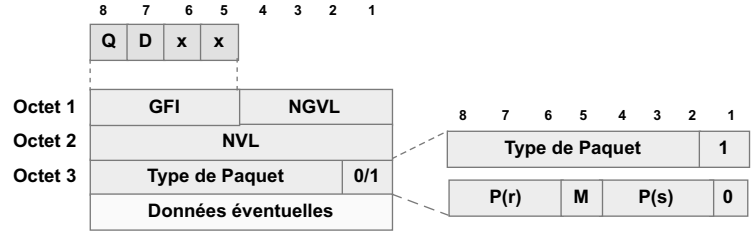


Figure 14.12 Le format des paquets X.25.

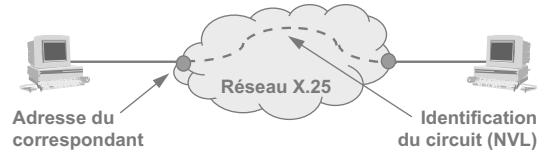
Le champ suivant identifie la voie logique (étiquette) : le **NVL** ou numéro de voie logique (**LCN**, *Logical Channel Number*) sur 12 bits (4 096 voies logiques identifiables) n'a qu'une signification locale. Le NVL est composé de deux champs, les quatre premiers bits de l'octet 1 identifient le groupe de voies logiques (**NGVL** ou **LGN**, *Logical Group Number*) auquel appartient la voie logique (octet 2).

© Dunod – La photocopie non autorisée est un délit

Enfin, le dernier champ de l'en-tête est similaire au champ Commande d'HDLC. Le premier bit différencie un paquet de données (bit à 0) des autres types de paquets (bit à 1). Dans les paquets de données, les champs $P_{(r)}$ et $P_{(s)}$ (sur 3 bits en mode normal) permettent de contrôler le séquencement des paquets. Ces compteurs ne font pas double usage avec ceux du niveau trame. En effet, une connexion de niveau 2 peut multiplexer plusieurs connexions de niveau 3. Enfin, le bit **M** (*More data*) est utilisé lorsque le paquet transmis a subi une fragmentation. M = 1 signifie que les paquets qui suivent appartiennent au même bloc de données. M = 0 identifie le dernier paquet ou un paquet non fragmenté.

➤ Gestion des circuits virtuels

Les réseaux X.25 autorisent les deux types de circuits virtuels (figure 14.13), les circuits virtuels commutés (CVC ou SVC) et les circuits virtuels permanents (CVP ou PVC, *Permanent Virtual Circuit*).



	Circuit Virtuel Commuté	Circuit Virtuel Permanent
Etablissement du circuit	A chaque appel	A l'abonnement
Potentialité de communication	Possibilité de mise en relation avec tout abonné	Liaison point à point
Temps d'établissement	Peut être long (1s)	Sans (Liaison permanente)

Figure 14.13 Les différences entre un CVC et un CVP.

Le circuit virtuel permanent est établi par l'opérateur à la configuration du raccordement de l'abonné. À l'inverse, le circuit virtuel commuté est construit appel par appel. Les identifiants de voie (NVL) sont attribués dynamiquement par chaque nœud (terminal utilisateur ou nœud du réseau). Le numéro affecté est choisi parmi ceux disponibles qui sont gérés par une table interne au nœud. Ce procédé peut conduire à une collision d'appels, c'est-à-dire à une affectation simultanée d'un même NVL à un appel sortant et à un appel entrant. En cas de collision d'appels, l'ETTD ignore l'appel entrant, l'ETCD (le réseau) traite l'appel en provenance de l'ETTD local et entame une procédure de déconnexion pour l'appel de l'ETTD distant (figure 14.14).

Pour minimiser le risque de collision d'appels, les appels sortants de l'ETTD sont émis sur la voie logique de numéro le plus élevé. Le réseau transmet les appels entrants sur le numéro de voie logique disponible le plus faible. À l'instar de la téléphonie, il est aussi possible de spécialiser les voies logiques : voies logiques spécialisées arrivée ou départ. Une voie qui accepte indifféremment les appels entrants ou sortants est dite **mixte**. L'affectation des NVL s'effectue comme le montre le diagramme de la figure 14.14. Les premiers numéros de voies logiques sont réservés aux circuits virtuels permanents. La voie logique 0 est en principe réservée à l'opérateur pour la signalisation d'incidents.

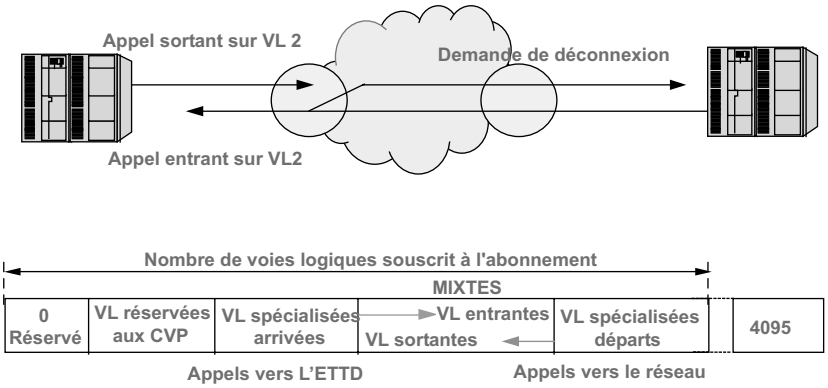


Figure 14.14 La gestion des numéros de voies logiques.

➤ Adressage des ETTD distants

Durant la procédure d'établissement et de la libération du CV, les ETTD sont identifiés par leur numéro réseau (adresse d'abonné). Les champs Adresse des paquets d'établissement sont codés en Décimal Codé Binaire (**DCB**) sur un quartet. Un champ Longueur d'adresse précède celle-ci. La recommandation X.25 admet deux types d'adresse. Implicitement, l'adressage est conforme à la recommandation X.121.

➤ Facilités ou services complémentaires

Les paramètres de la connexion réseau sont généralement fixés au moment du raccordement (abonnement), cependant certains peuvent être négociés ou renégociés appel par appel. Les facilités ou services complémentaires sont invoqués dans le paquet d'appel (ou paquet d'établissement). Le champ option est codé : code option et paramètres de l'option. Le tableau de la figure 14.15 fournit quelques exemples d'options.

Option	Code option	Codage	Description
Groupe fermé d'abonnés	0x03	DCB, 1 chiffre par quartet	Le GFA permet de constituer un réseau privé dans le réseau public. Seuls peuvent communiquer les hôtes appartenant au même GFA.
Taxation au demandé	0x01	0x01 (taxation demandée)	Elle permet de centraliser la facturation sur un même site (réduction quantitative).
Sélection rapide	0x01	0x80	Elle permet de joindre à un paquet d'appel jusqu'à 128 octets de données (même code que la taxation au demandé).
Classe de débit	0x02	1er quartet vers DTE 2e quartet du DTE Ex. de valeurs : 3 75 bit/s 7 1 200 bit/s B 19 200 bit/s C 48 000 bit/s D 64 000 bit/s	Elle est utilisée pour adapter le débit de l'hôte aux capacités de réception du destinataire sans avoir besoin de recourir au contrôle de flux.

Figure 14.15 Exemples d'options X.25.

© Dunod – La photocopie non autorisée est un délit

Option	Code option	Codage	Description
Taille des paquets	0x42	Taille en émission sur 1 octet Taille en réception sur 1 octet Exprimée en puissance de 2 de la taille. Ex. : 128 codée 7	Selon les ETCD, la taille en émission et en réception peut être différente.
Taille des fenêtres	0x43	Taille en émission 1 octet Taille en réception 1 octet	Selon les ETCD.

Figure 14.15 Exemples d'options X.25. (suite)

➤ Établissement et libération des circuits virtuels

L'ETTD qui prend l'initiative d'établir une connexion émet une demande d'appel (paquet d'appel). Le paquet d'appel sortant est émis sur la première voie logique disponible, il contient toutes les informations nécessaires à l'établissement du CV (figure 14.16), c'est-à-dire :

– L'étiquette affectée (**NVL**, Numéro de voie logique).
– L'adresse complète.
– Si des facilités sont demandées, la liste des facilités invoquées est précédée de la longueur totale du champ Facilités, sinon l'octet longueur du champ Facilités est à zéro.
– Enfin, si la facilité **sélection rapide** a été demandée, suivent des données utilisateur sur 16 octets ou 128.

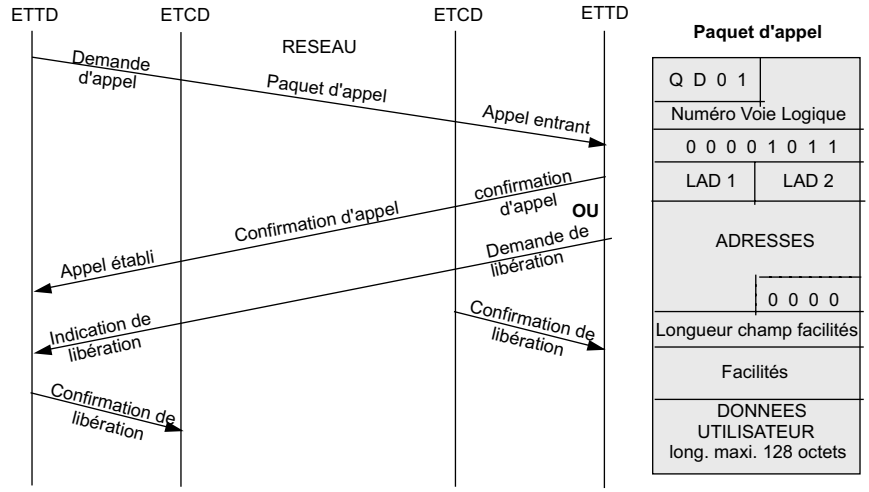


Figure 14.16 Diagramme d'établissement d'appel.
(LAD1 Longueur adresse appelant, LAD2 Longueur adresse appelé.)

L'appelé peut accepter (paquet de confirmation d'appel, figure 14.16) ou refuser l'appel (paquet de libération). Un paquet de confirmation de libération confirme à l'ETTD ou ETCD que le CV a bien été libéré. La libération d'un circuit virtuel peut être provoquée par le réseau suite à un refus d'appel (appelé occupé, refus de la taxation au demandé, GFA non accepté...) ou à un incident

interne au réseau. L'ETTD qui désire mettre fin à un échange (fin de connexion) émet un paquet de demande de libération (figure 14.17).

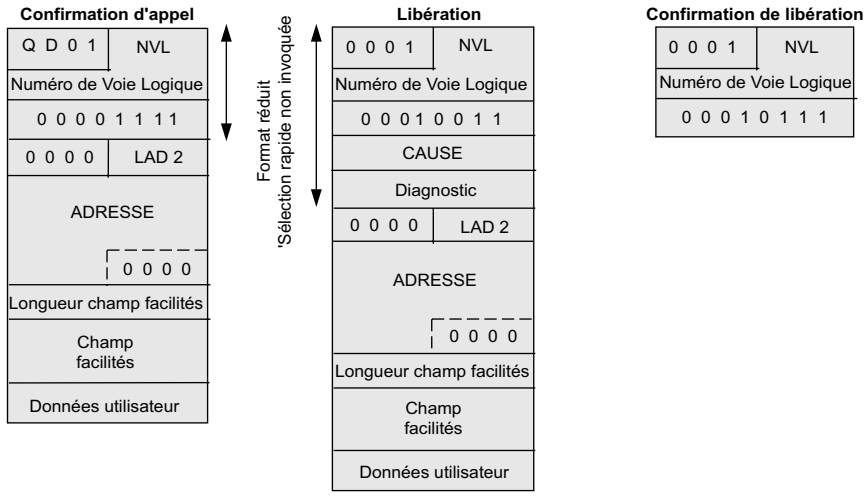


Figure 14.17 Le format des paquets de confirmation et libération.

➤ Échange de données

Chaque circuit virtuel établi peut supporter un transfert de données bidirectionnel limité, en débit, par le paramètre **classe de débit**. La figure 14.18 illustre les paquets utilisés lors d'un échange de données.



Figure 14.18 Format des paquets de données, d'acquittement et de contrôle de flux.

La taille du champ de données est définie à l'abonnement ou par l'opérateur, cette taille est fixée par la norme X.25 à 16, 32, 64, 128, 256, 512, 1024, 2 048 ou 4 096 octets. L'échange de données s'effectue selon un mécanisme similaire à celui étudié pour HDLC. Les compteurs $P_{(s)}$ et $P_{(r)}$ des paquets de données permettent de vérifier le séquencement des paquets (perte éventuelle d'un paquet) et d'acquitter ceux-ci ($P_{(r)}$, numéro du paquet attendu). Les paquets **RR** (*Receive Ready*) et **RNR** (*Receive Not Ready*), (figure 14.18) assurent l'acquittement et le contrôle de flux.

➤ Gestion des incidents

Lorsque le réseau, ou l'un des ETTD, détecte une désynchronisation des échanges (numéros $P_{(s)}$, et $P_{(r)}$), il demande une réinitialisation des compteurs par l'émission d'un paquet de demande de réinitialisation. Les données en cours de transfert sont abandonnées, les compteurs sont remis à zéro.

© Dunod – La photocopie non autorisée est un délit

La demande de réinitialisation ne concerne que le CV sur lequel elle a été émise. Le mécanisme de la réinitialisation est illustré par la figure 14.19.

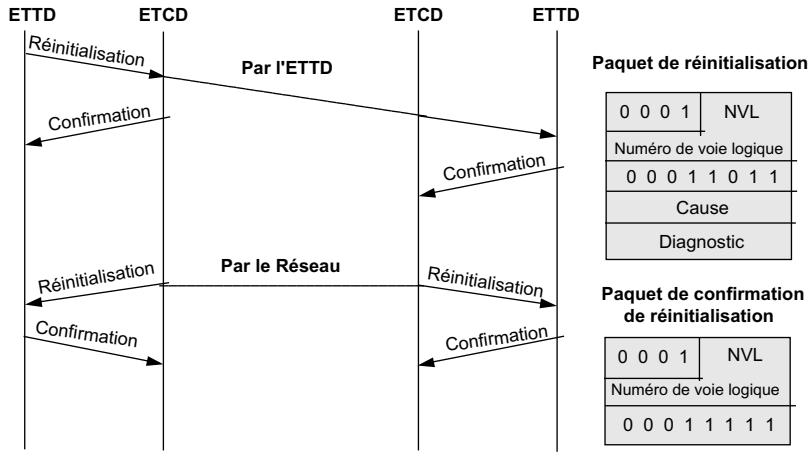


Figure 14.19 Le mécanisme de la réinitialisation.

Le mécanisme de reprise ou de redémarrage est déclenché suite à un incident grave sur le réseau (rupture de la liaison physique...). Il affecte tous les circuits virtuels commutés en cours et les circuits virtuels permanents. Les CVC établis sont libérés, les CVP actifs sont remis à l'état initial. Le mécanisme de la reprise est représenté figure 14.20.

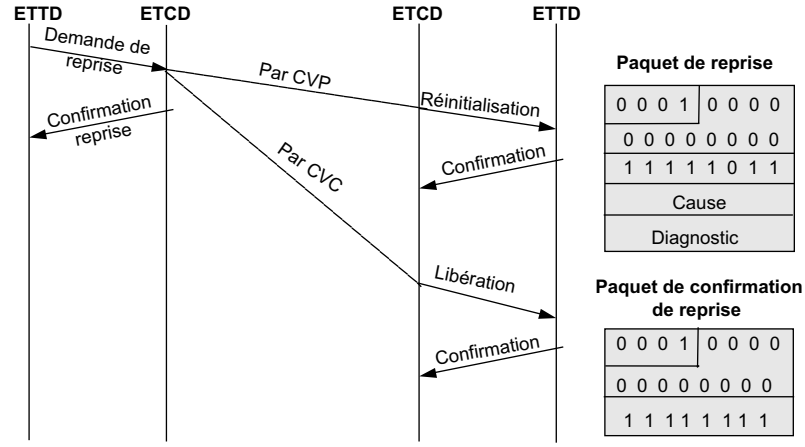


Figure 14.20 Le mécanisme de la reprise.

Les paquets de demande de reprise et d'indication de reprise sont émis sur la voie logique 0. Le champ Cause indique la raison de la reprise, le champ Diagnostic complète cette information. Le tableau de la figure 14.21 fournit quelques exemples de codage des champs Cause et Diagnostic des paquets de reprise et de diagnostic

Attention : la réinitialisation ne concerne que le CV sur lequel elle a été émise. La reprise est émise sur le CV 0, elle concerne tous les CV, y compris les CVP.

Cause	Signification	Diag	Signification
Reprise		24	Numéro de VL inexistant
01	Erreur de procédure locale	26	Paquet trop court
07	Fin d'incident	27	Paquet trop long
Réinitialisation		28	Erreur de codage du champ GFI
00	Par l'abonné distant	52	Longueur non multiple de 8
01	Dérangement de l'abonné distant	97	Modem abonné hors tension
03	Erreur de procédure locale	A1	Bit F reçu à tort
07	Incident dans le réseau	A4	Non-réponse à N2
09	Fin de dérangement	A9	Trop d'erreur de ligne

Figure 14.21 Les exemples de cause et de diagnostic d'erreur.

➤ Accès des terminaux asynchrones aux réseaux X.25

La norme X.25 définit un protocole pour l'accès en mode paquet de terminaux synchrones (**ETTD-P).** Les terminaux asynchrones (ou terminaux en mode caractères : **ETTD-C** : Minitel, terminal TTY, VT100...) nécessitent une adaptation pour converser à travers un réseau en mode paquet. Un concentrateur d'accès ou **PAD** (*Packet Assembler Disassembler*) assure, dans le sens terminal vers serveur, la conversion du mode caractère en mode paquet et inversement, dans le sens réseau vers terminal. Les recommandations X.28, X.29, X.3 régissent ce type d'accès, X.28 définit le dialogue en mode caractère entre le terminal et le PAD, X.3 précise le fonctionnement du PAD et X.29 décrit le dialogue de commande entre l'ETTD-P et le PAD, cette organisation est symbolisée par la figure 14.22.

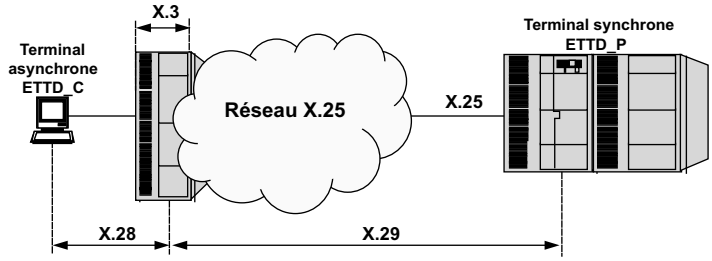


Figure 14.22 L'accès des ETTD-C aux réseaux X.25.

Les fonctions du PAD (X.3)

La fonction PAD a pour objectif essentiel d'encapsuler les données issues du terminal asynchrone dans un paquet X.25 et de désencapsuler les données à destination de ce terminal. L'avis X.3 précise les modalités essentielles de cette fonction :

– Il définit le nombre de caractères que le PAD devra avoir reçus avant d'émettre un paquet sur le réseau.
– Il précise les caractères de commande qui déclenchent l'émission d'un paquet même incomplet (retour chariot RC, BREAK...).
– Il détermine le temps maximum d'attente entre deux caractères avant d'envoyer un paquet (émission sur temporisation).

© Dunod – La photocopie non autorisée est un délit

D'autres fonctions relatives à la transmission ou à la gestion du terminal peuvent être remplies. Ce sont notamment :

– L'écho local ; sur un terminal asynchrone, l'affichage du caractère sur l'écran n'est pas celui introduit au clavier mais celui renvoyé en écho par l'ETTD distant (fonction de correction d'erreur par l'opérateur). Pour éviter un trafic inutile sur le réseau, l'écho du caractère introduit peut-être généré par le PAD (écho local). La fonction d'écho peut être annulée lors de l'introduction d'un mot de passe (frappe en aveugle).
– Le pliage de ligne ; c'est un paramètre qui permet d'adapter la longueur des messages reçus aux possibilités d'affichage du terminal (nombre de caractères/ligne), le PAD introduit les caractères CR/LF après *n* caractères.
– Le contrôle de flux par emploi d'une procédure de type XON, XOFF.

➤ Accès aux réseaux X.25

Généralités

Toutes les applications ne nécessitent pas un accès permanent au réseau, de ce fait, une liaison permanente peut s'avérer coûteuse compte tenu de son taux d'utilisation. C'est pour ces raisons qu'ont été définis des accès temporaires *via* le réseau téléphonique. La diversité des modes d'accès constitue l'un des facteurs de pérennité du protocole X.25.

X.25 distingue 2 types d'accès : les accès permanents ou accès directs établis *via* une liaison spécialisée ou le canal D de RNIS et les accès commutés ou accès indirects qui transitent *via* le RTC ou RNIS (canal B). La figure 14.23 illustre ces deux types d'accès.

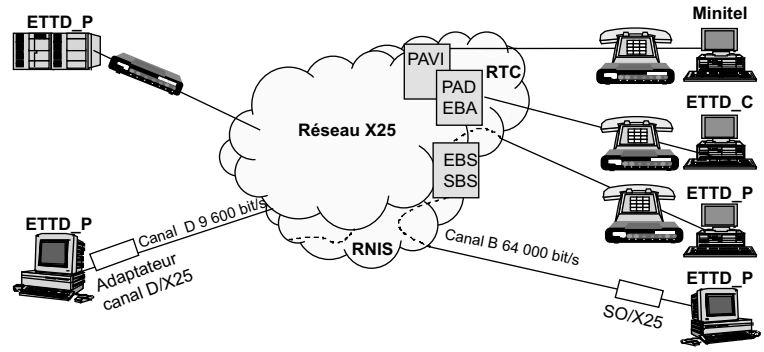


Figure 14.23 Les accès au réseau X.25.

Les accès directs

La liaison spécialisée constitue l'accès normal au réseau X.25. Un lien dépendant du débit de l'abonnement est établi de manière permanente entre le commutateur de rattachement de l'abonné et ce dernier. Ce type de raccordement est mal adapté à un besoin de connexion permanente avec un faible échange de données (taux de connexion important, taux d'activité faible). Le canal D des réseaux RNIS offre un accès permanent à 9 600 bit/s mieux adapté à ce cas de figure.

Les accès indirects

Les accès indirects (mode paquet ou caractère) transitent par un réseau intermédiaire (RTC ou RNIS) et convergent vers un point d'accès ou porte spécialisée selon le type d'accès (PAD, PAVI, EBS...). Un service d'identifiant peut être souscrit à l'abonnement. Les accès indirects sont essentiellement utilisés pour :

– des consultations de faible ou moyenne durée (Minitel ou autre) ;
– des transferts de petits fichiers ;
– des raccordements de secours pour des accès directs.

14.2 LE RELAIS DE TRAME OU FRAME RELAY

14.2.1 Généralités

Le relais de trames offre un service réseau en mode connecté conforme à l'avis Q.922 de l'UIT-T. La signalisation est du type canal sémaphore conforme à l'avis Q.933 (évolution de l'avis Q.931). Le relais de trame établit entre les équipements d'extrémité (**FRAD**, *Frame Relais Access Device*) un service de liaison virtuelle (figure 14.24). La liaison virtuelle peut être du type permanent (PVC, *Permanent Virtual Circuit*) ou temporaire et établi à la demande (SVC, *Switched Virtual Circuit*).

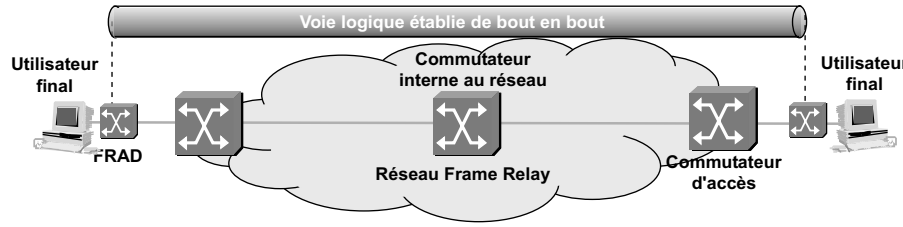


Figure 14.24 La liaison virtuelle du relais de trames.

Le relais de trames couvre les couches 1 et 2 du modèle OSI (figure 14.25), mais n'est pas conforme à ce dernier (modèle en plan de l'UIT). La couche physique assure l'adaptation au support physique.

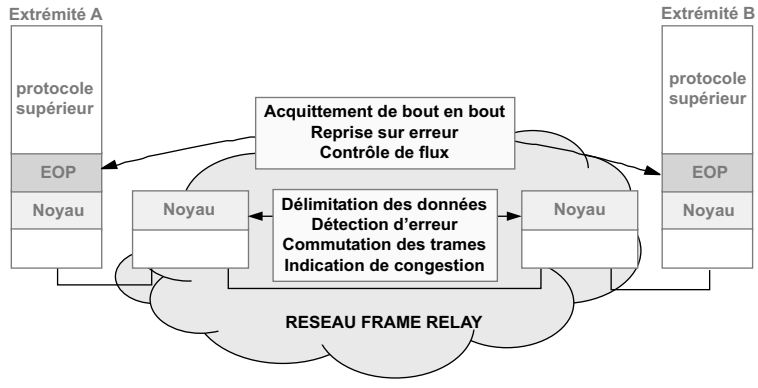


Figure 14.25 L'architecture du relais de trames.

© Dunod – La photocopie non autorisée est un délit

La couche 2 est subdivisée en deux sous-couches : le noyau (*Core*) et une sous-couche (**EOP**, *Element of Procedure*) complémentaire et facultative. Non normalisées, ses fonctionnalités sont laissées à la discrétion de l'utilisateur. Cette sous-couche 2 supérieure peut, par exemple, être HDLC LAP-B.

14.2.2 Le format de l'unité de données

Le relais de trames utilise une trame de type HDLC (*High Level Data Link Control*) dérivée du LAP-D, délimitée par deux fanions (0x7E, 01111110B), elle comporte un champ Adresse de taille variable de 2 à 4 octets, un champ Données et un champ de contrôle d'erreur (FCS). Le champ Contrôle (commande) d'HDLC est absent, il est inutile puisqu'il n'existe qu'un seul type de trame (signalisation par canal sémaphore). La figure 14.26 représente la trame Frame Relay.

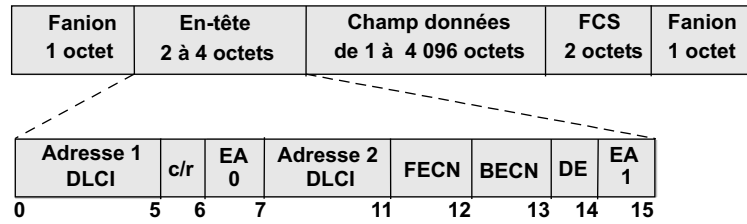


Figure 14.26 La trame Frame Relay.

L'identification de la voie virtuelle est réalisée par le champ Adresse (**DLCI**, *Data Link Connection Identifier*). Dans la version de base, il est composé d'un premier bloc de 6 bits et d'un second de 4 bits. Le champ **EA** (*End Address*) indique si le champ Adresse a une suite (EA = 0) ou s'il est le dernier (EA = 1).

Le champ **C/R** (*Commande/Response*) a la même signification que le bit P/F (*Poll/Final*) d'HDLC. Les bits **FECN** (*Forward Explicit Congestion Notification*) et **BECN** (*Backward Explicit Congestion Notification*) sont utilisés pour signaler aux organes d'extrémité l'état de congestion d'un des éléments du réseau. Le bit **DE** (*Discard Eligibility*) est positionné par les organes d'accès (**FRAD**, *Frame Relay Access Device*), il indique les trames à éliminer en priorité lors d'une congestion. Le FRAD est l'équipement d'interface entre le réseau de l'utilisateur et le réseau *Frame Relay*.

14.2.3 Les mécanismes élémentaires

L'adressage dans le réseau

La connexion est établie à travers une liaison virtuelle, comparable à un circuit virtuel X.25, identifiée par un identificateur de lien virtuel (**DLCI**, *Data Link Connection Identifier*) similaire au NVL d'X.25 (figure 14.27). Les DLCI 0 et 1023 sont réservés, le premier est réservé au protocole de signalisation (Q.933), le second pour la signalisation de la congestion. La connexion virtuelle (protocole orienté connexion) entre les extrémités résulte de la concaténation des DLCI. À l'instar des NVL d'X.25, les DLCI n'ont qu'une signification locale. Dans la figure 14.27, la liaison virtuelle entre A et C résulte de la concaténation des voies logiques : 245, 18, 35 et 25.

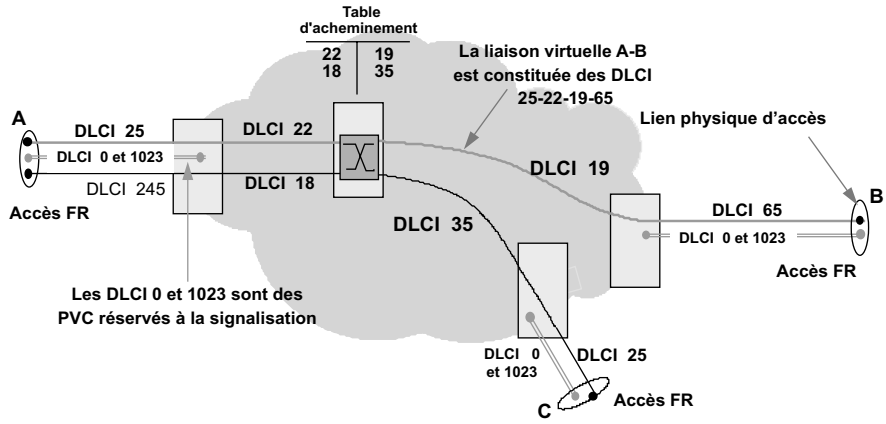


Figure 14.27 L'identification des voies virtuelles.

Les tables d'acheminement sont établies sous la responsabilité de l'opérateur (PVC) ou du réseau lors d'une demande de connexion (SVC). Dans ce dernier cas, la demande d'établissement est acheminée par le protocole Q.933 (signalisation par canal sémaphore, DLCI 0).

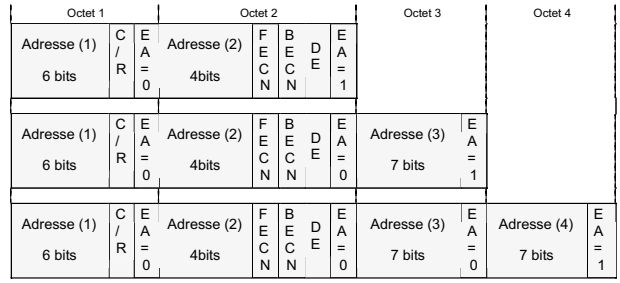


Figure 14.28 Le format d'adressage étendu.

Une capacité d'adressage sur 10 bits ne permet d'identifier que 1 024 (2^{10}) voies logiques, ce qui est suffisant pour la plupart des utilisateurs mais peut s'avérer faible pour l'identification des voies en interne dans le réseau. Aussi, un adressage étendu sur 17 ou 24 bits est prévu (figure 14.28). Le format représenté correspond au format du Frame Relay Forum (les bits FECN et BECN ont une position fixe). La figure 14.29 décrit les diverses plages d'adressage (adressage sur 10 bits).

DLCI	Utilisation
0	Établissement de circuits (Q.931)
1-15	Réservés
16-1007	DLCI utilisateurs (PVC, SVC)
1008-1018	Réservés
1019-1022	*Multicast*
1023	Signalisation de la congestion (CLLM ou LMI) et état des liens

Figure 14.29 Fonctions des différents DLCI à l'interface usager.

L'adressage des terminaux n'est pas fixé par la norme, le réseau peut spécifier des adresses de type E.164 (RNIS), X.121 (X.25) ou encore IP (TCP/IP).

© Dunod – La photocopie non autorisée est un délit

Le traitement des erreurs

Le traitement des erreurs n'est pas réalisé dans le réseau, chaque commutateur n'assure qu'une vérification d'intégrité de la trame :

- délimitation de la trame ;
- validation du DLCI ;
- contrôle d'erreur (FCS).

Toutes les trames non valides sont purement et simplement éliminées. Le traitement des erreurs est reporté sur les organes d'extrémité, il peut être mis en œuvre par la couche EOP ou confié aux protocoles de niveau supérieur, qui devront éventuellement mettre en œuvre des mécanismes de :

- numérotation des blocs de données pour la détection de perte.
- reprise sur temporisation.
- reprise sur erreur.

Le contrôle d'admission

La simplification du protocole a conduit à la suppression de tout contrôle de flux dans le réseau et à fragiliser celui-ci face aux problèmes de congestion. Aussi, toute nouvelle connexion ne peut être acceptée que si le réseau est apte à la satisfaire sans préjudice pour les connexions déjà établies. Toute demande de connexion est accompagnée d'un descripteur de trafic définissant en particulier le débit moyen et le débit de pointe demandés. Un contrat de trafic est passé entre la source et le réseau (**SLA**, *Service Level Agreement*), il comporte un descriptif complet des paramètres de la connexion et en particulier :

- Le **CIR** (*Committed Information Rate*) ou débit moyen garanti. Le CIR caractérise le débit moyen contractuel que doit garantir le réseau. La connexion ne sera acceptée que si la somme des CIR sur le lien (ou sur le nœud) ne dépasse pas un seuil déterminé par le gestionnaire du réseau.
- L'**EIR** (*Excess Information Rate*) ou surdébit autorisé au-dessus duquel tout bloc de données soumis au réseau est détruit ;
- Le temps d'analyse du trafic (Tc).

Le CIR définit le volume moyen admis dans le réseau ou **Bc** (*Committed Burst size*) tel que $Bc = CIR \cdot Tc$. L'EIR précise le volume maximal autorisé tel que $Bc + Be = (CIR + EIR) \cdot Tc$ où **Be** (*Excess Burst size*) représente le volume excédentaire admis au-dessus du contrat Bc (figure 14.30).

L'acceptation d'une nouvelle connexion ou l'établissement d'une nouvelle voie implique que chaque commutateur mémorise les différents paramètres des connexions déjà réalisées. Dans l'exemple donné figure 14.31, le FRAD d'entrée mémorise aussi la correspondance entre l'adresse IP distante et la voie virtuelle attribuée.

L'acceptation d'une nouvelle connexion n'est pas liée uniquement à la disponibilité de la bande passante. Elle dépend de la politique de gestion de la bande passante de l'opérateur qui peut admettre plus de données en entrée que le réseau ne peut en assimiler. La figure 14.32 illustre le principe d'une telle gestion. Les paramètres de QoS du Frame Relay sont, dans cette figure, comparés à ceux d'ATM (UBR, connexion sans aucune garantie de type best effort ; VBR, connexion à débit variable, temps réel ou non).

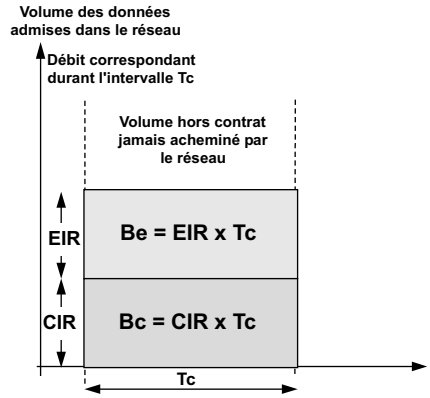


Figure 14.30 Relation entre les différents paramètres.

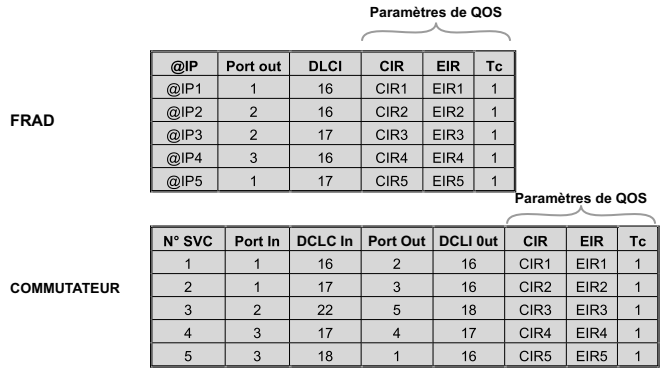


Figure 14.31 Description des tables d'acheminement.

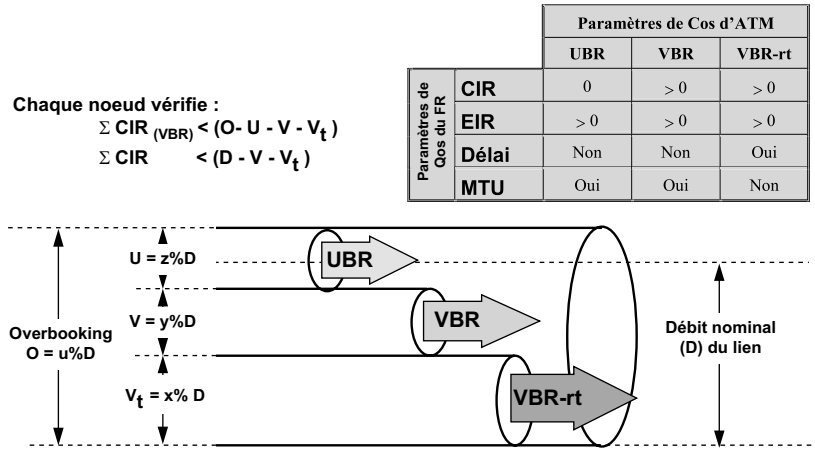


Figure 14.32 Politique de gestion de la bande passante.

La gestion de la congestion

Même si une fonction de contrôle d'admission est mise en œuvre (**CAC**, *Connexion Admission Control*), le réseau, du fait de la soumission simultanée de rafales, peut atteindre un état de congestion plus ou moins durable. Dans ces conditions, non seulement le commutateur d'entrée implémente une fonction de surveillance, mais aussi chaque commutateur.

Si le volume du trafic soumis est inférieur à Bc, tout le trafic soumis est transmis par le réseau. Si le volume de trafic soumis est compris dans l'intervalle]Bc...Be] les blocs de données sont transmis mais marqués (*Cell tagging*). Lors de l'éventuelle traversée d'un nœud congestionné, ces blocs seront éliminés en priorité. Les blocs transmis au-dessus de Be seront systématiquement éliminés. La figure 14.33 illustre ce propos.

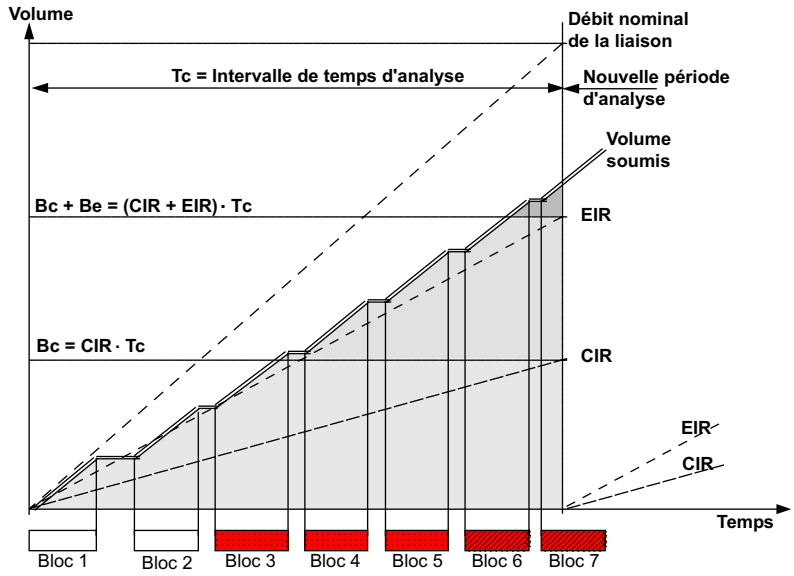


Figure 14.33 Le contrôle de congestion dans les réseaux Frame Relay.

Les blocs 1 et 2 sont transmis normalement à partir du bloc 3 le volume moyen garanti pour l'intervalle de temps Tc est dépassé, le bloc 3 et les suivants seront marqués comme dépassant le trafic moyen. Les blocs marqués (bit **DE**, *Discard Eligibility*) seront éliminés s'ils traversent un nœud en état de congestion. Les blocs 6 et 7 excèdent le volume maximal autorisé, ils ne seront pas admis dans le réseau.

L'analyse du débit de la source telle qu'elle est réalisée dans le schéma de la figure 14.33 n'est pas satisfaisante. En effet, examinons le débit d'une source illustré par la figure 14.34, on constate que durant chaque période d'examen Tc, le trafic moyen est resté en deçà du CIR, le bit DE n'a pas été positionné. Cette approche, par période fixe, a masqué les rafales.

Une période Tc glissante aurait permis la détection des rafales (figure 14.35). Généralement on adopte les valeurs suivantes : Tc = une seconde, mesure toutes les 100 ms.

La figure 14.36 fournit une analogie qui illustre parfaitement le mécanisme de la période d'analyse glissante (Tc). Elle matérialise en plus la fonction de lissage de trafic réalisée par le FRAD (*Frame Relay Access Device*) d'accès.

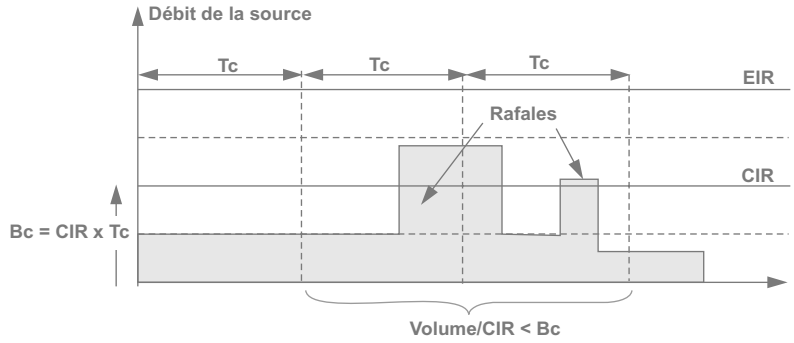


Figure 14.34 L'analyse du trafic avec une période Tc fixe.

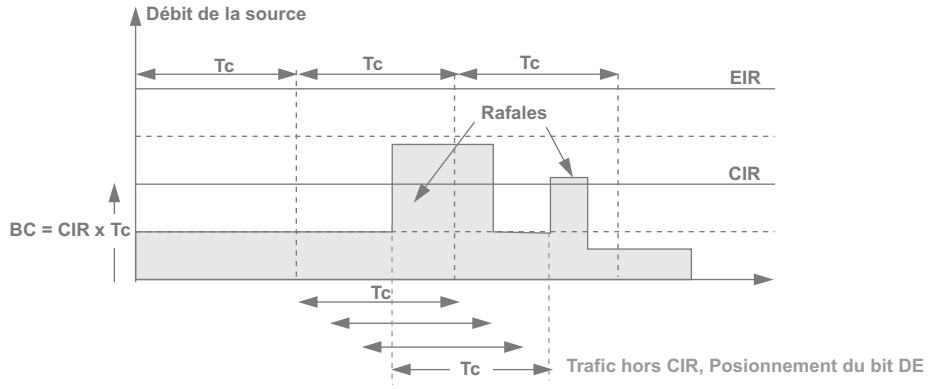


Figure 14.35 La détection des rafales avec un Tc glissant.

Les données sont admises dans un premier *buffer* qui réalise le lissage de trafic. Lorsque ce *buffer* est plein, elles sont admises dans un second *buffer*, acheminées par le réseau mais marquées comme trafic excédentaire toléré (DE=1). En cas de dépassement de la tolérance, toutes les données sont éliminées.

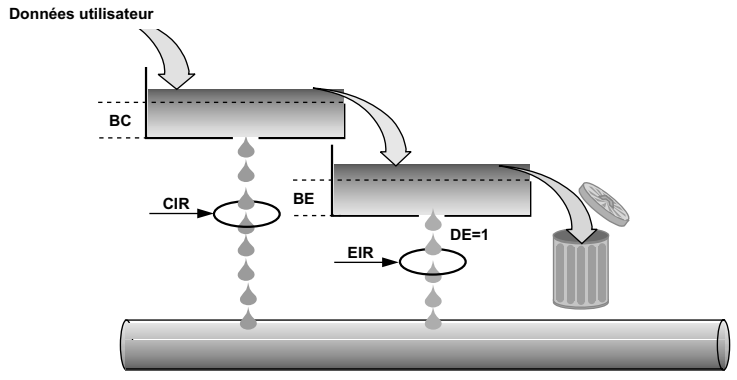


Figure 14.36 Illustration de la mise en œuvre de la fonction d'admission du trafic.

© Dunod – La photocopie non autorisée est un délit

L'élimination par les commutateurs internes au réseau en état de congestion du trafic excédentaire identifié par le bit DE n'est pas une solution complètement satisfaisante. En effet, si elle permet de résoudre l'état de congestion, elle n'en élimine pas la cause. Il est nécessaire d'en avertir les entités communicantes pour que, par autodiscipline, les sources ralentissent leur émission. Ce principe est illustré par la figure 14.37.

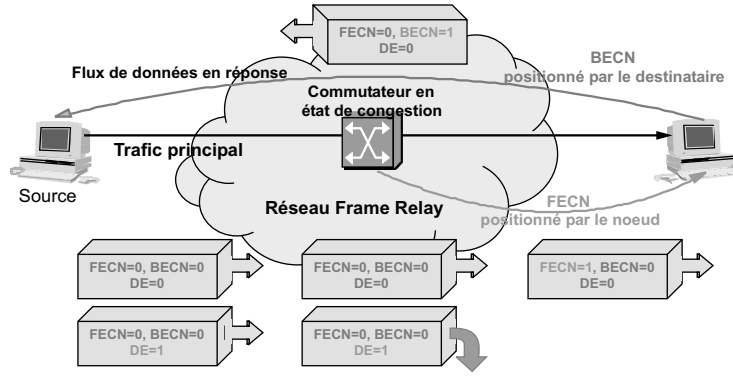


Figure 14.37 La notification de congestion.

Lorsqu'un bloc de données traverse un nœud en état de congestion, celui-ci positionne, dans toutes les trames le traversant, le bit **FECN** (*Forward Explicit Congestion Notification*). Ainsi, le destinataire est averti de l'état de congestion mais aussi que certaines trames ont pu être éliminées (bit DE=1). Cette indication est transmise aux couches supérieures afin que celles-ci mettent en œuvre, éventuellement, un mécanisme de contrôle de flux et de contrôle de séquencement (détection des trames perdues). Le destinataire profite des données en réponse pour avertir la source que le circuit qui le dessert (circuit aval) est congestionné (**BECN**, *Backward Explicit Congestion Notification*).

Ce mécanisme n'est pas très efficace car il suppose un trafic bidirectionnel ce qui peut introduire une inefficacité complète du système ou, du moins, une certaine inertie. Ce procédé est injuste. En effet, tous les hôtes dont les données transitent par le nœud congestionné sont invités à réduire leur trafic, même ceux qui ne sont pas responsables de cet état de fait. Pour y remédier des protocoles spécifiques ont été développés.

Les protocoles de gestion de la congestion

➤ Le protocole CLLM

Le protocole CLLM (origine ANSI T1 606) permet à tout nœud en état de congestion d'en avertir ses voisins et la source. Le message CLLM (*Consolided Link Layer Management*) contient la liste des voies logiques congestionnées et la cause de cette congestion. Le protocole CLLM est implémenté sur la trame **XID** de LAP-D (*eXchange IDentifier*).

➤ Le protocole LMI

Plus complet que le protocole **CLLM**, **LMI** (*Local Management Interface*) a été défini par le Frame Relay Forum pour prendre en charge toute la signalisation d'un réseau relais de trames. Le protocole LMI n'est disponible qu'à l'interface usager (**UNI**, *User Network Interface*). Il utilise le

DLCI 1023 (*Data Link Connection Identifier*), dernière voie logique identifiable dans l'adressage minimal à 10 bits, pour connaître l'état des circuits virtuels, de ce fait, les protocoles CLLM et LMI s'excluent mutuellement. Le protocole LMI (*Local Management Interface*) permet à l'utilisateur (**FRAD**) de connaître à tout instant :

– L'état de ses circuits virtuels permanents (*Virtual circuit status*) par l'échange de messages questions (*Status enquiry*, demande de statut) et de messages réponses (*Status*, état du lien).
– L'état du lien physique (*Link status*) par échange de messages numérotés (*Keep alive*).
– La modification du statut d'un lien (DLCI) sur l'initiative du réseau (messages asynchrones).

Les messages d'état du lien autorisent un contrôle de flux très efficace en signifiant à un équipement l'indisponibilité du lien (protocole de type XON/XOFF). La figure 14.38 symbolise l'échange de messages. La procédure de scrutation introduit un délai relativement important avant que le FRAD ne connaisse l'état d'un lien. La procédure asynchrone remédie à cet inconvénient, l'une des deux entités peut prendre l'initiative d'envoyer un message de demande de statut. Le protocole LMI utilise les trames non numérotées de LAP-D.

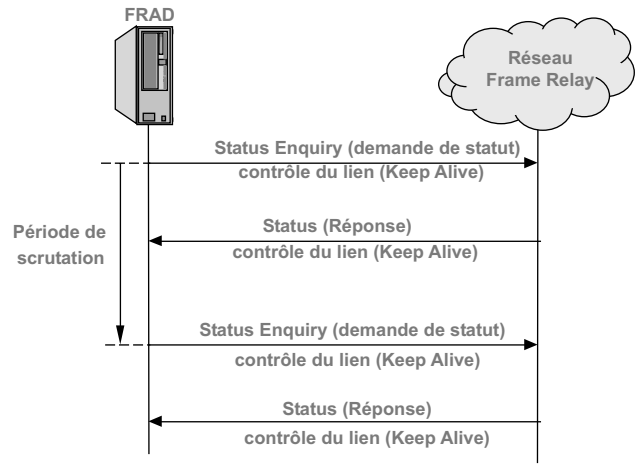


Figure 14.38 Échange de messages synchrones sur l'état des liens.

L'établissement de la connexion

Les circuits virtuels commutés sont établis à la demande de l'utilisateur[4]. Les messages d'établissement sont acheminés sur le DLCI 0 (Voie de signalisation bidirectionnelle).

Le message d'établissement est assez complexe. En effet, lors de la mise en service d'un circuit virtuel permanent, les différents paramètres de la liaison sont fixés à la souscription de l'abonnement et restent valables pendant toute sa durée. Ce n'est pas le cas des circuits virtuels commutés. À chaque appel, les paramètres de la liaison demandée doivent être fournis (message *Setup*). La figure 14.39 illustre l'échange de messages lors de l'établissement d'une connexion et la libération du circuit virtuel.

4. L'établissement d'un circuit virtuel commuté est régi par la recommandation Q.933 dérivée de la recommandation Q.931.

© Dunod – La photocopie non autorisée est un délit

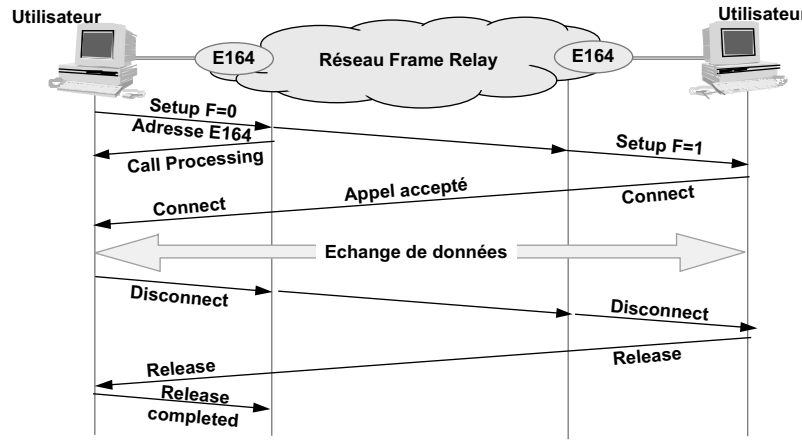


Figure 14.39 Établissement et libération d'une connexion commutée (SVC).

La demande de connexion (*Setup*) est acquittée deux fois, la première fois par le réseau (Signal de progression d'appel, *Call processing*) qui rend compte qu'il accepte la nouvelle connexion avec les paramètres précisés dans la demande et qu'il transmet celle-ci à l'appelé. Le message *Call processing* contient le DLCI affecté à la connexion (c'est le réseau qui détermine le DLCI à employer). L'appelé acquitte à son tour la demande de connexion (*Connect*).

Dans le message de *Setup*, le numéro de DLCI n'est obligatoire que dans le sens réseau/abonné (c'est le réseau qui fixe le numéro de DLCI). Dans le sens usager/réseau, s'il est présent, le numéro de DLCI ne constitue qu'une proposition que le réseau accepte ou refuse. C'est le réseau qui, en dernier, détermine le numéro de DLCI à utiliser.

Les paramètres de la liaison sont fixés dans chaque sens (liaison bidirectionnelle, éventuellement dissymétrique), ce sont :

– La charge utile des trames (MTU, *Maximum Transfert Unit*).
– Le débit garanti de la liaison (CIR).
– Le débit minimal acceptable (qualité de service).
– Le *Committed Burst size* (Bc).
– L'*Excess Burst size* (Be).

Conclusion, le relais de trames et X.25

Indépendamment des progrès technologiques réalisés dans les commutateurs, le gain de performance obtenu avec le relais de trames résulte de la simplification du protocole et de la suppression de contrôles redondants. Les figures 14.40 et 14.41 illustrent ces propos.

Le gain en performance du relais de trames par rapport à X.25 est de l'ordre de 5 à 10. Le succès actuel du relais de trames est essentiellement dû à sa simplicité face à ATM. Particulièrement adapté à l'interconnexion des systèmes exigeants en débit et générant des trafics sporadiques (réseaux locaux, applications client/serveur), il a été adapté au transport des flux isochrones comme la voix[5] (FRF11 et FRF12).

5. Voir chapitre 21, *Les réseaux privés de téléphonie et la voix sur IP*.

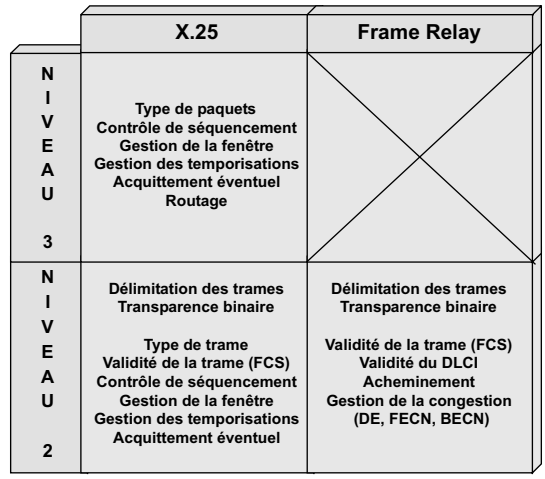


Figure 14.40 La comparaison des traitements X.25/relais de trames.

Fonctionnalités	X.25	Frame Relay
Commutation	Niveau 3	Niveau 2
Détection d'erreur	Oui (reprise)	Oui
Reprise sur erreur	Oui	Non (élimination)
Qualité réseau	Quelconque (reprise sur erreur)	Bonne (pas de reprise sur erreur)
Contrôle de congestion	Oui	Indication de congestion
Élimination sur congestion	Non	Oui
Contrôle de flux	Oui	Non
SVC	Oui	Oui
PVC	Oui	Oui
Taille maximale des PDU	2 048 octets	4 096 octets
Qualité de service	Non	Oui (Débit garanti, CIR)
Contrôle d'admission	Non	Oui
Délai de transit	100 ms	30 à 40 ms

Figure 14.41 La comparaison des fonctionnalités X.25/Relais de trames.

14.3 L'ATM (*ASYNCHRONOUS TRANSFER MODE*)

14.3.1 Généralités

L'ATM a été développé dans le cadre de l'évolution du réseau téléphonique (RNIS Large Bande, **B-ISDN** ou *Broadband Integrated Service Digital Network*). En effet, la commutation de circuits des réseaux voix traditionnels monopolise la bande passante alors que la commutation de paquets autorise le multiplexage statistique des sources et par conséquent optimise l'utilisation de la bande passante. C'est sur ces bases que le CNET (Centre national d'étude et de télécommunication) a

© Dunod – La photocopie non autorisée est un délit

décrit, en 1982, une technique de multiplexage asynchrone (**ATD**, *Asynchronous Time Division*) qui allait donner naissance à l'ATM (figure 14.42).

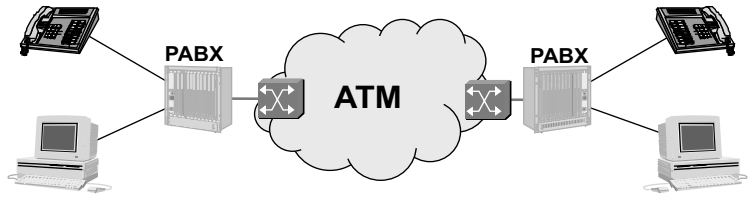


Figure 14.42 L'origine de l'ATM.

Intégrant à l'origine le traitement des données de tout type (voix/texte/images), un réseau ATM doit assurer :

– L'indépendance temporelle du réseau, c'est-à-dire qu'ATM autorise le transport de données à débit variable et sans relation temporelle entre elles (mode de transfert asynchrone).
– L'indépendance sémantique, c'est-à-dire que dans le réseau toutes les données subissent le même traitement (services non différenciés). Cette approche allège le travail du réseau mais reporte aux extrémités les traitements spécifiques à tel ou tel type de données.

L'ATM est une technologie en mode connecté, les données ne sont acheminées dans le réseau qu'après l'établissement d'une voie virtuelle (**VCC**, *Virtual Channel Connection*). Le circuit virtuel peut-être :

– bidirectionnel en mode point à point (*unicast*),
– unidirectionnel en mode point à multipoint (*multicast*).

14.3.2 La taille des unités de données ou cellules

Étudié dans le cadre du développement du RNIS large bande, ATM voit ses caractéristiques fortement conditionnées par le transfert de flux isochrone tel que la voix. Ce dernier point a été déterminant dans le choix de la taille des unités de données (cellules), celle-ci doit permettre une commutation rapide et minimiser la gigue d'insertion.

La figure 14.43 illustre l'effet de l'insertion de gigue. En effet, selon le traitement appliqué, les données 1, 2, 3 en entrée peuvent se présenter en sortie selon les trois cas représentés. On s'aperçoit alors que dans le cas 1, le paquet 3 a été inséré entre les paquets 1 et 2 rompant les caractéristiques temporelles qui reliaient les deux paquets.

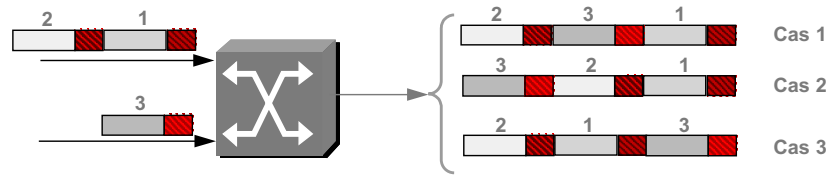


Figure 14.43 La taille des unités de données et la gigue d'insertion.

Ces deux impératifs (temps de commutation et gigue) militent pour une petite taille de données. Cependant, indépendamment du temps de bouche à oreille, limité à 150 ms pour un confort conversationnel optimal, le temps de traversée du réseau doit rester inférieur à 25 ms (temps maximal 24 ms) si on ne veut pas équiper le réseau de dispositifs d'annulation d'écho. De ce fait, il s'agit de rechercher une taille de cellule compatible avec l'élongation envisagée du réseau (figure 14.44).

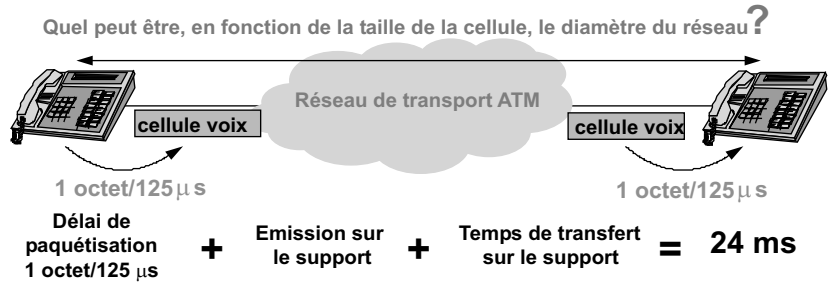


Figure 14.44 Le temps de transfert d'une cellule voix.

Compte tenu, d'une part que la paquétisation des données s'effectue à raison de un octet toutes les 125 μs (codage MIC) et, d'autre part en admettant une vitesse de propagation sur le support de 2.10^8 m/s et un débit du lien de 64 kbit/s (voix MIC, G.711), la figure 14.45 indique la distance maximale franchissable.

Taille de la cellule	Temps de paquétisation en ms	Temps de transfert sur le support	Temps de transport admissible en ms	Distance théorique en km
16	2	2	20	4 000
32	4	4	16	3 200
48	6	6	12	2 400
64	8	8	8	1 600
96	12	12	0	

Figure 14.45 Distance maximale franchissable sans annuleur d'écho.

La figure 14.45 montre que la limite maximale de la taille des unités de données est de 64 octets, c'est cette dernière taille qui avait été proposée à l'UIT par certains pays, notamment les États-Unis. En effet, compte tenu de la dimension de ce pays, les réseaux de transport étaient déjà équipés de systèmes d'annulation d'écho, une taille de 64 octets semblait, alors, présenter le meilleur rendement pour la transmission de données (rapport entre les données protocolaires et les données utiles). Pour des raisons inverses, les Européens préféraient une taille plus réduite : recherche de la distance maximale franchissable sans annuleur d'écho et meilleur rendement de multiplexage (figure 14.46), ils proposèrent une taille de 32 octets. Finalement, un compromis a été adopté et la taille des unités de données (cellules) fut fixée à 48 octets et 5 octets d'en-tête.

© Dunod – La photocopie non autorisée est un délit

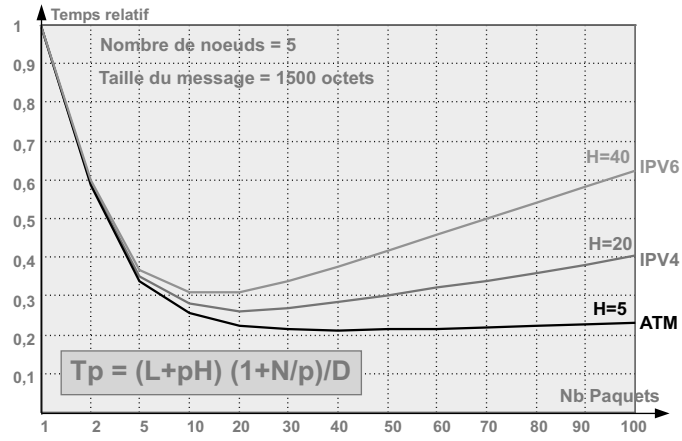


Figure 14.46 Taille optimale de l'unité de donnée.

14.3.3 Les mécanismes de base et le format de la cellule ATM

L'adressage dans les réseaux ATM

À l'instar de X.25 ou du Frame Relay, l'ATM utilise en interne dans le réseau un adressage de convention identifiant les voies virtuelles (multiplexage par étiquette) et un adressage hiérarchique à la périphérie du réseau de type E.164 pour les réseaux publics (adressage du RNIS).

La taille des tables de commutation est l'un des facteurs principaux intervenant dans l'efficacité de la commutation. La commutation est d'autant plus rapide que la taille des tables de commutation est faible. Compte tenu de cette remarque, l'ATM, à des fins d'efficacité, utilise deux niveaux d'identification. En effet, dans un réseau plusieurs sources partent d'un même commutateur d'entrée et se dirigent dans une même direction (route). Plutôt que de gérer les *N* connexions, il est plus aisé de les regrouper (identifiant secondaire) et de ne traiter dans le cœur du réseau que cet identifiant de second niveau (figure 14.47) :

– Un premier niveau identifie la voie virtuelle (**VCI,** *Virtual Channel Identifier*). Il s'agit de l'identifiant des flux échangés entre deux systèmes d'extrémités, notion similaire au numéro de voie logique d'X.25 ou du DLCI du Frame Relay.
– Un second niveau regroupe (agrégation de flux) un ensemble de voies virtuelles ayant une même destination (nœud intermédiaire ou interface d'usager) en un seul identifiant dit *Virtual Path Identifier* (**VPI**). Le VPI représente une connexion semi-permanente entre deux nœuds du réseau, elle est établie et contrôlée par l'administrateur du réseau.



Figure 14.47 La double identification d'ATM.

Les commutateurs de second niveau, appelés **brasseurs**, commutent l'ensemble des voies virtuelles affectées à un faisceau (acheminement selon le VPI), ce qui garantit des temps de commutation brefs. Les commutateurs sont généralement situés à la périphérie du réseau (commutateur d'accès), tandis que les brasseurs assurent la commutation des faisceaux virtuels en interne dans le réseau (figure 14.48).

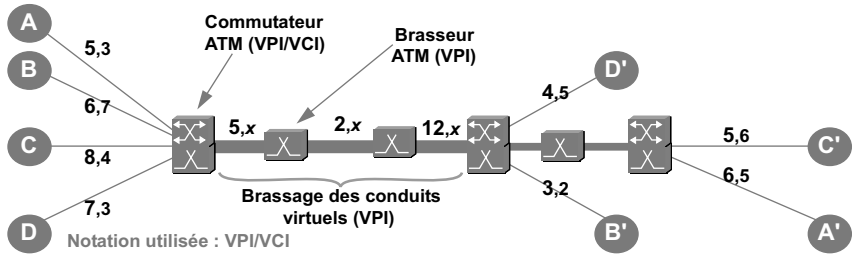


Figure 14.48 Le double niveau d'acheminement des cellules.

Le contrôle d'erreur

Même si la fiabilisation des supports de transmission autorise un allégement du contrôle d'erreur, il reste cependant nécessaire de protéger le réseau contre un acheminement erroné des blocs de données. À chaque commutateur, la validité des informations de routage (VPI/VCI) est contrôlée. Le champ **HEC** (*Header Error Control*) assure un contrôle d'erreur de type CRC sur l'en-tête, il autorise une autocorrection de celle-ci pour des erreurs simples ne portant que sur 1 bit (distance de Hamming de 4). En cas d'erreurs non corrigées ou d'erreurs multiples, les cellules sont éliminées. L'HEC ou octet de contrôle (figure 14.49) est le reste de la division booléenne (modulo 2) des quatre premiers octets de l'en-tête par le polynôme générateur : $G(x) = x^8 + x^2 + x + 1$, auquel est ajouté le polynôme $C(x) = x^6 + x^4 + x^2 + 1$ (addition booléenne soit un OU exclusif avec 01010101).

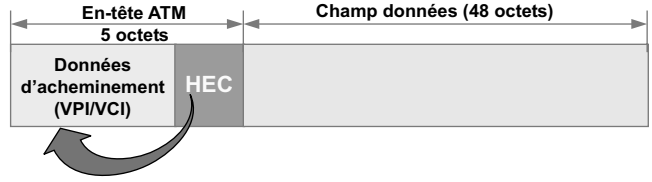


Figure 14.49 La portée du champ HEC.

Rappelons que la vérification de la validité des données, la reprise sur erreur ou sur temporisation sont éventuellement confiées aux couches supérieures des systèmes d'extrémité (*End Systems*).

La délimitation des cellules

L'ATM n'utilise aucun fanion pour délimiter les cellules. Celles-ci ayant une taille fixe et une fréquence de récurrence élevée, il suffit de se positionner correctement sur un octet pour reconnaître les limites des cellules, c'est le champ HEC qui remplit cette fonction. Le HEC est calculé au fil de l'eau sur le flot de bits reçu dans un registre FIFO de 40 bits (5 octets) représenté figure 14.50.

© Dunod – La photocopie non autorisée est un délit

Lorsque le contenu du cinquième octet du *buffer* correspond au résultat du calcul de l'HEC sur les 4 octets précédents, l'HEC est supposé trouvé. Dans ces conditions, le début de la cellule suivante (en-tête) se situe 48 octets plus loin. Un embrouillage du champ information élimine les risques de reproduction d'un faux « HEC » dans le champ données.



Figure 14.50 Principe du repérage du HEC.

Les formats de l'en-tête de cellule ATM

À des fins d'efficacité, l'en-tête ATM ne contient que les informations strictement nécessaires à l'acheminement, au contrôle du type de données et à la protection de l'en-tête. ATM utilise deux formats d'en-tête, le premier est utilisé à l'interface usager/réseau (**UNI**, *User to Network Interface*) et le second en interne dans le réseau (**NNI**, *Network to Network Interface*). La figure 14.51 représente ces deux formats.

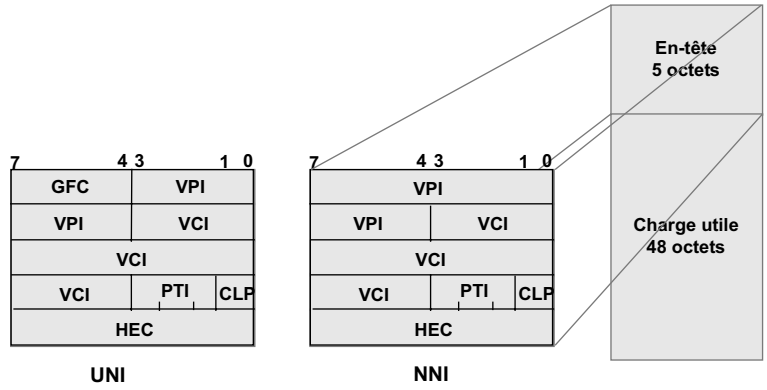


Figure 14.51 Les formats de l'en-tête de cellule ATM.

Le champ **GFC** (*Generic Flow Control*) devait, en mode contrôlé (*Controled*), assurer le partage équitable de l'accès au réseau aux différentes stations dans une configuration point à multipoint. En mode point à point, le GFC devait permettre la résolution des conflits d'accès (résolution des contentions) et assurer le contrôle de flux à l'interface usager/réseau. Non défini, ce champ doit être mis à 0.

Sa présence est inutile dans le réseau, les quatre bits correspondants sont « récupérés » pour étendre le champ VPI des cellules NNI. Cette technique conduit à définir deux types d'en-tête de cellule. Selon que l'on se situe à l'interface usager/réseau (UNI) ou à une interface réseau/réseau (NNI) :

– Les cellules UNI identifient 65 536 VCI (16 bits) et 256 VPI (8 bits).
– Les cellules NNI identifient 65 536 VCI et 4 096 VPI (12 bits).

Deux types de données transitent dans un réseau, celles d'origine utilisateur et les données propres à la gestion du réseau (signalisation, maintenance...). Le champ **PT** (*Payload Type*) sur trois bits (bits 3, 2, 1 du quatrième octet) indique le type de charge contenue dans le champ Données (figure 14.52).

Type Bit 3		EFCI Bit 2		User Bit 1	
0	Flux d'origine usager (Cellules usager)	0	Bit EFCI (*Explicit Forward Congestion Indication*), pas de congestion	0,1	A disposition de l'application, peut être utilisé par la couche d'adaptation pour indiquer la fin de la segmentation de l'unité de données (dernier fragment = 1)
		1	La cellule a traversé au moins un nœud congestionné.		
1	Flux d'origine réseau (Cellules réseau)	0	Flux de maintenance (Cellules OAM)	0	De section (Entre nœuds)
				1	De bout en bout
		1	Gestion des ressources (Cellules RM)	0	Réseau
				1	Réservé

Figure 14.52 La signification du champ Payload Type.

Le traitement de la congestion est similaire à celui utilisé dans le relais de trames. Le bit de préférence à l'écartement (**CLP**, *Cell Loss Priority*) indique, lors d'un état de congestion, les cellules à éliminer en priorité. Le positionnement de ce bit est de la responsabilité de la source. En fait, le bit CLP à 1 indique une cellule de priorité basse, à 0 il identifie une cellule de priorité haute.

Le bit CLP permet de spécifier, sur une même connexion, des flux différents. Il peut, par exemple, pour des transferts de vidéo compressée être positionné à 0 pour les informations essentielles et à 1 pour les autres.

14.3.4 Les différentes couches du modèle

Présentation

L'ATM comporte trois couches dont les fonctionnalités principales sont décrites ci-dessous. Les relations entre les différentes couches sont représentées en figure 14.53.

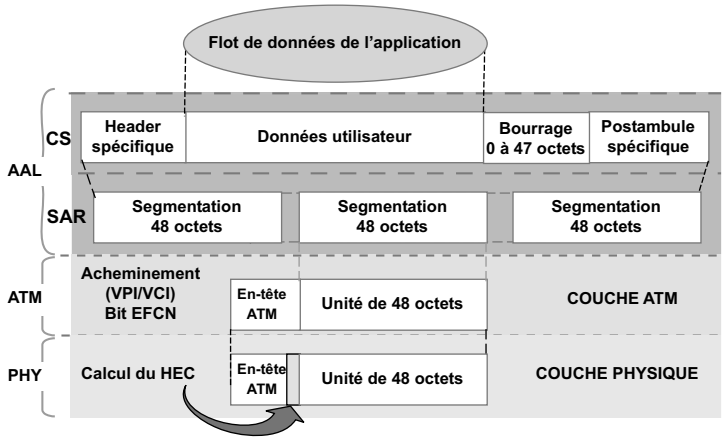


Figure 14.53 Relations entre les différentes couches de l'ATM.

© Dunod – La photocopie non autorisée est un délit

La couche **AAL** (*ATM Adaptation Layer*) garantit aux applications utilisateurs la qualité de service requise par l'application. Quatre types d'AAL sont proposés aux applications : AAL1, AAL2, AAL3/4 et AAL5. La couche AAL est divisée en deux sous-couches :

– La sous-couche de convergence (CS, *Convergence Sublayer*) est destinée à incorporer les informations spécifiques au type d'AAL utilisé.
– La sous-couche de segmentation et de réassemblage (SAR, *Segmentation and Reassemblage*) adapte le format de l'unité de données issue de la sous-couche CS au format requis par ATM (cellules de 48 octets).

La couche **ATM** est indépendante du sous-système de transport physique et des services d'applications qui l'utilisent. Elle assure les fonctions de multiplexage et démultiplexage des cellules, la génération et l'extraction des en-têtes, l'acheminement (commutation) des cellules et la translation des VPI/VCI enfin, le contrôle de flux (*GFC, Generic Flow Control*) à l'interface UNI (*User Network Interface*).

La couche physique (**PHY**) est chargée de fournir à la couche ATM un service de transport des cellules. Pour assurer, à la couche ATM, la transparence du support physique utilisé, la couche PHY est scindée en 2 sous-couches :

– La sous-couche **TC** (*Transmission Convergence*) assure l'adaptation des débits, le contrôle des données (HEC) et la délimitation des cellules.
– La sous-couche **PM** (*Physical Medium*) fournit l'accès au support physique et gère les mécanismes de synchronisation.

La couche ATM

La couche ATM est chargée :

– de l'acheminement des cellules dans le réseau,
– de l'ajout et du retrait des en-têtes ATM,
– du contrôle de flux (**GFC**, *Generic Flow Control*) à l'interface utilisateur (UNI),
– du contrôle d'admission en fonction de la qualité de service requise (**CAC**, *Connection Admission Call*),
– du lissage de trafic (*Traffic shopping*).

La figure 14.54 illustre le mécanisme de la commutation. Le premier étage du commutateur effectue le multiplexage et démultiplexage des circuits virtuels, alors que le second étage les commute. Ainsi, la voie virtuelle 1 (VC1) du conduit virtuel 2 du port d'entrée 2 (VP2) est translatée en voie virtuelle 2 (VC2) et affectée au conduit virtuel 1 du port de sortie 3 (VP1).

Le contrôle d'admission (**CAC**, *Connection Admission Call*) a pour objectif de garantir une certaine qualité de service (**QoS**) à la connexion établie en termes de débit, perte de cellules et de variation de délai de transfert (gigue). À cet effet, l'ATM Forum a défini cinq classes de service[6]

6. À l'origine, l'IUT avait défini quatre classes de service, la classe A (débit constant, mode connecté), classe B (débit variable, mode connecté), classe C (débit variable, mode connecté) enfin classe D (débit variable mode non connecté), ces classes correspondaient directement aux AAL1, 2, 3 et 4. Proches l'une de l'autre, les AAL 3 et 4 ont été réunies en

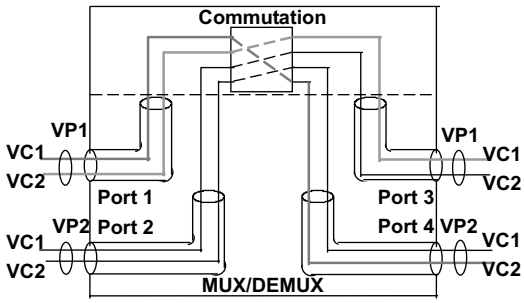


Table de commutation

Entrée		Sortie	
Port	VPI/VCI	Port	VPI/VCI
1	1,1	4	2,2
1	1,2	3	1,1
2	2,1	3	1,2
2	2,2	4	2,1

Figure 14.54 La commutation ATM.

(**CoS**, *Class of Service*) pour garantir à l'utilisateur un service de transport en relation avec ses besoins.

Le contrôle d'admission n'est efficace que s'il existe un mécanisme permanent de surveillance qui s'assure que la source respecte les paramètres de trafic définis par le contrat de service. Cette surveillance est réalisée par une fonction spécifique : l'**UPC** (*Usage Parameter Control*). L'UPC peut retarder une cellule, marquer une cellule (bit CLP à 1, *Cell Loss Priority*), détruire une cellule et même demander la fermeture d'une connexion.

La couche AAL

➤ Applications et couche AAL

La technologie ATM est transparente aux données transportées (transparence sémantique). De ce fait, il est nécessaire de réaliser, pour chaque type d'application, une adaptation spécifique afin d'affiner la qualité de service offerte aux applications, c'est le rôle de la couche **AAL** (*ATM Adaptation Layer*). Cinq types d'adaptations spécifiques ont été définis (figure 14.55).

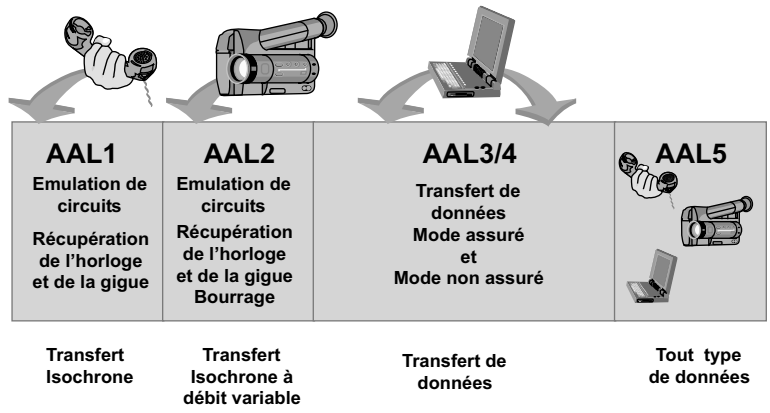


Figure 14.55 Les couches d'adaptation d'ATM.

une seule, et remplacée par l'AAL5 par l'ATM Forum (simplification de l'AAL3/4). Dans le même temps l'ATM Forum redéfinissait les classes de services.

© Dunod – La photocopie non autorisée est un délit

➤ La couche AAL1

La couche AAL1 permet un transfert isochrone par émulation de circuits, elle offre un service à débit constant (**CBR**, *Constant Bit Rate*). Elle n'assure que des fonctions minimales de segmentation et réassemblage, séquencement des unités de données et récupération de la gigue de cellules et de l'horloge (figure 14.56).

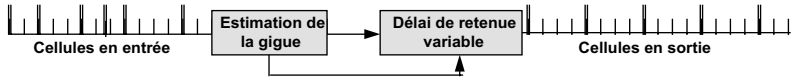


Figure 14.56 Principe de la récupération de gigue.

L'AAL1, conçue essentiellement pour les trafics de type isochrone non compressé, n'offre qu'un service CBR (*Constant Bit Rate*). Elle n'utilise pas les possibilités du multiplexage par étiquette et monopolise inutilement des ressources réseau (émulation de circuits).

➤ La couche AAL2

La couche AAL2 diffère essentiellement de l'AAL1 par la possibilité de débit variable (**VBR**, *Variable Bit Rate*). L'AAL2, spécifique au transfert isochrone compressé (service VBR), assure la synchronisation des extrémités et offre une référence temporelle. Essentiellement destinée à la vidéo, l'AAL2 semble aujourd'hui abandonnée. En effet, la compression d'images de type MPEG-2 possède sa propre référence temporelle et, dans ces conditions, il semble plus efficace d'utiliser l'AAL5. Cependant AAL2 est utilisée dans les réseaux sans fils de troisième génération (**UMTS**, *Universal Mobile Telecommuncations System*).

➤ La couche AAL3/4

Les couches AAL3 et 4 avaient été étudiées pour les transferts de type données (flux sporadiques). Elles se différenciaient par l'approche mode connecté (AAL3) et non connecté (AAL4). Elles ont été regroupées pour n'en former qu'une seule, l'AAL3/4, aujourd'hui complètement abandonnée au profit de l'AAL5 plus efficace.

➤ La couche AAL5

Proposée par l'ATM Forum, la couche AAL5 est une simplification de la couche AAL3/4 dont elle adopte la même architecture. Ces objectifs sont similaires mais elle offre un service plus efficace. La structure des données est représentée figure 14.57.

La couche AAL 5 autorise un transfert de données efficace, la SDU (*Service Data Unit*) est alignée sur un multiple de 48 octets (Champ **PAD**). Le champ **UU** (**CPCS UU**, *Service Data Unit Common Part Convergence Sublayer User-to-User Indication*) indique à l'usager le début, la suite et la fin du bloc de données. Le champ **CPI** (*Common Part Indication*) est utilisé pour aligner le suffixe (*Trailer*) sur 8 octets, une utilisation future est en cours de définition. Le champ **LI** (*Length Indicator*) indique la longueur exacte des données utiles, tandis qu'un CRC sur 32 bits sécurise la SDU. Il n'y a pas de délimiteur de début et de fin, seul, le dernier bit du type de protocole (**PTI**, *Payload Type Identifier*) de l'en-tête ATM (bit 2 ou bit *Last Cell*) est à 1 dans le dernier fragment.

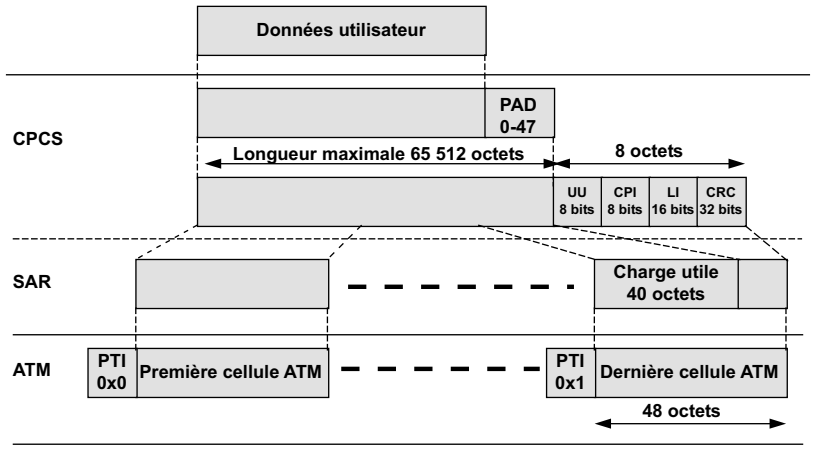


Figure 14.57 La structure de données de la couche AAL5.

L'AAL5, définie par l'ATM Forum pour remplacer l'AAL3/4, semble la seule susceptible de subsister. Cependant, il serait nécessaire d'y apporter quelques modifications, notamment de pouvoir désactiver la détection d'erreur lors de transfert voix ou image peu sensible aux erreurs portant sur quelques bits. Des adaptations spécifiques (propriétaires) lui permettent d'assurer de manière efficace le transfert des flux voix (récupération des silences et de la gigue).

14.3.5 La qualité de service dans l'ATM

Les classes de service de l'ATM Forum

Conçu à l'origine pour traiter des flux de tout type, ATM différencie les traitements d'extrémité (AAL) et offre à chacun une connexion en adéquation avec ses besoins : c'est la notion de **classe de service**. Les classes de service permettent à l'utilisateur de spécifier ses besoins : c'est la notion de **contrat de service**. Si le réseau a la capacité de satisfaire les demandes formulées, il accepte la connexion, sinon il peut proposer des paramètres de repli (figure 14.58).

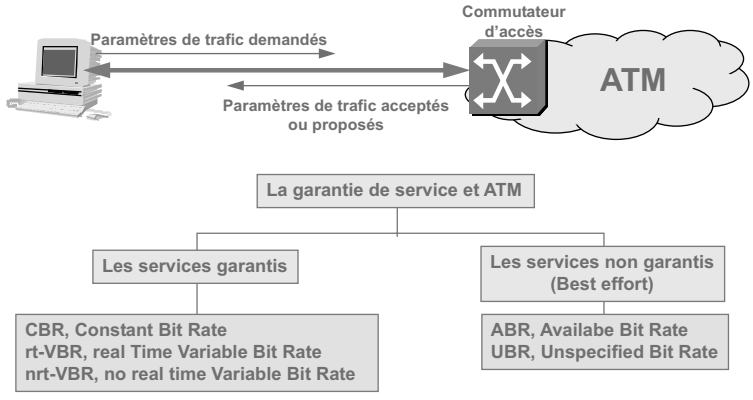


Figure 14.58 Le contrat de service et les classes de service.

© Dunod – La photocopie non autorisée est un délit

La classe de service **CBR** (*Constant Bit Rate* ou **DBR**, *Deterministe Bit Rate*) définit un raccordement à débit constant qui correspond à une émulation de circuit. Elle est destinée aux applications de type voix ou vidéo non compressée. Le débit doit être garanti de bout en bout.

La classe **VBR** (*Variable Bit Rate* ou **SBR**, *Statistical Bit Rate*) s'applique aux trafics sporadiques, la connexion définit un débit minimal et un débit maximal. Pour les applications temps réel (*VBR-rt*, *VBR real time*) les variations maximales tolérées du délai de transfert (gigue) sont indiquées lors de la connexion. La classe VBR-rt correspond aux applications de type voix ou vidéo compressées. La classe VBR-nrt (*VBR no real time*) est généralement requise pour les applications de type transactionnel.

Les classes CBR et VBR garantissent aux applications une certaine qualité de service, le réseau doit s'adapter aux besoins de celles-ci. Cependant certaines applications, notamment celles de type données, sont moins exigeantes en terme de débit. Afin de mieux utiliser les capacités du réseau, il est alors préférable que ce soit les applications qui s'adaptent aux capacités de transfert de ce dernier et non l'inverse. La classe de service **ABR** (*Available Bit Rate*) ne spécifie, à la connexion, qu'un débit minimal et maximal, il n'y a aucun débit moyen garanti, les applications utilisent le débit disponible sur le réseau (entre les deux bornes prédéfinies). La classe ABR est adaptée à l'interconnexion de réseaux locaux.

De même, une classe de service de type datagramme ou *best effort* a été définie : l'**UBR** (*Unspeciefied Bit Rate*). L'UBR ne fournit aucune garantie de débit, ni de remise des cellules. Si l'état du réseau le permet, toutes les cellules soumises sont transmises, en cas de congestion elles sont éliminées sans qu'aucun mécanisme d'avertissement de la source, ni de demande de ralentissement de débit ne soit mis en œuvre. La classe UBR convient aux applications de type messagerie et sauvegarde à distance (*Remote backup*).

La figure 14.59 illustre comment la bande passante d'un conduit peut être partagée entre les différentes classes de service.

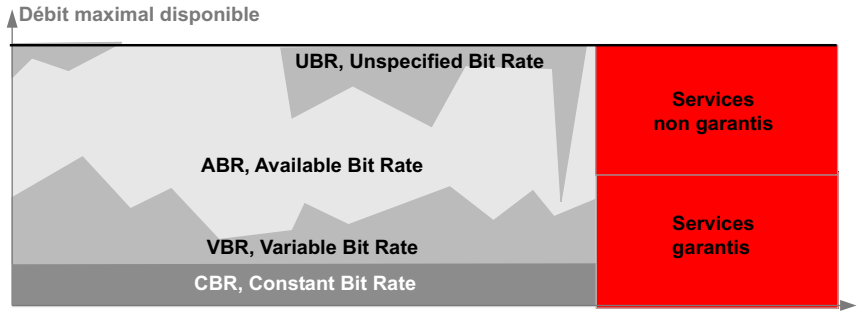


Figure 14.59 Le partage de la bande passante selon la classe de service.

Le contrat de service

Le contrat de service (*Connection Trafic Descriptor*) définit en termes de qualité de service (QoS) et de paramètres de trafic les caractéristiques de la connexion demandée. Trois variables définissent la qualité de service. Ce sont :

– **CTD** (*Cell Transfert Delay*) qui exprime le temps maximal garanti au transfert de bout en bout d'une cellule par le réseau.

– **CDV** (*Cell Delay Variation*) qui fixe la borne maximale des variations de temps de transfert des cellules (gigue), ce paramètre n'est précisé que pour les transferts de flux isochrone.
– **CLR** (*Cell Loss Ratio*) qui définit un taux de perte maximal des cellules transmises (CLR = nombre de cellules perdues/nombre de cellules transmises).

Les paramètres de trafic sont :

– **PCR** (*Peak Cell Rate*) qui correspond au débit maximal qui sera soumis par la source et accepté par le réseau (débit de crête).
– **SCR** (*Sustainable Cell Rate*) qui précise le débit moyen envisagé soumis au réseau par cette connexion.
– **MBS** (*Maximum Burst Size*) qui définit la taille maximale des rafales admissibles par le réseau.
– **MCR** (*Minimum Cell Rate*) qui spécifie le débit minimum garanti par le réseau.

La figure 14.60 indique, en fonction de la classe de service invoquée, les paramètres valides.

		Classes de service				
Paramètres		CBR	VBR-rt	VBR-nrt	ABR	UBR
Paramètres de QoS						
CTD	*Cell Transfert Delay*	•	•	•		
CDV	*Cell Delay Variation*	•	•			
CLR	*Cell Loss Ratio*	•	•	•	•	
Paramètres de trafic						
PCR	*Peak Cell Rate*	•	•	•	•	
SCR	*Sustainable Cell Rate*		•	•		
MBS	*Maximum Burst Size*		•	•		
MCR	*Minimum Cell Rate*				•	

Figure 14.60 La relation entre les paramètres du contrat de service et la classe de service.

14.3.6 Le contrôle de flux et de congestion

Les mécanismes

Un réseau ATM est un réseau de files d'attente et comme tel, sensible à la congestion. Les mécanismes mis en œuvre pour la prévenir et y remédier sont similaires à ceux utilisés dans le Frame Relay :

– élection de cellules à détruire en priorité en cas de congestion (bit **CLP**, *Cell Los Priority*). Le bit CLP peut être positionné à 1 par la source ou par tout commutateur si le flux, sur le circuit virtuel, dépasse le débit autorisé. CLP à 1 indique les cellules à écarter en priorité ; à 0, il identifie les cellules de priorité haute ;
– contrôle d'admission d'une nouvelle connexion dans le réseau (**CAC**, *Connection Admission Call*). Il consiste à n'accepter une nouvelle connexion que si celle-ci peut être satisfaite en terme de qualité de service requise sans préjudice de la qualité de service garantie aux connexions déjà actives ;

© Dunod – La photocopie non autorisée est un délit

– contrôle du débit de la source (**UPC**, *User Parametre Control*. Il consiste à surveiller en permanence le débit de la source par rapport à un contrat de service défini à la connexion (SVC) ou à l'abonnement (PVC).

Le contrôle du débit de la source (UPC) définit trois niveaux :

– le trafic est conforme au contrat de service, les cellules sont transmises ;
– le trafic est supérieur au contrat de trafic, les cellules sont marquées. Le bit CLP est positionné par le commutateur (*Cell tagging*). Les cellules marquées (CLP = 1) seront détruites si le flux traverse un commutateur en état de congestion ;
– le trafic est supérieur au contrat de service et le réseau est en état de congestion, les cellules sont alors éliminées (*Cell discarding*).

Le contrôle de congestion explicite

À l'instar du Frame Relay, l'ATM met en place un système d'information de l'état de congestion (**EFCN**, *Explicit Forward Congestion Notification*). Le mécanisme est similaire, lorsqu'un commutateur est en état de congestion (seuil de remplissage des *buffers*), il positionne le bit **EFCI** (*Explicit Forward Congestion Indication*) du champ **PTI** (*Payload Type Identification*). Le destinataire du flux est alors informé que les cellules ont traversé un commutateur en état de congestion (figure 14.61).

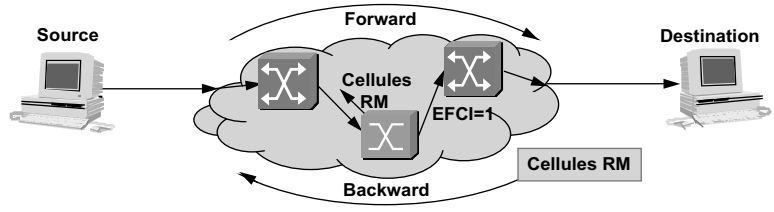


Figure 14.61 Le mécanisme de signalisation de la congestion.

Le destinataire envoie alors à la source des cellules spécifiques pour l'informer de cet état et lui demander de réduire son débit (cellules **RM**, *Ressource Management*), cette méthode est dite : **BECN** (*Backward Explicit Congestion Notification*). Les commutateurs en état de congestion peuvent de même, insérer des cellules RM dans les flux en direction de leurs usagers pour leur demander de réduire leur débit (cellules RM dites **RR**, *Relative Rate*) ou les informer explicitement du débit disponible (cellule RM dites **ECR**, *Explicit Cell Rate*).

14.3.7 La signalisation et le routage

Généralités

La signalisation concerne l'ensemble des procédures destinées à l'établissement dynamique, au maintien et à la fermeture d'une connexion virtuelle commutée. Compte tenu des éléments à prendre en compte, notamment la qualité de service (QoS), la signalisation ATM est relativement complexe. De type **CCS** (*Common Channel Signaling*) ou signalisation par canal sémaphore, elle diffère selon que l'on se situe à l'interface usager d'un réseau public ou privé, à l'interface entre deux réseaux privés ou publics (figure 14.62).

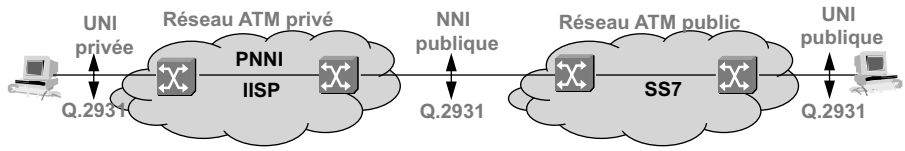


Figure 14.62 La signalisation dans ATM.

L'établissement du circuit virtuel

En mode commuté, l'établissement d'un SVC est préalable à tout envoi de données. Le message de signalisation *Setup* est émis par l'appelant, il comporte tous les éléments nécessaires à l'établissement d'un SVC (bidirectionnel). Compte tenu de sa taille, ce message est composé de plusieurs cellules ATM émises sur le VPI/VCI réservé : 0/5.

Le message *Setup* est acheminé par le réseau qui détermine le meilleur chemin en fonction de la QoS requise. Le message *Call Proceeding* indique à l'émetteur que sa demande a bien été prise en compte, qu'elle est acceptée par le commutateur d'accès et que celui-ci transmet sa requête. Si la connexion est acceptée de bout en bout, le message est acquitté par le message *Connect* qui fixe le couple VPI/VCI à utiliser. La figure 14.63 présente le diagramme d'échange de messages lors de l'établissement et de la rupture d'un SVC. Le message *Setup* contient toutes les informations nécessaires à l'établissement du SVC :

– L'adresse source et destination.
– La bande passante demandée (**UCR**, *User Cell Rate*).
– La QoS par indication de la classe de service (CBR, VBR, ABR, UBR).
– Le type d'AAL requis.

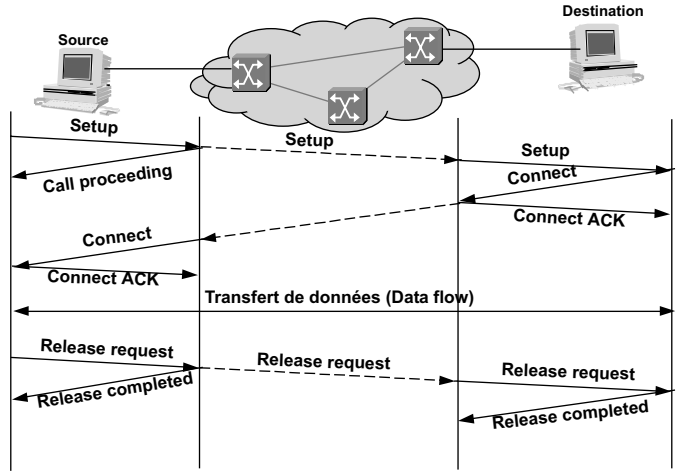


Figure 14.63 Le diagramme des messages d'établissement.

Le routage PNNI

PNNI (*Private Network to Network Interface*) est un protocole de routage du type état des liens (*Link status*). Pour établir un SVC répondant à la QoS exigée, chaque commutateur doit avoir

© Dunod – La photocopie non autorisée est un délit

connaissance de la topologie du réseau et des caractéristiques de trafic disponibles sur les différents commutateurs du réseau :

– Débit disponible (*Available Cell Rate*).
– Délai de transfert (*Maximum Cell Transfer Delay*).
– Variation du délai de transfert ou gigue (*Cell Delay Variation*).
– Taux de perte de cellules (*Cell Loss Ratio*).
– Débit maximal admissible (*Maximum Cell Rate*).

Pour éviter un échange d'information prohibitif, PNNI segmente le réseau en groupes de commutateurs hiérarchisés (*Peer group*). Un *peer group* est constitué d'un ensemble de nœuds logiques (les nœuds physiques sont les nœuds réels au plus bas de la hiérarchie). Dans chaque groupe, un commutateur maître est désigné. Chaque commutateur informe le maître de son état et récupère auprès de celui-ci les informations sur l'état des autres membres du groupe, de ce fait tous les membres du groupe ont une vision identique du groupe. Chaque commutateur maître du niveau *N* appartient au *peer group* du niveau *N*+1, cette double appartenance permet au maître de renseigner ses homologues de la topologie du groupe subordonné. De même, chaque commutateur du niveau *N* est informé de la topologie des autres groupes par son maître. Chaque commutateur dispose alors d'une cartographie simplifiée du réseau à partir de laquelle il va effectuer un routage à « tâtons ». La figure 14.64 schématise cette architecture.

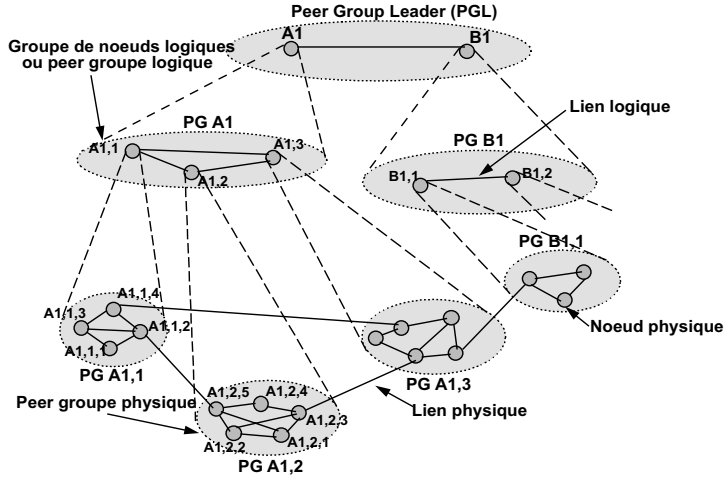


Figure 14.64 L'architecture logique du réseau selon PNNI.

En fonction de la qualité de service requise par la demande d'établissement, le commutateur d'accès effectue un contrôle d'admission (**CAC**, *Connection and Admission Control*). Si le commutateur d'entrée peut accepter la connexion, à partir de sa connaissance de l'état du réseau, il établit une liste spécifique de routage (**DTL**, *Designated Transit List*) contenant les commutateurs répondant aux exigences de la demande. Le commutateur transmet alors la demande au commutateur suivant en y annexant la liste de routage (routage similaire à un routage par la source).

Chaque commutateur de la liste effectue un contrôle d'admission, s'il accepte la demande il la transmet au suivant dans la liste de routage. S'il ne peut accepter celle-ci (son état est différent de

l'état connu par le commutateur source), il réachemine la demande vers le commutateur précédent qui recalcule une route (*Crank back fonction).*

L'adressage dans les réseaux ATM

La fonction essentielle d'un processus de routage est de mettre en relation deux entités adressées, ce qui nécessite, en principe qu'elles appartiennent au même espace d'adressage. Ce n'est pas toujours le cas pour les réseaux ATM. L'adressage dans les réseaux publics utilise le format E.164 de l'UIT (15 chiffres), tandis que l'adressage dans les réseaux privés supporte deux types d'adressage différents : les adresses NSAP (ISO) et une extension de l'adressage E.164.

Les adresses privées ATM, définies par l'ATM Forum, comportent deux parties, l'une identifie le réseau de raccordement (*Network prefix* ou préfixe réseau) c'est-à-dire l'adresse WAN, l'autre à la disposition de l'utilisateur identifie le système d'extrémité (**ESI**, *End System Identifier*) et l'application utilisateur (**SEL**, *SELector field*).

La figure 14.65 représente le format général des adresses privées utilisées dans ATM. Le champ **AFI** (*Autority Format Identifier*), sur un octet, indique l'autorité de gestion et le format utilisé pour représenter l'adresse.

AFI 1 octet	**IDI** 2 octets	**DSP** 17 octets		
39	DCC	Adresse réseau	ESI	SEL
47	IDC	Adresse réseau	ESI	SEL
45	Adresse E164 codé NSAP 8 octets	Sous-adresse 4 octets	ESI 6 octets	SEL 1 octet

Figure 14.65 La structure des adresses privées ATM.

Les adresses **DCC** (*Data Country Code*) et **IDC** (*International Designator Code*) sont réservées à l'adressage des réseaux ATM des opérateurs privés, tandis que les adresses au format E.164 peuvent être vus, chez la personne privée, comme une extension de l'adressage du réseau public (sous-adresse privée).

Le champ **IDI** (*Initial Domain Identification*), sur deux octets, spécifie le domaine d'adressage. Enfin, le champ **DSP** (*Domain Specific Part*) correspond à l'adresse effective du terminal.

14.3.8 L'administration des réseaux ATM

L'ATM Forum n'a pas retenu, pour l'administration des réseaux ATM, les principes énoncés par l'ISO. Il a défini un protocole **ILMI** (*Interim Local Management Interface*) s'appuyant sur le protocole **SNMP** (*Simple Network Management Protocol*).

Le protocole **ILMI** (*Interim Local Management Interface*), introduit par la RFC 1695, fournit les informations de statut, de configuration et de diagnostic du système, il est aussi utilisé pour l'enregistrement d'adresse (extension du protocole).

Basé sur les agents SNMP et l'AAL5, ILMI utilise les commandes SNMP sur un VCC (*Virtual Circuit Connection*) réservé (VPI/VCI : 0/16). La figure 14.66 illustre l'architecture du système d'administration.

© Dunod – La photocopie non autorisée est un délit

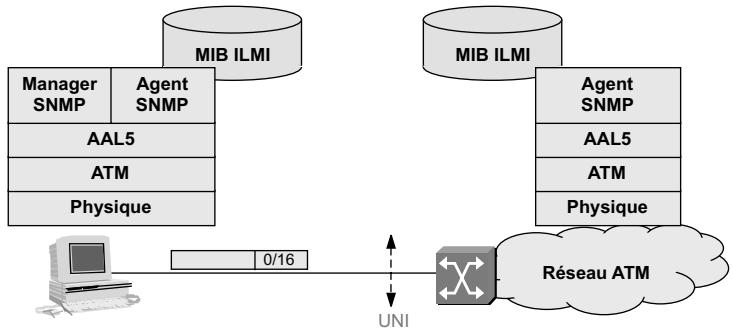


Figure 14.66 L'administration des réseaux ATM.

Une extension de la MIB[7] (*Management Information Base*) ILMI, la MIB ATM autorise l'accès aux informations des commutateurs ATM.

14.4 CONCLUSION

Autorisant un partage optimal de la bande passante, l'ATM est le protocole de cœur de réseau utilisé par la majorité des opérateurs actuels, le Frame Relay est aujourd'hui cantonné aux réseaux privés et à l'accès aux réseaux ATM alors qu'X.25, pour des raisons de compatibilité avec les existants ne subsiste plus que dans quelques réseaux privés et les liaisons d'accès à certains réseaux publics.

Cependant l'évolution des besoins s'oriente plus vers le respect par le réseau des exigences en termes de qualité de service plus qu'en débit absolu. Cette exigence impose l'intégration de mécanismes de qualité de service (QoS) dans les composants du réseau et des mécanismes spécifiques dans les applications pour les invoquer. La qualité de service est prise en compte dans ATM par la notion de classe de service, dans IP avec l'intégration de DiffServ et dans les réseaux locaux par l'approche 802.1p. La pluralité de normes et de protocoles d'origines différentes engendre de véritables difficultés pour obtenir la qualité de service de bout en bout (figure 14.67).

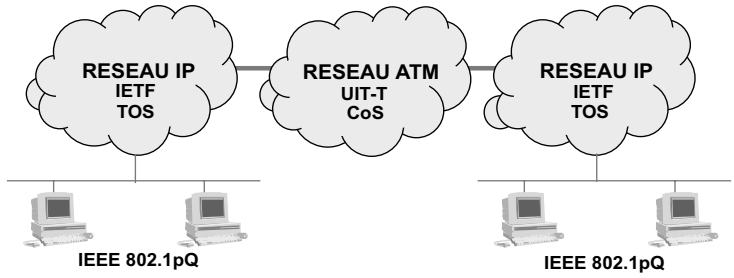


Figure 14.67 La problématique de la QoS de bout en bout.

Le quasi monopole des applications IP engendre un besoin de réseau tout IP. C'est l'un des objectifs de MPLS (*MultiProtocol Label Switching*) que d'offrir aux applications IP un service de type IP de bout en bout sur les infrastructures réseaux existantes.

7. Une MIB est un ensemble d'informations d'administration réseau.

EXERCICES

Exercice 14.1 Reconstitution d'un paquet d'appel

Reconstituez le paquet d'appel émis par une station vers un ETTD distant. L'adressage utilisé est du type X.121, l'ETTD est relié au réseau par une LS (valeur 1) : ligne 89 sur le commutateur 1 du département de la Seine (75). Les services complémentaires suivants seront invoqués :

- facturation à l'appelé ;
- GFA valeur locale 3 ;
- négociation de la taille des paquets, 64 en émission, 128 en réception ;
- négociation de la taille fenêtre, 2 en réception, 7 en émission.

On supposera que le réseau n'utilise qu'une numérotation des paquets modulo 8. On admettra que l'appel est le premier émis par l'ETTD dont l'abonnement comporte 20 CV. L'opérateur utilise un format d'adresse du type :

<mode d'accès (1 quartet), département (2 quartets), commutateur (2 quartets), ligne abonné (4 quartets)>

Les valeurs entre parenthèses indiquent la longueur du champ en quartets.

Exercice 14.2 Dialogue X.25

À l'aide de la trace du niveau physique représentée figure 14.68, reconstituez et commentez le dialogue entre l'ETTD et le réseau.

Ligne	Origine	Champ
1	ETCD	7E 01 0F 68 B9 7E
2	ETCD	7E 01 0F 68 B9 7E
3	ETCD	7E 01 0F 68 B9 7E
4	ETTD	7E 01 3F EB 7F 7E
5	ETCD	7E 01 73 83 5E 7E
6	ETCD	7E 03 00 10 00 FB 07 A4 EA 6F 7E
7	ETTD	7E 03 21 A4 56 7E
8	ETTD	7E 01 20 10 00 FF 8D 06 7E
9	ETCD	7E 01 21 14 98 7E
10	ETTD	7E 01 22 10 03 0B 09 19 20 20 59 30 02 01 01 C4 01 00 67 89 7E
11	ETCD	7E 01 41 12 14 7E
12		7E 03 42 10 03 0F 70 A9 7E
13	ETTD	7E 03 41 A2 DA 7E
14	ETTD	7E 01 44 10 03 00 E0 00 00 01 00 20 08 00 10 00 C2 00 50 49 00 08 08 00 00 00 50 52 00 08 00 00 0E 60 50 6B 00 14 02 00 00 23 01 00 10 01 18 50 C9 05 00 00 00 00 01 24 7E

Figure 14.68 La trace X.25.

© Dunod – La photocopie non autorisée est un délit

Exercice 14.3 Définition d'un protocole

Vous avez été recruté par un nouvel opérateur afin de participer à la conception de son réseau national. Après avoir défini la topologie du réseau, il vous reste à préciser l'aspect protocolaire. À cet effet, on vous demande de réfléchir aux points suivants :

1. Sachant que le temps théorique de transfert d'un message de longueur L en commutation de paquets est donné par la relation :

$$Tp = \frac{L + pH}{D}\left(1 + \frac{N}{p}\right)$$

où L est la longueur du message en bits,
p le nombre de paquets,
H la taille en bits des données protocolaires,
N nombre de nœuds traversés (nœuds origine et destination non compris),
D débit en bit/s.

On vous demande de déterminer la taille optimale de l'unité de données (temps de traversée du réseau minimal). Pour cela on formule les hypothèses suivantes :

- Tous les clients sont raccordés *via* une interface 802.3, on admettra que la longueur du message utilise au maximum les capacités de transfert du réseau local (MTU de la trame 802.3, 1 500 octets).
- La topologie du réseau WAN est telle qu'un paquet traverse en moyenne 3,25 nœuds.
- Les données de services du protocole WAN seront limitées à 5 octets.
- On ne retiendra que la valeur entière du résultat final.

2. Le réseau offrira un service en mode connecté, on envisage d'utiliser un contrôle de flux du type Stop and Wait. C'est-à-dire que, dès qu'un nœud reçoit un paquet saturant, il envoie à la source une demande d'arrêt d'émission. Le contrôle de flux sera instauré, d'une part entre le nœud client et le nœud d'accès au réseau (contrôle de flux à l'interface usager) et, d'autre part entre les nœuds du réseau. Est-il réaliste d'instaurer de tels mécanismes sachant que :

- En interne au réseau :
  - La distance moyenne séparant deux nœuds est de 100 km.
  - Le débit interne du réseau de 622 Mbit/s.
  - La vitesse de propagation des données sera supposée être de $2 \cdot 10^8$ m/s.
- À l'interface usager :
  - La distance maximale de la liaison d'abonnée est estimée à 20 km
  - Le débit maximal offert à l'usager est de 2,048 Mbit/s

On admettra que le temps de traitement par les nœuds des unités de données est négligeable.

3. Combien de connexions simultanées (CV) le réseau peut accepter si on a réservé, dans les 5 octets d'en-tête, 28 bits à l'espace d'adressage ?

4. On admet que **chacun** des liens est affecté d'un taux d'erreur binaire de $Teb = 10^{-9}$

a) Quelle est la probabilité qu'un paquet arrive à destination sans erreur (9 décimales) ?
b) Avec au moins 1 bit erroné (9 décimales) ?

5. Compte tenu de la probabilité d'erreur relativement importante. Est-il possible de garantir, même à charge constante, aux utilisateurs un temps de traversée du réseau borné et une gigue nulle ?
6. Vous envisagez des accès *via* le réseau téléphonique. Quel sera le débit maximal possible par ce moyen d'accès compte tenu des données suivantes :

   Le rapport signal à bruit moyen du RTC est de 10^3.
   Le RTC est équipé de filtres (bande passante téléphonique normalisée).

Vous comptez utiliser des modems dont les différents instants significatifs sont repérés à 0, $\pi/4$, $\pi/2$, $3\pi/4$, π, $5\pi/4$, $3\pi/2$, $7\pi/4$, chaque vecteur pouvant être défini à +3V ou +1V. Est-ce réalisable, quel serait le débit du modem réalisé ?

Exercice 14.4 Protocole ATM

Pourquoi, l'utilisation de la liaison virtuelle identifiée VPI/VCI 0/0 est-elle interdite pour transmettre des unités de données d'administration, de signalisation ou usagers ?

Exercice 14.5 Priorité ou réservation de ressources

La notion de classes de service d'ATM est relativement complexe à mettre en œuvre, les systèmes à priorité sont plus faciles à implémenter. Quel est, d'après vous, le meilleur système pour garantir une qualité de service, notamment pour les flux isochrones ?

Exercice 14.6 Évolution de l'encapsulation d'IP

Complétez la figure 14.69 qui résume les différentes possibilités d'encapsulation du protocole IP pour en assurer le transport sur un réseau WAN.

Type d'encapsulation	Mise en œuvre	Caractéristiques
IP/ATM/SDH/WDM		
IP/SDH/WDM		
IP/WDM		

Figure 14.69 L'encapsulation IP.

Chapitre **15**

MPLS, *Multiprotocol Label Switching*

15.1 GÉNÉRALITÉS

Les applications informatiques s'appuient essentiellement sur le protocole TCP/IP. Les données sont généralement transportées par encapsulation dans un protocole en mode connecté (X.25, Frame Relay ou ATM). Indépendamment des problèmes de mise en relation des espaces d'adressage et de la difficulté du respect de la qualité de service de bout en bout, la gestion (établissement, maintien et rupture) des circuits virtuels conduit à des solutions plus ou moins complexes. **MPLS** (*MultiProtocol Label Switching*) pallie cette rupture de technologie, il offre un service en mode connecté transparent aux applications IP. En fait, MPLS migre un réseau IP routé en un réseau IP commuté, il associe la souplesse du routage de niveau 3 à l'efficacité de l'acheminement de niveau 2. C'est un protocole de conciliation généralement présenté comme un protocole de niveau 2-5 (figure 15.1).

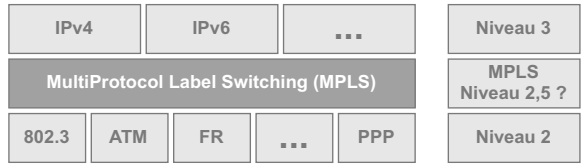


Figure 15.1 Le modèle de référence et l'architecture MPLS.

15.2 PRINCIPE

MPLS substitue un protocole de routage IP (RIPv2, OSPF, BGP) au protocole de signalisation propre au réseau de transport. À chaque route identifiée par le protocole de routage, MPLS associe un label (référence de commutation). Chaque datagramme IP se voit, en entrée du réseau MPLS et en fonction de l'adresse destination (fonction de routage) attribuer un label. Par la suite dans le réseau, le datagramme sera acheminé en fonction de ce label (commutation). Ainsi, un réseau MPLS associe deux fonctions : routage en périphérie et commutation en cœur de réseau (figure 15.2).

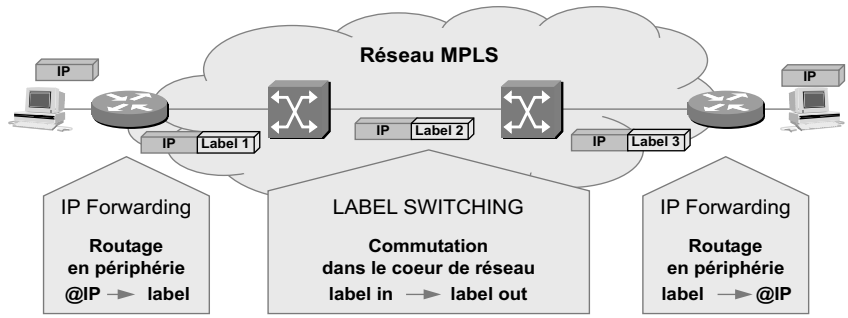


Figure 15.2 Les fonctions de base du réseau MPLS.

15.3 LE RÉSEAU MPLS

15.3.1 Le commutateur MPLS

Un réseau MPLS est constitué d'un ensemble de commutateurs MPLS. Un commutateur MPLS ou *Label Switching Router* (**LSR**) correspond à l'association d'un routeur et d'un commutateur. La figure 15.3 présente la structure d'un tel commutateur. En principe un commutateur Frame Relay ou ATM peut évoluer en commutateur MPLS par une simple mise à jour du logiciel.

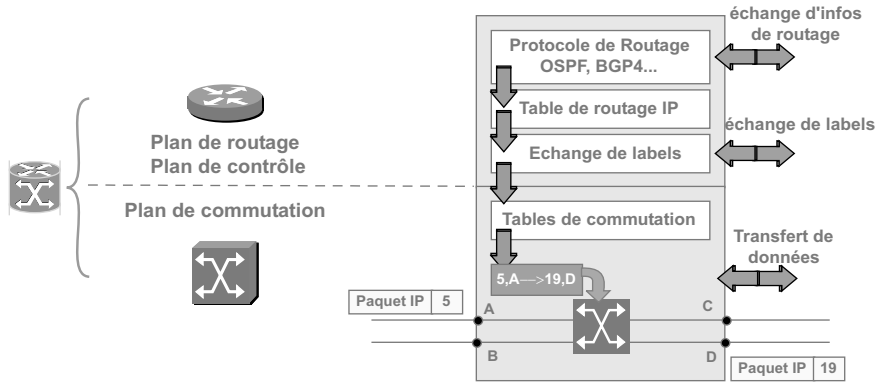


Figure 15.3 La structure d'un Label Switching Router (LSR).

Le plan de routage ou plan de contrôle met en œuvre un protocole de routage IP, un label est affecté à chaque adresse IP pouvant être jointe. Un protocole spécifique distribue les labels aux LSR voisins (**LDP**, *Label Distribution Protocol*). Le datagramme IP labelisé en entrée du réseau (paquet MPLS) est ensuite commuté de manière similaire à la commutation traditionnelle (*Port In, Label In → Port out, Label Out*). Les labels sont affectés en fonction d'un nœud de sortie et non d'une adresse IP destination. Tous les paquets à destination d'un même nœud de sortie reçoivent le même label et subissent donc le même traitement dans le réseau. Ce principe appelé agrégation de routes à la périphérie allège les tables d'acheminement et participe à l'amélioration des performances.

15.3.2 Le principe de base d'un réseau MPLS

L'agrégation de route à la périphérie rend plus aisée la croissance du réseau. L'augmentation du nombre de sites raccordés est transparente au cœur du réseau, seuls les organes de périphéries sont affectés (accroissement éventuel du nombre de LSR de périphérie). Les LSR de périphérie ou *Label Edge Router* (**LER**) sont à l'interface entre le réseau IP et le réseau MPLS. La figure 15.4 illustre le principe de l'agrégation de routes en périphérie.

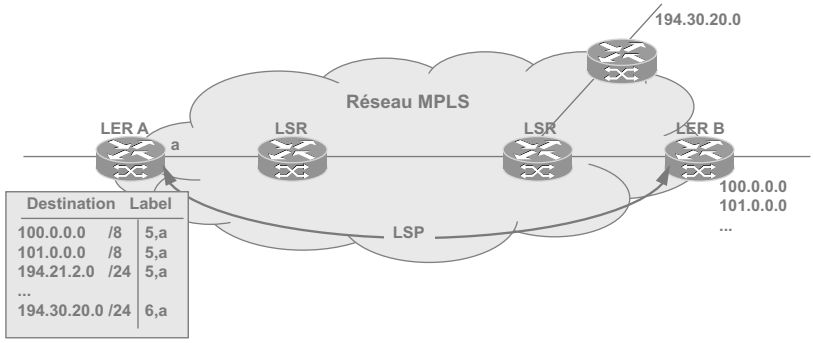


Figure 15.4 Principe de l'agrégation de routes en périphérie.

Dans le réseau de la figure 15.4, toutes les adresses réseaux connues du LER B reçoivent en entrée le même label. L'ensemble des datagrammes qui reçoit un même label forme une **FEC** (*Forwarding Equivalence Class*). Le circuit virtuel défini pour une classe d'équivalence est appelé **LSP** (*Label Switched Path*). Le LSP « aller » et le LSP « retour » sont définis indépendamment l'un de l'autre, de ce fait, les voies aller et retour peuvent donc être différentes (équilibrage de charge, qualité de service...). La figure 15.5 illustre le traitement d'un datagramme IP entre son entrée dans le réseau MPLS et sa sortie.

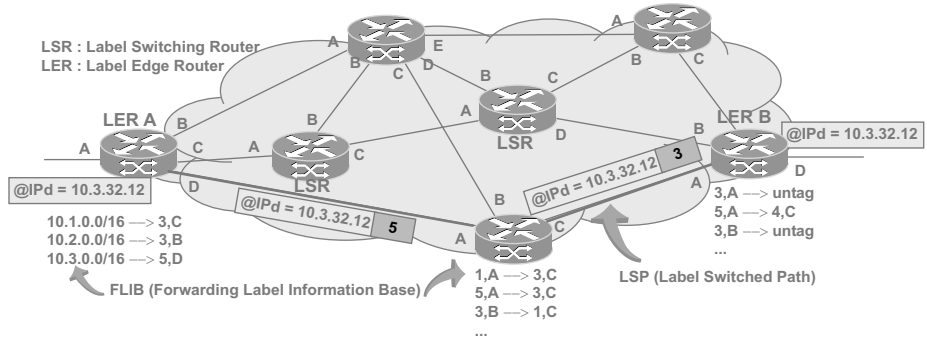


Figure 15.5 L'acheminement d'un datagramme IP dans un réseau MPLS.

Le LER A *(MPLS ingress node)*, recevant le datagramme IP consulte sa table de labels (**FLIB**, *Forwarding Label Information Base*). Pour l'adresse IP 10.3.32.12, le label affecté est 5 et le port de sortie D. Le datagramme est labelisé 5 (*Push tag*). Le LER suivant reçoit sur son port A, un paquet MPLS labelisé 5, il consulte sa table de labels (FLIB), dans laquelle il est indiqué qu'il doit changer le label en 3 et commuter le paquet MPLS en C. À l'instar des autres systèmes reposant sur la notion de circuits virtuels, le label n'a qu'une valeur locale, il est modifié par chaque nœud (*Swap tag*). Enfin, le LER de sortie (*MPLS egress node*) examine sa FLIB et constate qu'il doit

© Dunod – La photocopie non autorisée est un délit

supprimer le label (*Untag*), il consulte alors sa table de routage IP et achemine le datagramme IP sur le port de sortie D.

Dans un réseau MPLS, un même paquet MPLS peut recevoir plusieurs labels (*Push tag*). L'empilement de labels permet notamment de définir une agrégation de routes en interne dans le réseau et des réseaux virtuels (**VPN**, *Virtual Private Network*). L'opération *Pop tag* permet de supprimer le label de haut de pile, alors que *Untag* supprime le dernier label.

15.3.3 Les mécanismes particuliers

Le dépilement du pénultième saut

Dans le réseau de la figure 15.5, le LER de sortie dit aussi « *egress* LER » effectue une double consultation. La LFIB lui indique de supprimer le dernier label (*Untag*), puis la table de routage IP d'acheminer le datagramme vers le prochain routeur IP (sortie du domaine MPLS). Entre le dernier LSR et le LER aucune opération ne nécessite la présence d'un label. Afin d'optimiser le travail du LER de sortie, c'est l'avant-dernier LSR traversé qui supprime le label (**PHP**, *Penultimate Hop Popping*). La figure 15.6 illustre ce principe. C'est l'identification du protocole supérieur contenu dans l'unité de données du niveau liaison qui permet d'identifier le contenu et de déterminer si un « tag » MPLS est présent ou non.

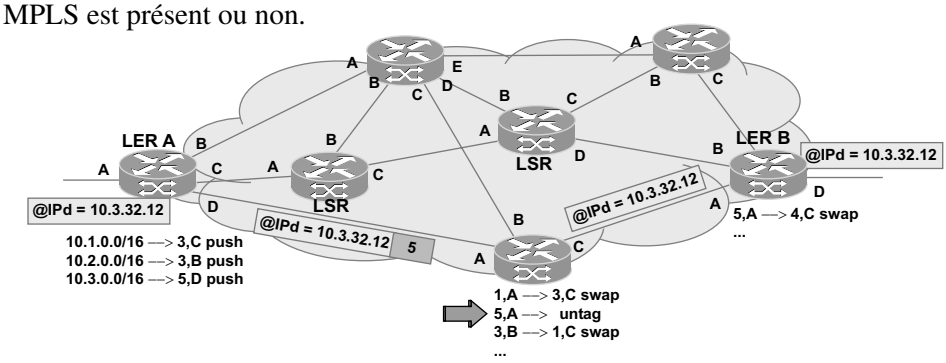


Figure 15.6 Le dépilement du pénultième saut.

L'agrégation de routes dans le réseau

La figure 15.7 illustre le principe de l'agrégation de routes, les flux A, B et C partagent un même chemin.

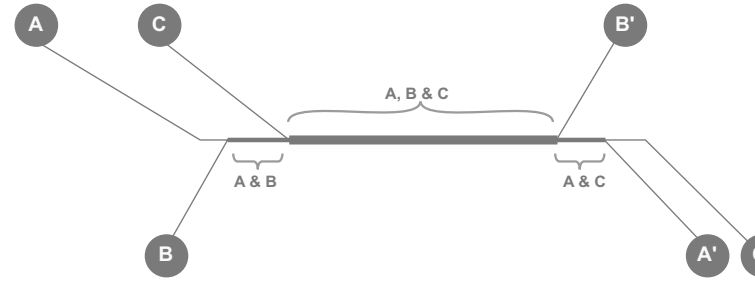


Figure 15.7 Principe de l'agrégation de routes.

Les tables de commutation seraient allégées si, pour ces flux, un seul label était attribué. Il reste cependant nécessaire de pouvoir les distinguer lorsque les chemins se séparent.

À cet effet, à chaque fois que plusieurs flux partagent le même chemin, un label supplémentaire, identifiant ce parcours commun, est ajouté aux paquets MPLS (*Push tag),* il est extrait (*Pop tag*) à la sortie du tronc commun. La figure 15.8 illustre les opérations sur les labels lors d'une agrégation de routes en interne.

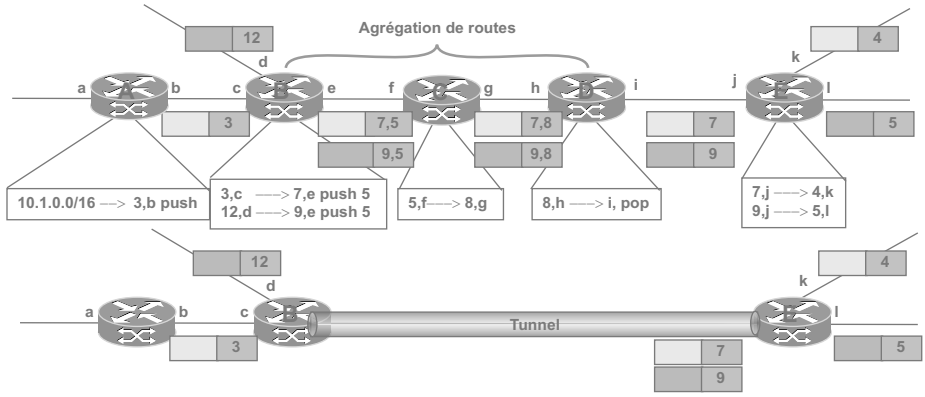


Figure 15.8 L'opération sur les labels lors d'une agrégation de routes.

L'agrégation de routes ou routage hiérarchique est assimilable à la réalisation d'un tunnel entre le LSR de convergence des routes et celui d'éclatement. Le LSR d'entrée attribue un label d'identification à chaque flux, ici 7 et 9 puis un label de tunnel 5. Dans le trajet, seul le label de tunnel peut être modifié. Ce label est extrait par l'avant-dernier LSR du tunnel (dernière opération de commutation collective).

L'encapsulation ou l'en-tête MPLS

➤ L'en-tête MPLS, la *shim header*

Hors le champ label sur 20 bits, l'en-tête MPLS ou *shim header* (figure 15.9) permet de gérer différents niveaux de priorité (champ Exp pour *Experimental*). Le bit S (*Stack*) indique la fin de pile (S = 1, dernier label). Le champ TTL (*Time To Live*) permet de rendre transparent, à IP, la traversée d'un réseau MPLS. En entrée du réseau, le LER *ingress* recopie la valeur du TTL du datagramme IP dans l'en-tête MPLS, le réseau MPLS décrémente le TTL de la même manière que l'aurait fait un réseau IP. En sortie, le LER *egress* recopie cette valeur dans le datagramme de sortie.

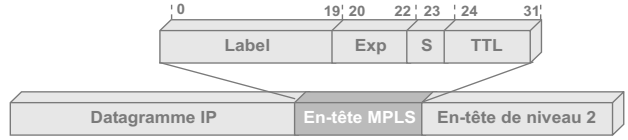


Figure 15.9 Le format de l'en-tête de compensation MPLS.

© Dunod – La photocopie non autorisée est un délit

➤ MPLS et les protocoles de niveau 2

La principale difficulté de l'encapsulation de paquets MPLS dans les protocoles de niveau liaison est en relation directe avec la MTU de ces protocoles. La figure 15.10 illustre ces encapsulations. Dans le cas du protocole PPP (*Point to Point Protocol*), celui-ci utilise des trames de taille fixe négociées par le protocole LCP (*Logical Control Protocol*) lors de l'établissement de la connexion PPP. L'insertion de labels a pour conséquence directe l'accroissement de la taille de la trame. Les différents LSR doivent avoir la capacité de fragmenter la trame PPP si celle-ci dépasse une valeur prédéterminée (*Max IP Datagram Size for Labelling*). Le champ TTL de l'en-tête MPLS n'est renseigné que dans le premier en-tête MPLS à partir de la valeur champ TTL du datagramme IP. La valeur modifiée par chaque LSR traversé est recopiée dans le champ TTL du datagramme IP par le LER de sortie.

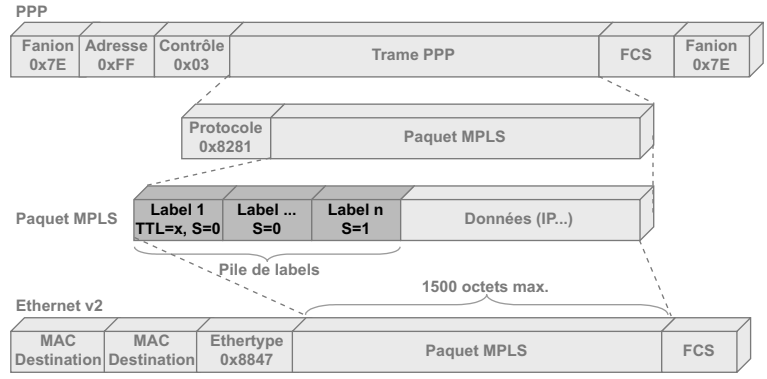


Figure 15.10 MPLS et les protocoles de niveau 2.

De même, la taille maximale des trames Ethernet est limitée par la carte transporteur à 1 518 octets (1 500 utiles). En conséquence, l'utilisation de MPLS au-dessus d'Ethernet nécessite une modification de ce protocole. En l'absence de normalisation, certains constructeurs ont porté cette taille à 1 526 octets (1 518 plus deux en-têtes MPLS). Si Ethernet v2 peut être adapté pour admettre l'encapsulation de paquets MPLS, il n'en est pas de même de la version de l'IEEE (802.3). En effet, en 802.3 une valeur du champ protocole supérieure à 1 500 indique qu'il s'agit d'Ethernet v2 !

15.4 MPLS ET LES INFRASTRUCTURES EXISTANTES

15.4.1 Généralités

Lorsque MPLS est utilisé sur une infrastructure de commutation traditionnelle, celui-ci utilise les techniques de la technologie sous-jacente, cette possibilité confère à MPLS une grande facilité d'adaptation puisqu'il ne remet pas en cause les investissements réalisés. Dans ces réseaux, la valeur du premier label MPLS affecté est utilisée comme étiquette de commutation : DLCI pour le Frame Relay ou VPI/VC pour les réseaux ATM (figure 15.11). Un protocole de routage IP traditionnel et un protocole de distribution des labels se substituent à la signalisation d'origine.

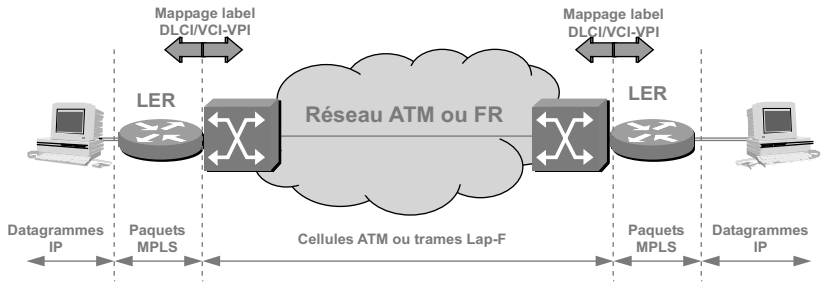


Figure 15.11 MPLS et les infrastructures réseaux.

15.4.2 La gestion du TTL

Le champ TTL (*Time To Live*) permet de limiter les conséquences d'un bouclage dans le réseau. Fixée par la source, la valeur du TTL est décrémentée par chaque nœud traversé. Lorsque la valeur du TTL vaut 0, le datagramme est éliminé. Le réseau MPLS doit avoir le même comportement. En sortie d'un réseau MPLS, le TTL du datagramme IP doit avoir la même valeur que s'il avait traversé un réseau IP (figure 15.12). Ce mécanisme n'est pas possible sur des infrastructures Frame Relay et ATM puisque l'en-tête de commutation Frame Relay et ATM ne contenant aucun champ similaire au TTL, le réseau MPLS n'a pas accès à cette information.

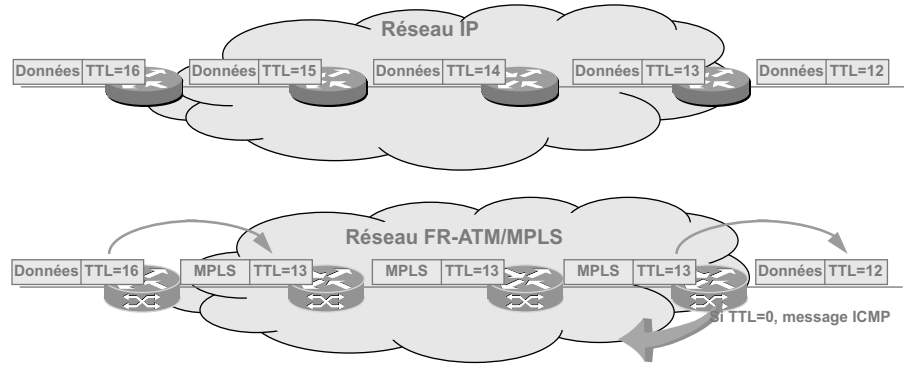


Figure 15.12 Le mécanisme du TTL.

Dans ces deux types d'infrastructure, le nombre de sauts est déterminé par le protocole de distribution des labels. Le champ TTL de l'en-tête MPLS est décrémenté du nombre de sauts dans le réseau par l'*ingress* LER (LER d'entrée), puis transmis de manière transparente dans le réseau. L'*egress* LER (LER de sortie), décrémente de 1 la valeur du TTL reçu et la recopie dans le datagramme IP. Dans le cas où la valeur du TTL deviendrait nulle, que cette valeur soit le fait du LER d'entrée ou de sortie, le réseau MPLS doit, à l'instar d'un réseau IP traditionnel, émettre un message ICMP à destination de la source.

15.4.3 MPLS et ATM

Les encapsulations d'IP dans le Frame Relay et dans ATM sont régis par RFC 1490 (encapsulation SNAP pour le FR) et la RFC 1483 (ATM). La figure 15.13 illustre l'encapsulation ATM de la

© Dunod – La photocopie non autorisée est un délit

RFC 1483. Le paquet MPLS est segmenté en cellules ATM, la segmentation de l'AAL5 est gérée par le dernier bit du champ *Payload Type* de la cellule ATM qui est positionné à 1 dans la dernière cellule. Le label de tête de pile non utilisé par l'ATM-LSR *egress* est positionné à 0. Le champ VPI/VCI est renseigné à partir du protocole de distribution de labels.

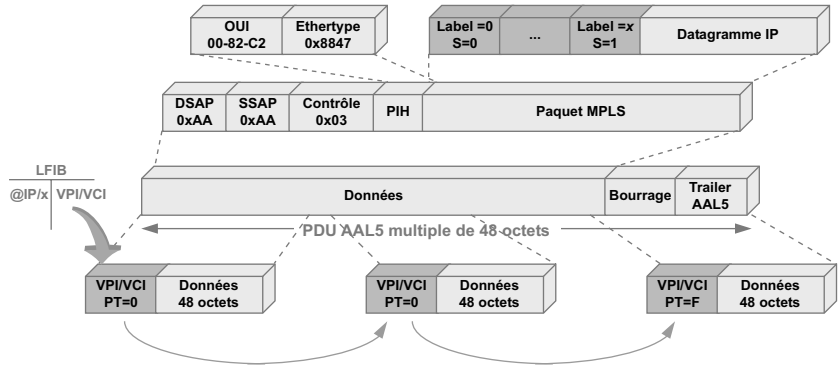


Figure 15.13 Le transport d'un paquet MPLS dans un réseau ATM.

Dans un réseau ATM traditionnel, seules les données d'une même source sont acheminées sur un circuit virtuel (**VC**, *Virtual Channel*), alors que dans un réseau ATM/MPLS, si un commutateur ATM-LSR utilise la technique d'agrégation de routes, des données des différentes sources sont émises dès que reçues et identifiées par le même VCI/VPI. Le commutateur de sortie ne dispose alors d'aucun moyen de détecter un éventuel entrelacement de cellules ATM (*Cell interlaving*).

L'ATM-LSR A de la figure 15.14 agrège les flux entrants (labels L1 et L2) en un seul flux (label L4). Les cellules émises sur le lien dans leur ordre d'arrivée sont entrelacées. L'ATM-LSR de sortie B réassemble les cellules en un datagramme IP en se fixant sur le dernier bit du champ PT (*Payload Type,* matérialisé par « F » dans la figure) qui indique en ATM la dernière cellule d'une même PDU AAL5. Les deux datagrammes réassemblés de la figure 15.14 sont erronés. L'agrégation des flux dite aussi fusion des VC n'est envisageable dans un réseau ATM que si l'ATM-LSR ne retransmet les cellules qu'il reçoit qu'après avoir reçu la dernière cellule (figure 15.15).

Cette méthode dite **mode rétention** est consommatrice de ressource CPU, elle accroît le temps de latence dans le réseau, aussi lui préfère-t-on le mode dit **dissociation**. Dans ce mode, illustré par la figure 15.16, le réseau établi un LSP (*Label Switching Path*) par flux, perdant ainsi le bénéfice de l'agrégation des flux.

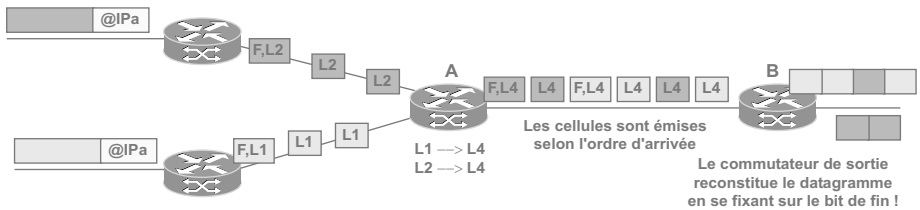


Figure 15.14 L'entrelacement de cellules.

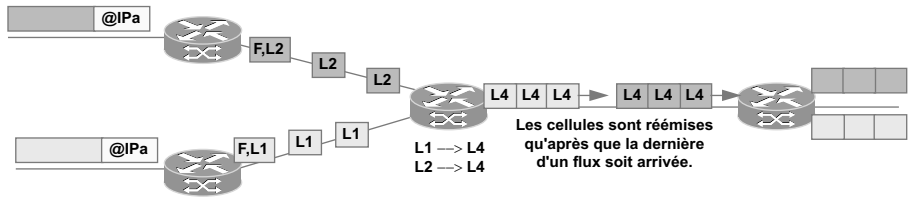


Figure 15.15 La fusion des flux dans le mode rétention.

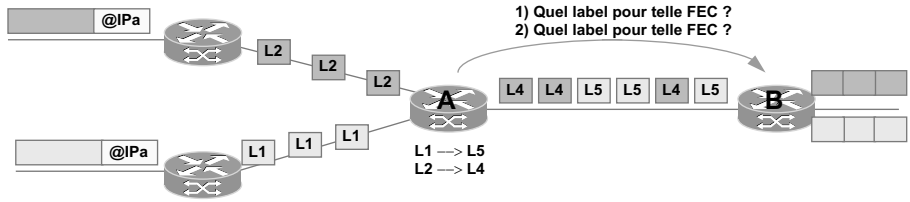


Figure 15.16 L'ATM et le mode dissociation.

Dans le mode dissociation, l'ATM-LSR recevant sur des interfaces différentes des flux à destination un même ATM-LSR suivant, demande, à ce dernier, de lui fournir un identifiant (label) pour chacun de ces flux. Cette méthode de distribution des labels est dite distribution de labels descendante à la demande (*Downstream on demand*), voir § 15.5.2.

15.5 LA CONSTRUCTION DES ROUTES DANS UN RÉSEAU MPLS

15.5.1 Généralités

Dans un réseau IP commuté, deux méthodes peuvent être utilisées pour définir les routes (**LSP**, *Label Switching Path*). À chaque destination est associée une route, même si aucun flux n'est acheminé vers celle-ci, cette méthode fondée sur la topologie du réseau (*Topology based*) est la méthode de base des réseaux MPLS. L'autre méthode consiste à ne construire une route que lorsqu'un flux de données est susceptible de l'utiliser (*Traffic based*), cette seconde méthode génère un trafic de signalisation relativement important.

La construction des LSP et la mise en relation des différents labels peuvent être déterminées manuellement ; cette méthode n'est évidemment utilisable que sur de petits réseaux. Les LSP peuvent être construits de manière similaire au routage IP, la construction des routes est réalisée de proche en proche (*Hop by hop routing*), le contrôle est dit décentralisé ou routage distribué. Le routage *hop by hop* peut s'appuyer sur un protocole de routage traditionnel IP (découverte des routes) auquel on adjoint un protocole de distribution des labels (**LDP**, *Label Distribution Protocol*). Il est aussi possible d'adapter les protocoles de routage traditionnels pour leur permettre le transport des labels comme **MBGP** (*MPLS Border Gateway Protocol*) qui est une adaptation de BGP4.

Une autre approche du routage dite « routage explicite ou routage par la source (*Explicit routing*) » spécifie une liste de nœuds pour chaque flux. La route est généralement construite sous contrainte de qualité de service (*QoS based*) ou de gestion du trafic (*Traffic engineering*). Les protocoles de routage explicites sont des adaptations des autres protocoles. **CR-LDP** (*Constraint Routing – Label Distribution Protocol*) est une extension de LDP, **RSVP-TE** (*ReSerVation Protocol –*

© Dunod – La photocopie non autorisée est un délit

Traffic Engineering) qui est une adaptation de RSVP et **OSPF-TE** (OSPF-*Traffic Engineering*) une évolution de OSPF

15.5.2 Le protocole LDP (RFC 3036)

Principe

LDP (*Label Distribution Protocol*) s'appuie sur les protocoles de routage IP dont il utilise les tables de routage. LDP définit un ensemble de procédures et de messages pour l'échange de labels entre LSR. À chaque fois qu'une destination IP est découverte, LDP sollicite, pour obtenir un label pour cette destination, le LSR amont (*Downstream on demand*) ou en attribue un au LSR aval (*Unsolicited downstream*). La figure 15.17 schématise les échanges LDP.

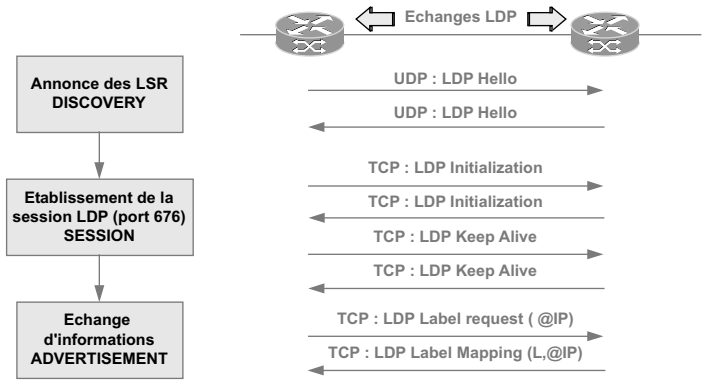


Figure 15.17 Les échanges LDP.

La découverte de ses voisins est la première fonction assurée par LDP. À cet effet, il émet périodiquement des messages « Hello » pour découvrir ses adjacences (adresse *multicast* 224.0.0.2). Les LSR adjacents s'identifient en communiquant leur adresse IP et leur **LSR-ID** (LSR *IDentifier*). Lorsqu'une relation de voisinage est découverte, le LSR de plus petit identifiant ouvre une session TCP (LDP *Initialization*) avec son voisin. La gestion des associations est réalisée par quatre types de messages :

- ***Label request*** ou demande de label, envoyé par le LSR amont pour demander quel label il doit utiliser pour une FEC spécifique.
- ***Label mapping***, message d'attribution de label à une FEC, ce message peut être émis en réponse au message *Label request* (distribution en mode non sollicité) ou spontanément après la découverte d'une nouvelle classe d'équivalence (distribution en mode non sollicité).
- ***Label withdraw***, message de suppression de labels, ce message informe un LSR qu'une association FEC/Label doit être invalidée, l'association n'est pas détruite, elle n'est plus utilisée.
- ***Label release***, ce message, similaire au précédent, détruit une association.

La distribution des labels

Deux modes de distribution de labels peuvent être utilisés. Dans le premier (figure 15.18), chaque LSR amont informe ses voisins qu'il sait joindre une FEC et que ceux-ci doivent utiliser tel label pour telle FEC. Ce mode est dit distribution en mode non sollicité (*Unsollicited dowstrean*).

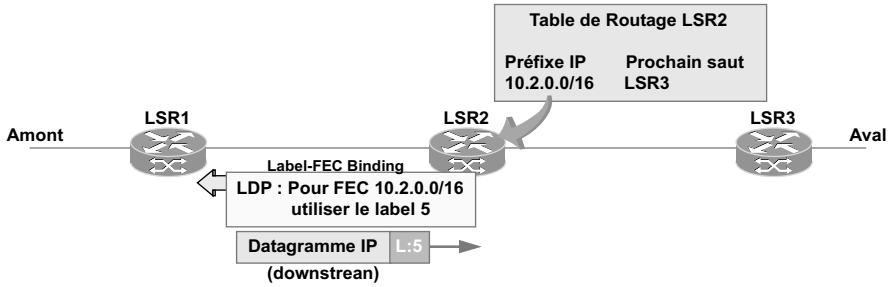


Figure 15.18 La distribution de labels en mode non sollicité.

Le LSR2 qui découvre que pour la FEC 10.2.0.0/16 le prochain saut (*Next hop*) est son voisin (LSR3) en informe ses autres voisins en leur demandant d'utiliser pour cette FEC le label 5. Dans ce mode de distribution des labels, il n'est pas impossible que le LSR1 dispose déjà d'une route pour cette classe d'équivalence. Deux politiques de conservation des associations sont alors possibles. Dans le mode dit de conservation libérale (*Liberal label retention*), le LSR1 conserve dans sa base de labels (**LIB**, *Label Information Base*) tous les labels même ceux non utilisés par la table d'acheminement (**FIB**, *Forwarding Information Base*). Cette méthode est consommatrice d'espace mémoire, mais permet en cas de changement de la topologie (lien défaillant...) de réagir rapidement. Dans le second mode dit mode de rétention conservatrice (*Conservatrice label retention*) seules ne sont conservées que les associations effectivement utilisées, ce mode est moins réactif aux dysfonctionnements du réseau.

Dans le second mode de distribution des labels, le LSR qui découvre que son voisin est le prochain saut pour une FEC donnée, lui demande de lui fournir pour cette FEC un label (figure 15.19).

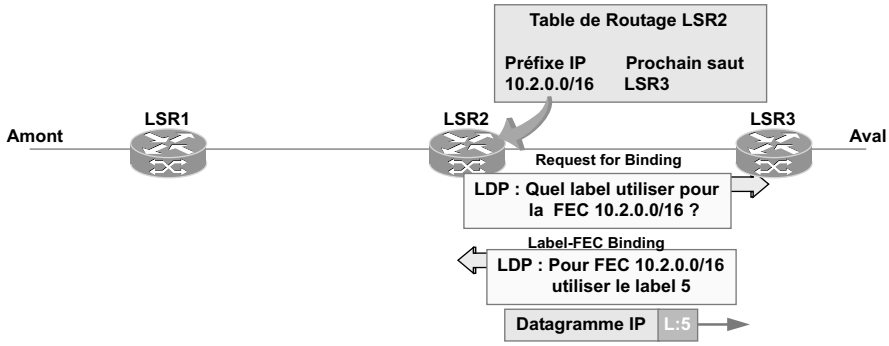


Figure 15.19 La distribution de labels en mode sollicité.

En principe, les réseaux MPLS supportent les deux modes. ATM n'a pas accès à la couche 3, dans MPLS en mode cellule seul le mode sollicité est supporté par les réseaux ATM-MPLS. Dans ces réseaux, la diffusion des labels se propage de l'*egress* LSR vers *ingress* LSR. La distribution est dite en mode contrôlé ordonné (figure 15.20).

© Dunod – La photocopie non autorisée est un délit

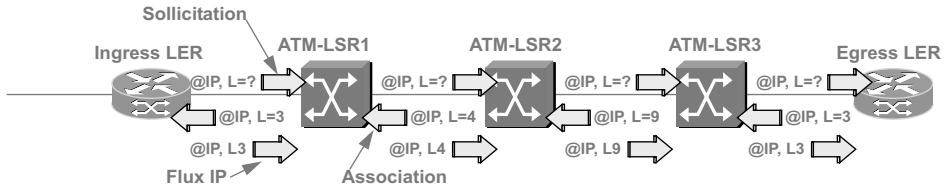


Figure 15.20 La distribution en mode ordonné.

15.6 MPLS ET L'INGÉNIERIE DE TRAFIC

Indépendamment de la détermination de routes, les opérateurs désirent disposer d'outils leur permettant de gérer au mieux le trafic dans le réseau en :

– répartissant le trafic sur plusieurs chemins (*Load balancing*) ;
– assurant une haute disponibilité à leur réseau (reroutage) ;
– associant à une route une qualité de service (QoS).

Ces services nécessitent de mettre en œuvre un routage explicite. Des adaptations des protocoles de routage traditionnel ont pris en compte ces exigences : **CR-LDP** (*Constraint Routing LDP*), **RSVP-TE** (*RSVP Traffic Engineering*).

L'ingénierie de trafic consiste à réaliser dans un réseau MPLS des tunnels pour répartir le trafic (*Load balancing*) ou affecter un flux à un chemin respectant une QoS invoquée. CR-LDP ou RSVP-TE crée un état dans le réseau (*Hard state*), en cas de défaillance d'un nœud il est alors nécessaire de reconstruire explicitement une route de bout en bout. Dans la figure 15.21, les flux à destination du LER3 sont répartis sur deux tunnels MPLS (ingénierie de trafic).

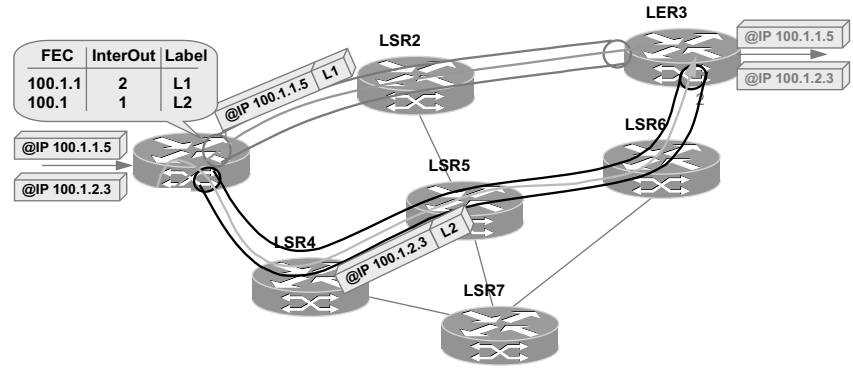


Figure 15.21 Principe de la répartition des charges.

15.7 LES VPN MPLS

15.7.1 Notions de base sur les VPN

Définitions

Un réseau privé est dit virtuel (**VPN**, *Virtual Private Network*) lorsque, sur une infrastructure partagée (réseau public ou privé), on développe des mécanismes tels que la communication ne

soit possible qu'entre clients du VPN. Les mécanismes utilisés peuvent être un simple identifiant de VPN ou une technique de chiffrement des communications. Seuls peuvent établir une communication, les clients utilisant le même identifiant ou possédant la même clé de chiffrement/déchiffrement. Les VPN MPLS appartiennent à la première catégorie. On distingue deux modes de réalisation des VPN MPLS, le modèle « ***overlay*** » et le modèle « ***peer*** » dit encore modèle « homologue ».

Le modèle « overlay »

Réaliser un VPN *overlay* consiste à relier les sites clients par des circuits virtuels permanents. L'interconnexion des sites clients est réalisée par la définition d'un ensemble de circuits virtuels. Les relations sont du type point à point. La figure 15.22 illustre une relation de type *overlay* entre deux sites.

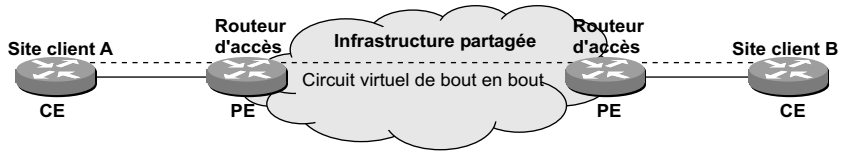


Figure 15.22 Principe du modèle overlay.

Dans ce modèle, le circuit virtuel est établi du site client A au site client B. Le routeur du site client est dénommé routeur **CE** (*Customer Edge Router*), le routeur d'accès au réseau partagé (routeur **PE**, *Provider Edge Router*). Si l'approche théorique de ce modèle est simple, la réalisation de réseaux VPN *overlay* est relativement complexe. Il faut définir avec précision les relations entre sites et créer autant de circuits virtuels que de relations point à point à émuler. Le nombre de circuits à définir croît comme le carré du nombre de sites (N [N–1]/2). Compte tenu du nombre de circuits à définir, les réseaux VPN *overlay* réalisent rarement un maillage complet. Dans ce cas, certains sites sont définis comme sites de transit, ce qui nécessite une étude volumétrique précise des flux entre les sites (figure 15.23).

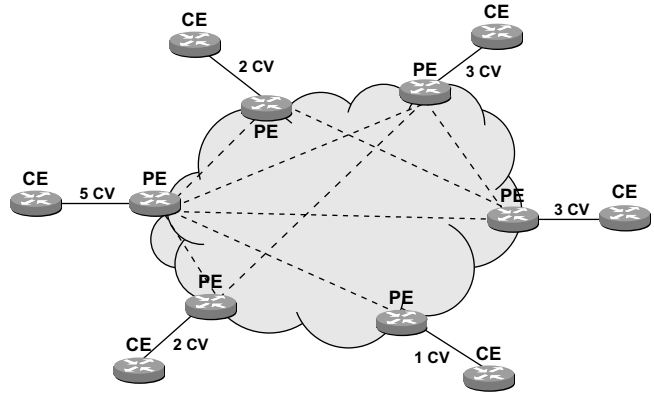


Figure 15.23 Exemple de VPN overlay.

© Dunod – La photocopie non autorisée est un délit

Dans le réseau exemple de la figure 15.23, le VPN construit entre tous les sites représentés chacun par leur routeur client (CE) ne comportent que huit circuits virtuels dans l'infrastructure partagée. La communication entre certains sites transite par d'autres sites clients[1].

Chaque nœud du réseau opérateur contient une entrée pour chaque circuit virtuel défini entre les sites clients. Indépendamment de la difficulté que peut présenter la gestion d'un nombre important de circuits virtuels, l'ajout d'un site à un VPN n'est pas transparent à l'infrastructure du réseau opérateur. Le modèle homologue ou *peer* remédie à cette difficulté.

Le modèle peer

Dans le modèle *peer* (figure 15.24), les VPN sont ignorés du cœur de réseau, les données échangées entre les clients d'un même VPN sont acheminées dans le réseau comme des données ordinaires. Les informations relatives aux VPN sont échangées entre le routeur client (**CE**, *Customer Edge*) et le routeur de périphérie (**PE**, *Provider Edge*). Seuls les routeurs de périphérie du réseau ont connaissance des VPN, le routage des données en est facilité. Les routeurs de cœur de réseau (**P Router**, *Provider router*) n'ont plus de nombreux circuits virtuels à gérer et l'ajout d'un client n'a aucun impact sur le réseau, de ce fait, l'évolution des VPN *peer* est aisée.

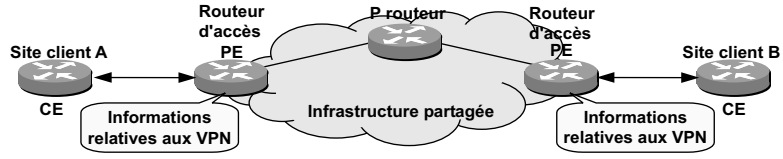


Figure 15.24 Principe des VPN peer.

Les tables de routages des routeurs de périphérie (PE) contiennent les routes annoncées par les VPN clients. Si le routeur d'accès est partagé par plusieurs clients VPN différents, le risque de rebond dans ce routeur n'est pas nul. Une autre architecture est envisageable dite à routeur dédié, elle améliore la sécurité en assurant un cloisonnement entre les différents VPN (figure 15.25).

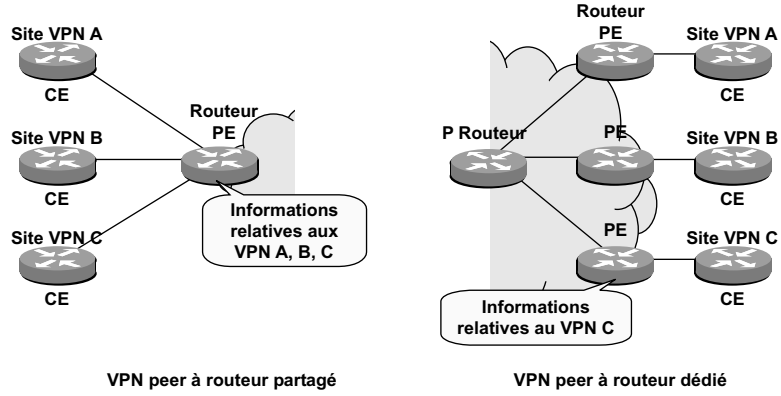


Figure 15.25 Les différents modèles de VPN peer.

1. Une configuration de type étoile (topologie dite aussi *hub-and-spoke*) n'interdit nullement les communications entre tous les sites (communication *any-to-any*), celles-ci n'étant pas réservées seulement aux topologies de type maillage complet.

15.7.2 Principe général des VPN MPLS

MPLS utilise le modèle *peer* dit aussi *homologue*. Pour assurer la gestion des VPN qui leur sont rattachés les *Provider Edge Router* entretiennent une table d'acheminement spécifique à chaque interface (**VRF**, *VPN Routing and Forwarding*). La VRF contient la désignation du PE, auquel sont rattachés le client VPN destinataire, la classe d'équivalence associée (**FEC**, *Forwarding Equivalence Class*), considéré par cette table comme le prochain saut (*Next hop*) et le label identifiant le VPN d'appartenance. La VRF contient ainsi tous les éléments d'acheminement, y compris une copie dédiée de la LFIB, de ce fait une VRF correspond à un routeur dédié au VPN (**routeur virtuel**). L'acheminement dans le réseau est réalisé par consultation de la **LFIB** (*Label Forwarding Information Base*). La figure 15.26 illustre l'affectation et la commutation de labels d'un VPN MPLS.

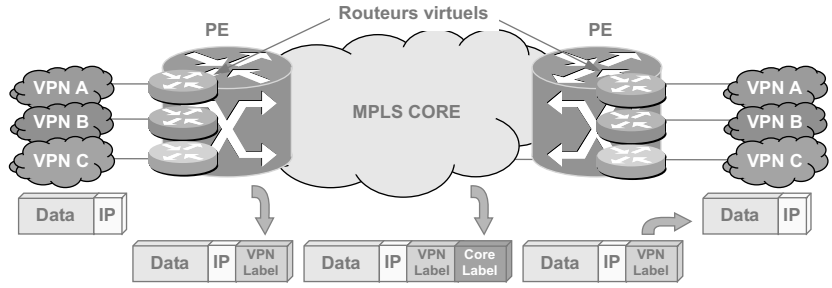


Figure 15.26 L'affectation des labels dans un VPN MPLS.

La VRF (*VPN Routing and Forwarding*) assure le routage dans le VPN, elle considère le réseau MPLS comme un lien en point à point entre le PE (*Provider edge*) d'entrée et le PE de sortie. La VRF d'entrée indique, en fonction du client VPN destinataire, le PE de sortie considéré comme étant le prochain saut dans le réseau VPN, tandis que la LFIB assure l'acheminement dans le réseau MPLS et voit comme prochain saut le routeur aval sur la route définie par la FEC (*Forwarding Equivalence Class*) du PE de sortie. La figure 15.27 illustre l'affectation des labels et l'acheminement dans le réseau.

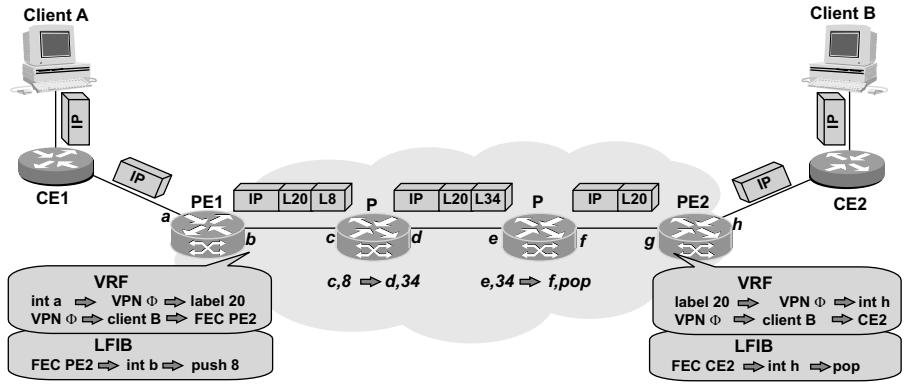


Figure 15.27 L'acheminement dans le réseau MPLS.

© Dunod – La photocopie non autorisée est un délit

Cette vision implique l'utilisation d'un protocole de routage pour assurer l'échange d'information de routage de chaque VPN entre les routeurs PE, ce qui revient à définir une instance de routage par VPN ! Il est donc nécessaire d'utiliser un protocole du type BGP (*Border Gateway Protocol*) ou IS-IS (*Intermediate System - Intermediate System*) capable de transporter des adresses appartenant à des ensembles d'adressage différents. De ce fait, MPLS superpose deux protocoles de routage, le routage entre PE (**MP-BGP**, *Multi-Protocol BGP*) et un protocole de routage « classique » entre les différents nœuds du réseau (IGP). La figure 15.28 illustre ce principe.

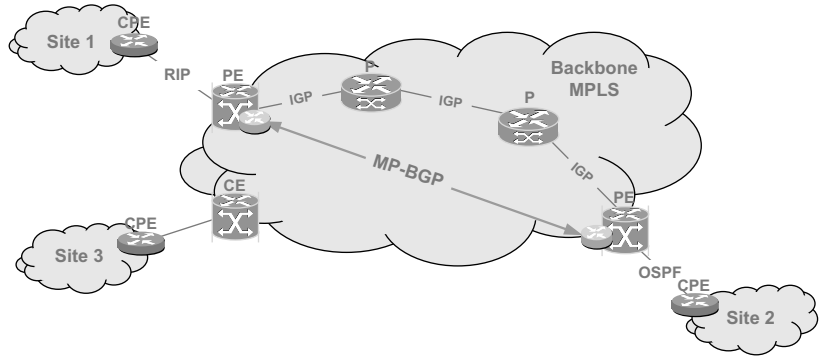


Figure 15.28 La superposition des protocoles de routage.

Un second problème doit être résolu : d'une part un client VPN peut appartenir à plusieurs VPN et d'autre part l'utilisation de plus en plus fréquente, par les entreprises, des adresses privées de la RFC 1918 conduisent à un chevauchement d'adresses. L'unicité d'adresse ne peut être garantie, sauf à renuméroter les sites clients ou à mettre en œuvre un système de translation d'adresse. La première méthode est pénalisante pour l'entreprise qui doit revoir tout son plan d'adressage, la seconde n'est pas sans impact sur les performances du réseau.

La solution consiste à rendre, artificiellement, les adresses uniques sur le réseau en leur ajoutant un identifiant spécifique dit « **distingueur** » de route sur 64 bits (*Route Distinguisher*) et à modifier le protocole de routage pour qu'il accepte de telles adresses (**MP-BGP**, *MultiProtocol BGP*). La figure 15.29 fournit le format dit de communauté étendue de cette nouvelle adresse dite adresse VPN-IPv4.

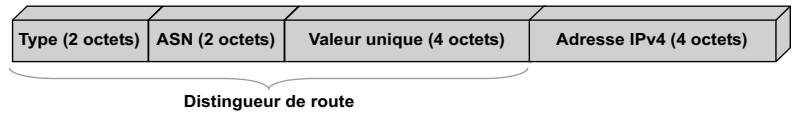


Figure 15.29 Le format de l'adresse VPN-IPv4.

Le champ type précise comment est construit le distingueur de route. Celui-ci est généralement déterminé à partir du numéro de système autonome (**ASN**, *Autonomous System Number*), valeur de l'octet de poids fort du champ type 0x00, et d'une valeur unique attribuée par l'opérateur de VPN.

15.8 CONCLUSION

MPLS apporte au protocole IP, non orienté connexion, les avantages du mode connecté tout en conservant la souplesse du mode non connecté, en outre il permet :

- la diminution du temps de transit dans les réseaux, mais il est, aujourd'hui, concurrencé par les giga- voire téra-routeurs ;
- l'ingénierie de trafic, qui autorise dans un réseau IP une haute disponibilité et la prévention de la congestion ;
- la mise en œuvre de la QoS et notamment d'offrir un service voix sur un réseau IP ;
- une gestion souple des VPN.

Dans l'état actuel des techniques, les réseaux sont constitués d'un empilement de protocoles ayant chacun leur protocole de signalisation et d'administration ainsi que des techniques de configuration spécifiques. Cependant, si MPLS inséré entre IP et le protocole de transport de niveau 2 optimise les performances du réseau et simplifie la gestion de la bande passante, pour optimiser l'utilisation de celle-ci et faciliter l'administration globale des réseaux, il conviendrait de redéfinir une architecture globale. C'est l'objectif de **G-MPLS** (*Generalized MPLS*) qui étend le domaine MPLS jusqu'au niveau optique en faisant correspondre un label à une longueur d'onde (**MPλS**).

EXERCICE

Exercice 15.1 Routage et commutation

Complétez la figure 15.30 et déduisez-en les avantages de MPLS.

Critères	Mode orienté connexion	Mode non connecté
Mise en relation nécessaire		
Délai de connexion Délai de déconnexion		
Type de circuit offert		
Allocation de ressources		
Contrôle de flux possible		
Séquencement des informations		
Reprise sur incident		
Complexité		
Optimisation des réseaux		
Résistance à la défaillance		
Adressage		

Figure 15.30 Le routage et la commutation.

Chapitre **16**

Les réseaux locaux et métropolitains

16.1 INTRODUCTION

16.1.1 Définition

L'évolution générale des systèmes d'information et des moyens d'y accéder a engendré une modification significative des méthodes de travail. D'individuel, le travail est devenu collectif. Les besoins d'information et de communication dans le groupe de travail ont été décuplés. Le micro-ordinateur et le réseau local sont à l'épicentre de cette mutation (figure 16.1).

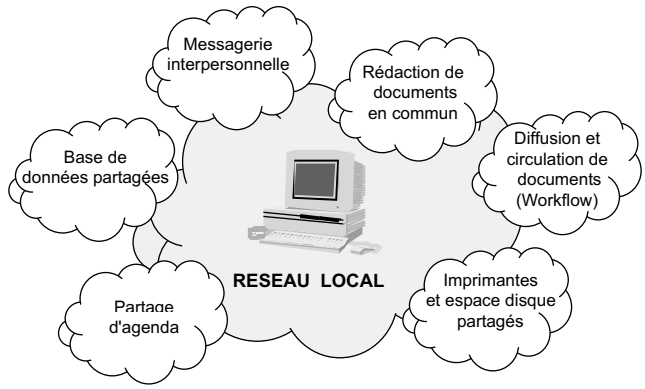


Figure 16.1 Le réseau local et le micro-ordinateur épicentre du travail collectif.

Un réseau local (**LAN**, *Local Area Network*) est un ensemble de moyens autonomes de calcul (micro-ordinateurs, stations de travail ou autres) reliés entre eux pour s'échanger des informations et/ou partager des ressources matérielles (imprimantes, espace disque...) ou logicielles (programmes, bases de données...).

16.1.2 Distinction entre réseau local et informatique traditionnelle

Entre un terminal passif, par exemple un terminal Telnet, en informatique traditionnelle centralisée, et un poste client d'un réseau local, le plus souvent un micro-ordinateur, la différence essentielle concerne la localisation des traitements et de la politique d'accès (figure 16.2).

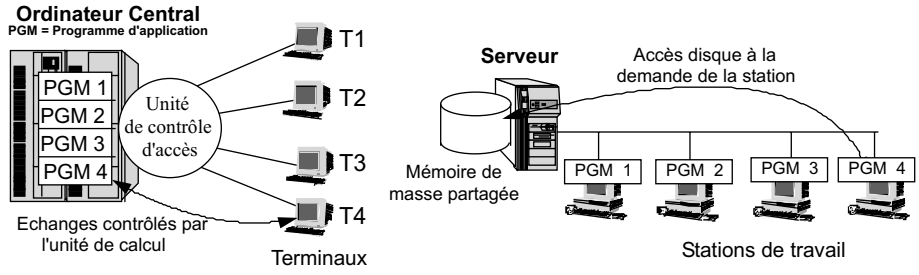


Figure 16.2 La localisation de la puissance de calcul.

Un terminal passif ne dispose d'aucune puissance de calcul, les diverses applications partagent le temps processeur de l'ordinateur central (**CPU**, *Central Processing Unit*). Celui-ci contrôle le traitement et organise les accès (politique d'accès centralisé : *polling/selecting* ou relation maître/esclave). Un poste client (**station**) d'un réseau local dispose d'une puissance de calcul autonome, le programme principal s'exécute en local, il n'émet des requêtes au serveur que pour utiliser les ressources partagées et offertes par ce dernier. Il n'y a pas de subordination entre les différents constituants du réseau. Dans ces conditions, ceux-ci partageant le même média, une discipline d'accès (**protocole d'accès**) doit être implémentée dans chaque unité (politique ou contrôle d'accès décentralisé).

Un réseau local distingue deux types de machines, celles qui offrent des ressources en partage : les serveurs, et celles qui utilisent ces ressources : les postes clients, postes de travail ou stations. Dans les réseaux locaux de la dernière génération toutes les machines peuvent offrir des ressources en partage et utiliser celles offertes par les autres stations du réseau. Ce type de réseau est désigné sous le nom de *peer to peer* ou poste à poste ou encore d'égal à égal. En fait, dans les réseaux importants, une machine dédiée aux fonctions traditionnelles de serveur subsiste. Celle-ci assure la gestion des utilisateurs, la sécurité d'accès, la distribution des logiciels...

16.1.3 Les réseaux locaux et l'accès aux systèmes traditionnels

Pour l'utilisateur, la distinction entre les systèmes est masquée. Une station d'un réseau local peut donner accès aux applications d'un ordinateur central (mini ou *mainframe*). Le programme client émule alors un terminal de l'autre système. L'une des stations assure les fonctions de passerelle vers le système central.

Dans la figure 16.3 une station du réseau local exécute un programme qui émule un terminal dédié du système centralisé (**émulation de terminal**) et permet l'accès au PGM1 qui se déroule sur l'ordinateur central. Une autre machine du réseau local, dite passerelle (*Gateway*), permet l'accès à la machine centrale qui peut être locale ou distante, c'est un concentrateur d'accès. Sur l'ordinateur central, un autre programme d'émulation simule un dialogue local entre le terminal et l'application. C'est ce programme d'émulation qui contrôle le dialogue avec l'application PGM1. L'émulateur local convertit, vis-à-vis de l'utilisateur, le poste de travail en terminal passif dédié.

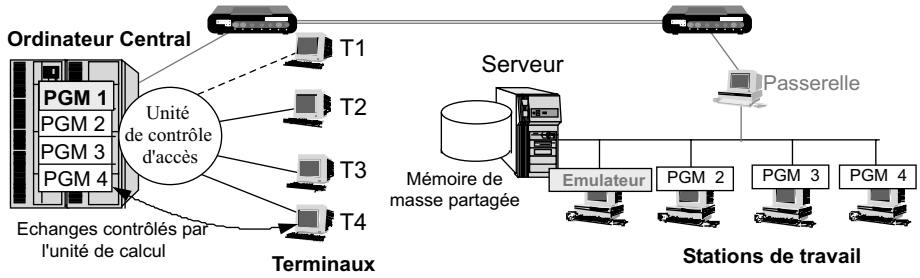


Figure 16.3 L'accès aux moyens de calcul traditionnels via un réseau local.

16.1.4 Les constituants d'un réseau local

Architecture informatique dédiée à l'échange d'information et au partage de ressources physiques, un réseau local est essentiellement constitué par (figure 16.4) :

- un câblage reliant les différents nœuds selon une certaine topologie ;
- une méthode d'accès au support pour assurer son partage ;
- une méthode d'adressage pour identifier chaque nœud ;
- un ensemble cohérent de protocoles (pile) pour permettre la communication ;
- un système d'exploitation spécifique (**NOS**, *Network Operating System*) capable de prendre en charge les périphériques distants partagés et d'en contrôler l'utilisation (administration et sécurité) ;
- un ensemble de programmes utilisant les ressources mises en commun.

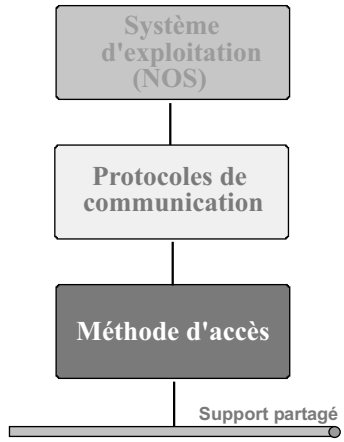


Figure 16.4 Les principaux constituants d'un nœud de réseau local.

Pour assurer l'intégralité de ces fonctionnalités, il a fallu adapter l'architecture du modèle de référence de l'ISO. L'architecture OSI répond à l'interconnexion de systèmes en mode point à point, alors que les réseaux locaux partagent un support unique en **mode diffusion**. Les couches

© Dunod – La photocopie non autorisée est un délit

hautes du modèle qui gèrent la communication restent applicables aux réseaux locaux. Cependant, les couches basses qui organisent l'accès au support devront être adaptées (figure 16.5).

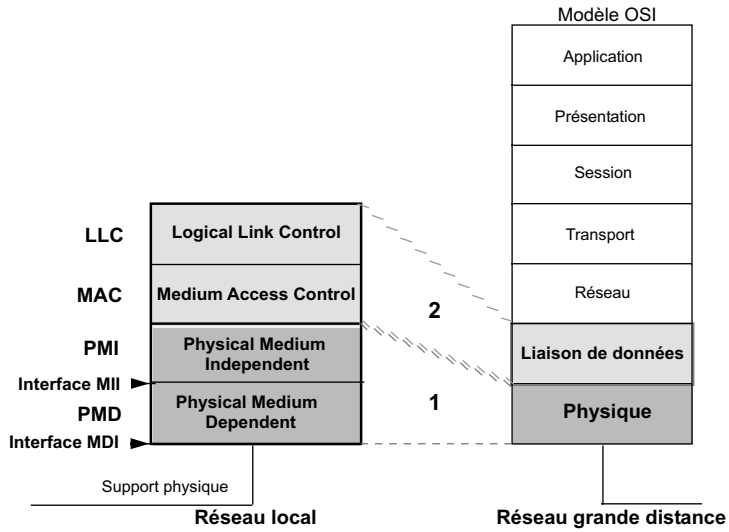


Figure 16.5 La structure des niveaux 1 et 2 dans les réseaux locaux.

Afin de décrire une interface indépendante du support, le niveau physique a été scindé en deux. La sous-couche basse (sous-couche **PMD**, *Physical Medium Dependent*) assure le transfert des données (bits) sur une gamme de supports variés : câble coaxial, paire torsadée, fibre optique, réseaux sans fil. La sous-couche supérieure (**PMI**, *Physical Medium Independent*) est chargée de la détection de présence d'un signal, du codage et de la récupération de l'horloge (synchronisation).

Le niveau liaison a, aussi, été divisé en deux. La sous-couche la plus basse (sous-couche **MAC,** *Medium Access Control*) contrôle l'accès partagé au support et le contrôle d'erreur. La sous-couche supérieure (sous-couche **LLC**, *Logical Link Control* ou Contrôle du lien logique) remplit les fonctions traditionnellement dévolues à la couche liaison (établissement d'un lien logique).

Cependant, deux problèmes importants restent à résoudre : l'adressage des machines connectées et l'analyse des commandes. Le modèle de référence définit l'adressage des systèmes au niveau réseau. Cette adresse détermine le point de raccordement de l'hôte dans le réseau étendu. Si, dans les réseaux locaux, ce mode d'adressage était maintenu, chaque message circulant sur le réseau provoquerait, dans chaque poste raccordé, une interruption processeur. Le processeur examinerait l'adresse pour s'apercevoir que le message ne lui est pas destiné, ce qui grèverait gravement les performances de toutes les stations du réseau. Dans les réseaux locaux, il n'y a aucun besoin de localisation, il suffit de distinguer une interface parmi toutes celles raccordées localement à un même réseau. Chaque interface est alors distinguée par un numéro, appelé adresse physique ou adresse MAC (adressage à plat). Le message ne sera transmis aux couches supérieures que s'il concerne l'interface du nœud destinataire.

Sur une machine connectée en réseau local, les différentes commandes peuvent être adressées soit au système local soit à un système distant. Il est nécessaire de disposer de mécanismes permettant de distinguer ces deux types d'appel. Une couche fonctionnelle dite « redirecteur », spécifique au système d'exploitation réseau, a pour rôle de diriger les appels vers le système cible. La notion

de redirecteur[1] n'est pas définie par l'ISO. Cependant, on peut admettre qu'elle se situe au niveau de la couche présentation. La figure 16.6 illustre cette architecture.

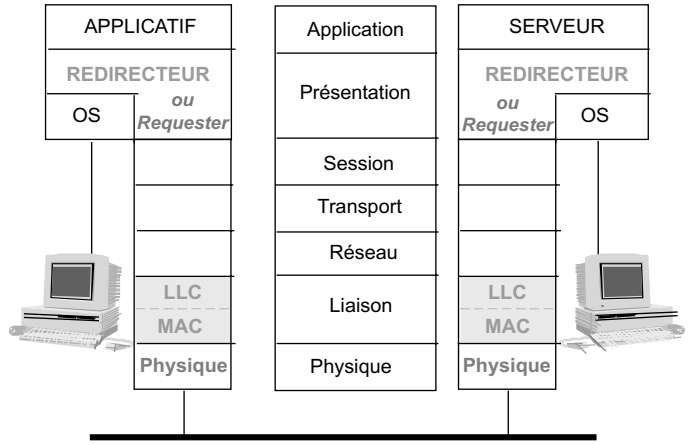


Figure 16.6 L'architecture générale des réseaux locaux.

16.1.5 Les réseaux locaux et la normalisation

Devant la diversité des besoins et des produits proposés, l'**IEEE** (*Institute of Electrical and Electronic Engineers*) a créé le groupe de travail 802 (février 1980) chargé de définir des standards (Standards 802.x). En 1988, l'ISO a repris la plupart de ces standards pour les normaliser et en faire des normes internationales (série ISO 8802.*x*).

Aujourd'hui, l'IEEE poursuit, au profit de l'ISO, son travail de normalisation. Le groupe 802 est divisé en sous-groupes de travail, chacun chargé d'une tâche normative spécifique (figure 16.7).

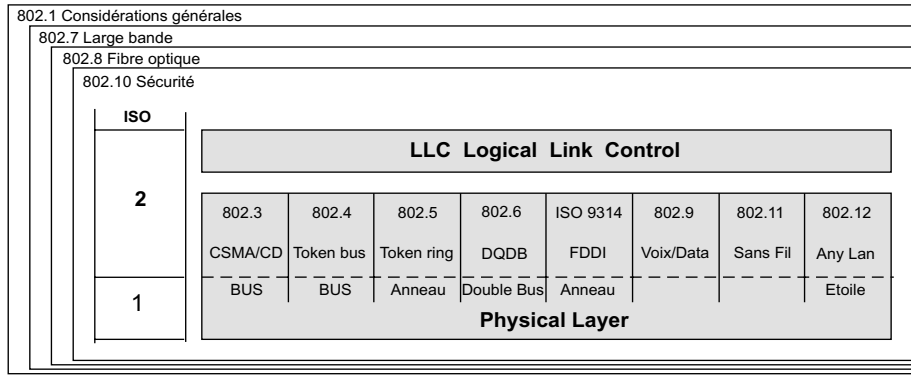


Figure 16.7 La schématisation de l'organisation des comités 802.

1. Le redirecteur, désignation Microsoft, est couramment appelé *requester* ou *shell* chez Novell.

© Dunod – La photocopie non autorisée est un délit

On peut, par exemple, citer :

– le Comité 802.1 qui définit l'architecture générale des réseaux et détermine le format d'adressage, les techniques d'interconnexion et d'administration ;
– le Comité 802.2 qui précise les fonctionnalités de la couche liaison de données (sous-couche **LLC**, *Logical Link Control*). Il a défini trois types de services : **LLC1** (service en mode non connecté), **LLC2** (service en mode connecté proche d'HDLC) et **LCC3** (service en mode non connecté mais avec acquittement) ;
– les Comités 802.3 à 802.6 et 802.11 à 802.16 qui spécifient les méthodes d'accès (sous-couche MAC) et les couches physiques correspondantes ;
– les Comités 802.7 et 802.8 qui assurent la coordination des autres comités dans les domaines du large bande (802.7) et de la fibre optique (802.8) ;
– les Comités 802.11 et 802.16 qui étudient les réseaux sans fil (*Wireless LAN*).

16.2 ÉTUDE SUCCINCTE DES DIFFÉRENTES COUCHES

Ce paragraphe se propose d'étudier de manière générique les niveaux 1 et 2 des réseaux locaux. Les algorithmes d'accès au support seront détaillés lors de l'étude de la couche MAC de chaque type de réseau.

16.2.1 La couche physique

La couche physique spécifie les modes de raccordement (topologie et câblage), les niveaux électriques et le codage des informations émises.

Les topologies et les méthodes d'accès

La topologie d'un réseau décrit la manière dont les différents composants du réseau sont reliés. Les réseaux locaux utilisent les topologies de base comme le bus, l'anneau et l'étoile (figure 16.8) ou des combinaisons de celles-ci (étoile de bus, grappe d'étoiles...).

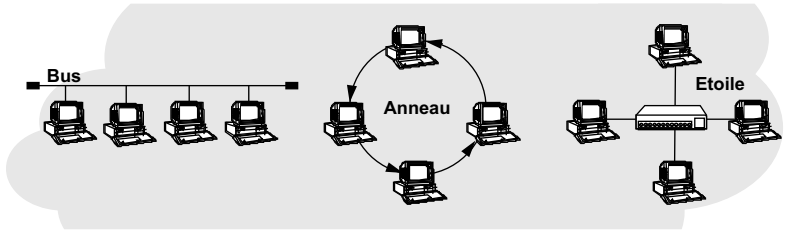


Figure 16.8 Les topologies de base.

Sur un bus, les unités sont au même niveau hiérarchique, les messages sont reçus par l'ensemble des stations (diffusion). Le système n'étant pas hiérarchisé, une station peut accéder au support à tout moment. Ce mode d'accès n'interdit pas à deux stations d'émettre en même temps, les messages sont alors altérés : il y a **collision** ou **contention**. Pour résoudre ce problème, des règles d'accès au support doivent être fixées :

– la station vérifie, avant d'émettre, qu'aucune autre n'est en émission (écoute du support), cette méthode d'accès est utilisée par les réseaux IEEE 802.3 appelés couramment « **Ethernet**[2] » ;
– selon une autre méthode, chaque station se voit successivement attribuer le droit d'émettre par un message particulier : le *token* ou jeton. Chaque station qui reçoit le jeton l'adresse à la suivante (jeton adressé). Cette méthode est utilisée dans les réseaux industriels de type IEEE 802.4 ou **Token Bus**.

L'anneau est un cas particulier d'une liaison multipoint, il implique une circulation unidirectionnelle des messages. Le message est relayé par toutes les stations jusqu'à son destinataire. Dans ce type de topologie le droit d'émettre (jeton) est transmis à la station qui suit physiquement celle qui le détient (jeton non adressé). Cette méthode d'accès est mise en œuvre dans le réseau IEEE 802.5 ou **Token Ring**.

Les topologies en étoile sont une variante des liaisons point à point, ils constituent *n* liaisons point à point autour d'un concentrateur. Ce dernier peut n'être qu'un répéteur (*hub*[3] du réseau IEEE 802.3 10 base T) ou participer activement à la distribution de l'accès au support (IEEE 802.12 ou AnyLAN). Dans ce dernier cas, une station qui désire émettre formule une demande au concentrateur qui lui alloue ou non le droit d'émettre.

Le câblage

➤ Généralités

Les réseaux locaux utilisent tous les types de support : les câbles cuivre (coaxial, paires torsadées), les supports optiques (fibre optique) et les supports hertziens (réseaux sans fil). Le câble coaxial a longtemps été utilisé (réseaux de type Ethernet), mais il est aujourd'hui remplacé par la paire torsadée moins chère et plus facile d'installation. La fibre optique est essentiellement réservée aux réseaux haut débit et à l'interconnexion de réseaux. La figure 16.9 présente une synthèse des différentes caractéristiques des câbles.

Type de câble	Immunité Électromagnétique	Débit courant	Distance	Utilisation
Coaxial	Bonne	10 Mbit/s	2 500 m par brin de 500 m	Ethernet, en environnement perturbé ou confidentiel.
Paires torsadées UTP	Faible	10 à 100 Mbit/s	100 m d'un élément actif	Ethernet sur paires torsadées.
Paires torsadées FTP	Moyenne	10 à 100 Mbit/s	100 m d'un élément actif	Ethernet paires torsadées, Token Ring.
Fibre optique	Excellente	100 à 1 Gbit/s	De quelques km à une centaine de km	FDDI (100 Mbit/s), Gigabit Ethernet...

Figure 16.9 Les différents câbles mis en œuvre dans les réseaux locaux.

2. Ethernet est un nom de marque déposé par Xerox. Ce nom est passé dans le langage courant et désigne les réseaux de type CSMA/CD.
3. Un *hub* n'est ni réellement un concentrateur, ni seulement un répéteur. Ces termes, couramment utilisés pour désigner un hub sont imprécis. Dans la suite de cet ouvrage nous n'utiliserons que le terme de hub.

© Dunod – La photocopie non autorisée est un délit

➤ Le précâblage d'immeuble

Le développement intensif des postes de travail en réseau local a révélé des problèmes liés au câblage. Les réseaux locaux ont tous, aujourd'hui, une topologie physique en étoile, d'où l'idée de réaliser, dans les immeubles de bureaux, un précâblage (figure 16.10). Un système de précâblage doit :

– assurer que tout poste de travail ne sera qu'à quelques mètres d'une prise informatique ou téléphonique ;
– être indépendant du type de réseau et de la topologie réseau choisis.

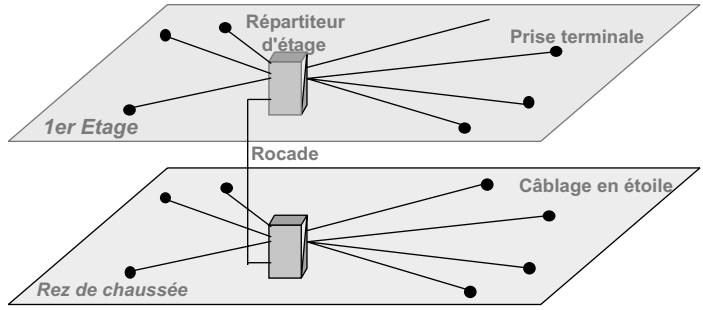


Figure 16.10 La structure générale d'un précâblage d'immeuble.

Différents systèmes de câblage ont été définis par les principaux constructeurs, ce sont principalement l'**ICS** (*IBM Cabling System*), le **BCS** (*Bull Cabling System*), *l'Open Link* de **DEC** et le **PDS Systimax** d'origine AT&T. Ces systèmes ont en commun l'utilisation de la paire torsadée et une topologie physique en étoile. Le cœur du câblage est constitué de panneaux, dits **panneaux de brassage**, qui permettent, à l'aide de jarretières, de réaliser la connexion des postes de travail selon la topologie requise par le réseau. Ces systèmes diffèrent essentiellement par le type de câble utilisé (UTP, FTP). Le débat sur les différentes impédances s'est aujourd'hui tari au profit du câble 100 Ω. La dernière version de la norme ISO (ISO 11801 du 23/10/2002) déclasse le 120 Ω en classe D.

Les câbles sont classés en catégorie selon les spécifications auxquels ils répondent : atténuation, bande passante, *Next*... (figure 16.11).

Catégorie	Classe	Impédance	Fréquence max.	Applications
3	C	100-120 Ω	16 MHz	Token Ring 4 Mbit/s 10 Base T Fast Ethernet 100 VG AnyLAN 100 Base T4
4	D	100 Ω	20 MHz	Token Ring 16 Mbit/s
5	D	100 Ω	100 MHz	100 Base Tx ATM 155 Mbit/s ATM 622 Mbit/s (Draft) 1000 Base T (Cat 5E)
6	E	100 Ω	250 MHz	1000 Base Tx ATM 1,2 Gbit/s (Draft)

Figure 16.11 Les catégories de paires torsadées.

Les câbles de catégorie 5 et 5e sont aujourd'hui les plus installés. Les dernières installations concernent essentiellement la catégorie 6, alors qu'un câble UTP catégorie 6a vient d'être défini, il autorise un débit de 10 Gbit/s sur 100 m. La figure 16.12 représente les différents constituants participant à la réalisation physique d'un câblage en paires torsadées. Un local technique (local de brassage) abrite une armoire technique ou armoire de brassage. Celle-ci accueille les éléments actifs (hub, MAU ou *Medium Access Unit*), parfois les serveurs (salle réseau). Le précâblage consiste à « tirer » des câbles entre le panneau de brassage et les prises murales. Pour raccorder une station, il suffit de connecter celle-ci à la prise murale par un cordon dit de raccordement. À l'autre extrémité, au panneau de brassage, on tire une jarretière (cordon de raccordement ou de brassage) entre la prise RJ45 du panneau de brassage correspondant à la prise murale à raccorder et un port de l'élément actif. Chaque point de raccordement pouvant constituer une désadaptation d'impédance et engendrer des ondes stationnaires, il est impératif de veiller à la qualité de tous ces éléments et de vérifier qu'ils sont qualifiés pour le type de réseau mis en œuvre.

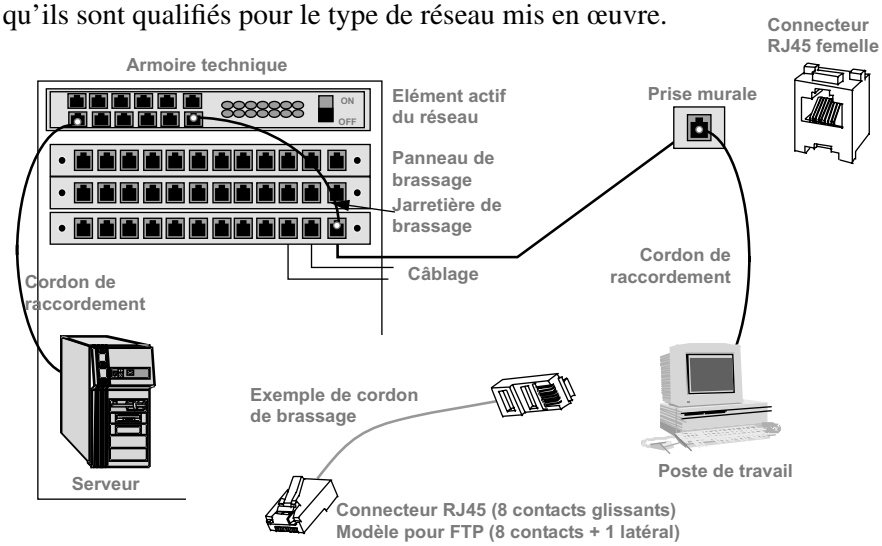


Figure 16.12 Les constituants physiques d'un réseau local.

Les seules contraintes d'installation de la paire torsadée concernent la distance minimale à respecter entre le câble et les sources de rayonnement électromagnétique (distribution courant fort, tubes fluorescents, machinerie électrique...). Par exemple, le cheminement parallèle de câbles courant faible et courant fort doit respecter un écartement minimal de 5 cm si le cheminement est inférieur à 10 m, 15 cm jusqu'à 30 m et 30 cm au-delà. Le rayon de courbure des câbles (1,5 fois le diamètre du câble) et la longueur maximale de « détorsadage » des paires pour réaliser la connectique (1,5 cm) sont des points à examiner lors de la recette d'un câblage.

16.2.2 La sous-couche MAC

La sous-couche **MAC** (*Medium Access Control*) gère l'accès au support physique, elle règle les problèmes d'adressage (adresse MAC) et effectue un contrôle d'erreur (**FCS**, *Frame Check Sequence*).

Les méthodes d'accès

Ce sont les méthodes d'accès qui distinguent les différents types de réseau et déterminent leurs performances dans tel ou tel environnement. Deux méthodes dominent le monde des réseaux locaux :

© Dunod – La photocopie non autorisée est un délit

les méthodes aléatoires ou à contention, mises en œuvre dans les réseaux de type « Ethernet », et les méthodes à réservation fondées sur le passage du droit d'émettre (jeton) dont le Token Ring est l'implémentation la plus connue.

➤ Les méthodes à contention

Les méthodes à contention ou **CSMA** (*Carrier Send Multiple Access* ou accès multiple avec écoute de la porteuse) sont utilisées dans deux types de réseaux :

- le réseau AppleTalk (**CSMA/CA**, *Collision Avoidance* ou à prévention de collision). L'architecture réseau d'Apple est essentiellement destinée au partage de l'imprimante LaserWriter, d'un débit très réduit (230,4 kbit/s), cette architecture est, aujourd'hui, obsolète ;
- le réseau dit « Ethernet » ou **CSMA/CD** (*Collision Detection* ou à détection de collision). D'origine DEC, Intel et Xerox (Ethernet DIX standard ou Ethernet v2), Ethernet utilise une méthode d'accès qui a été normalisée par l'IEEE (802.3) et par l'ISO (ISO 8802.3), il représente plus de 90 % des réseaux locaux installés.

Les réseaux à contention, ou dérivés de ce principe (Ethernet, réseaux commutés, VLAN et réseaux sans fil) constituent, aujourd'hui, l'essentiel des réseaux utilisés. Ils feront l'objet du chapitre suivant.

➤ Les méthodes à réservation

Évolution du polling/selecting, les méthodes à réservation en diffèrent par une distribution décentralisée du droit d'émettre. L'autorisation d'émettre est matérialisée par une trame particulière : le jeton ou *token* qui circule d'équipement en équipement soit dans l'ordre physique des éléments (*Token Ring* ou anneau à jeton) soit dans l'ordre logique des stations (*Token Bus* ou bus à jeton). Le jeton circule en permanence sur le réseau, toutes les stations le reçoivent successivement et ne peuvent émettre des données que s'il est libre.

L'adressage MAC

➤ Généralités

L'adresse MAC désigne de manière unique une station sur le réseau. À des fins de facilité d'administration, elle est gravée dans l'adaptateur réseau (**NIC**, *Network Interface Card*) par le fabriquant de l'adaptateur. Pour garantir l'unicité d'adresse, c'est l'IEEE qui les attribue. L'IEEE propose deux formats d'adresse : un format long sur 48 bits et un format court sur 16 bits. La figure 16.13 présente l'adressage IEEE[4], les bits sont représentés dans l'ordre d'émission sur le support (bits de poids faible devant).

Seul, en principe, l'adressage long est utilisé. Le premier bit (bit I/G) distingue une adresse individuelle ou *unicast* (I=0) d'un adressage de groupe (*multicast* ou *broadcast*, I=1). Le bit suivant (bit U/L) détermine si l'adresse qui suit est universelle : adressage IEEE (U=0) ou local (L=1). Dans ce dernier cas, c'est l'administrateur de réseau qui gère l'espace d'adressage et garantit l'unicité d'adressage. L'adressage IEEE est un adressage à plat, il distingue, sur le réseau, une machine parmi les autres, mais il ne permet pas d'en déterminer la position géographique.

4. Devant la multiplication des équipements à identifier, en 1995, l'IEEE a défini un nouveau format d'adressage sur 64 bits (EUI-64).

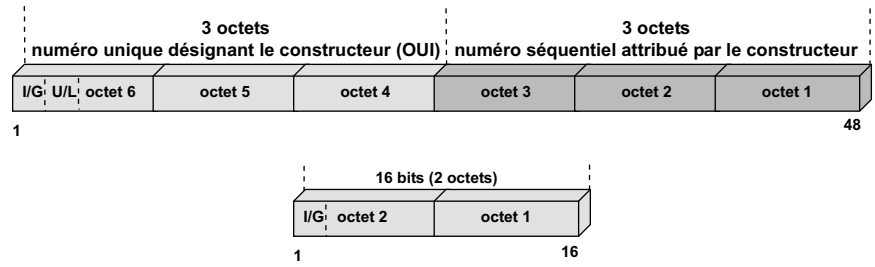


Figure 16.13 L'adressage IEEE.

Dans l'adressage universel, les 22 bits suivants désignent le constructeur ou le revendeur de l'adaptateur réseau. L'IEEE attribue à chaque constructeur[5] un ou plusieurs numéros qui l'identifient (**OUI**, *Organization Unit Identifier*). Les 24 bits suivants appartiennent à une série séquentielle et sont inscrits dans l'adaptateur sous la responsabilité du fabricant (**SN**, *Serial Number*). La RFC 1340 récapitule la liste des numéros attribués, un court extrait en est donné figure 16.14.

Numéro constructeur (en hexadécimal)	Constructeur	Numéro constructeur (en hexadécimal)	Constructeur
00-00-0C	Cisco	08-00-02	3Com-Bridge
00-00-0F	NexT	08-00-05	Symbolics
00-00-10	Sytek	08-00-06	Siemens Nixdorf
00-00-1D	Cabletron	08-00-07	Apple
00-00-2A	TRW	08-00-09	HP
00-00-5E	IANA	08-00-0A	Nestar Systems
00-00-65	Network General	08-00-0B	Unisys
00-00-6B	MIPS	08-00-10	AT&T
00-00-77	MIPS	08-00-11	Tektronics
00-00-81	Synoptics	08-00-14	Excelan
00-00-89	Cayman Systems	08-00-20	Sun
00-00-93	Proteon	08-00-2B	DEC
00-00-A2	Wellfleet	08-00-38	Bull
00-00-A7	NCD	08-00-39	Spider
00-00-A9	Network Systems	08-00-46	Sony
00-00-AA	Xerox	08-00-4E	BICC
00-00-C0	Western Digital	08-00-5A	IBM
00-00-C9	Emulex	08-00-69	Silicon Graphics
00-AA-00	Intel	08-00-6E	Excelan
00-DD-00	Ungermann-Bass	08-00-7C	Vitalink
00-DD-01	Ungermann-Bass	08-00-90	Retix

Figure 16.14 Extrait de la RFC 1340.

➤ Les différentes adresses MAC

L'adresse individuelle ou unicast

L'adresse *unicast* est utilisée pour les échanges entre stations. Notons que tout adaptateur possède une adresse *unicast* gravée dans la carte lors de sa fabrication, mais l'administrateur du réseau peut substituer une adresse *d'unicast* locale (bit L à 1) à l'adresse d'origine de la carte.

5. La fourniture par l'IEEE d'un OUI est une prestation payante, le coût actuel est de 1 000 $ US.

© Dunod – La photocopie non autorisée est un délit

L'adresse de diffusion généralisée ou broadcast

Une adresse de *broadcast* est une adresse de diffusion générale. Tous les bits sont à 1 (FF-FF-FF-FF-FF-FF). Cette adresse est notamment utilisée pour chercher une station dont on connaît l'adresse IP mais non l'adresse MAC (protocole de résolution d'adresses, ARP ou *Address Resolution Protocol*).

L'usage abusif de *broadcast* par certaines applications peut être très pénalisant, surtout sur des liens WAN généralement à faible débit vis-à-vis du débit des liens locaux. Aussi, en principe, les routeurs ne diffusent pas les *broadcasts*, les ponts les diffusent mais il est possible de les paramétrer pour en interdire la transmission.

L'adresse de diffusion restreinte ou multicast

Une adresse de *multicast* ou de groupe (bit G = 1) désigne un ensemble de stations. Les applications fournissent à la station (couche MAC) la liste des adresses de groupe auxquelles elle doit répondre (abonnement). Ces adresses sont utilisées, par exemple, pour la diffusion vidéo. Des plages d'adresses *multicasts* ont été définies pour permettre l'encapsulation d'adresses IP *multicast*, cette plage s'étend de :

01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF (RFC 1112)

Pour autoriser une diffusion sélective, les adresses MAC du groupe de diffusion doivent être identiques. À cet effet, l'adresse MAC de chaque station du groupe est déduite de l'adresse IP *multicast* du groupe. La figure 16.15 montre comment est réalisée la construction d'une adresse *multicast* IEEE (adresse MAC) à partir d'une adresse IP *multicast* (classe D).

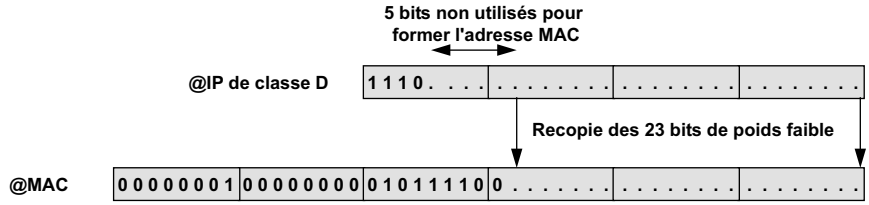


Figure 16.15 La construction d'une @MAC multicast à partir d'une @IP de classe D.

➤ Format canonique et non canonique

Les bits d'adresse sont toujours transmis bits de poids faible en premier[6] (figure 16.13), ce qui ne correspond pas à l'écriture naturelle des valeurs. Lorsque l'adresse est écrite au format IEEE (bit de poids faible en tête, octet de poids fort devant), l'adresse est dite au format canonique, les valeurs des différents octets s'écrivent en les séparant par « : », dans le cas inverse[7] (écriture naturelle), le format est dit non canonique et les différents octets sont écrits en les séparant par un tiret[8] (figure 16.14). Les réseaux de type Ethernet utilisent le format canonique, les réseaux Token Ring le format non canonique.

6. LSB (*Least Significant Bit first*) ou bits de poids faible en premier.

7. MSB (*Most Significant Bit first*) ou bits de poids fort en premier.

8. Cette convention d'écriture n'est pas toujours respectée. Dans cet ouvrage, nous n'utiliserons que la notation non canonique (sauf précision explicite), c'est-à-dire bits de poids fort devant (MSB).

Le contrôle d'erreur

La couche MAC réalise un contrôle d'intégrité. L'en-queue de la trame MAC contient le champ de contrôle d'erreur par CRC[9] sur 32 bits (**FCS**, *Frame Control Sequence*). Le polynôme générateur, identique pour tous les types de réseaux normalisés par l'IEEE, est :

$$x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + 1$$

La couche MAC rejette toute trame erronée mais n'effectue aucune reprise sur erreur. Cette tâche est éventuellement réalisée par les couches supérieures. La figure 16.16 représente le format général de la trame MAC. L'en-tête et l'en-queue sont spécifiques à chaque type de réseau.



Figure 16.16 Le format général de la trame MAC.

16.2.3 La couche liaison (LLC)

Généralités

La sous-couche **LLC**[10] (*Logical Link Control*) assure un service comparable à celui offert par la couche liaison du modèle de référence. Elle masque à la couche supérieure le type de réseau utilisé (Ethernet, Token Ring...). Les services de la sous-couche LLC sont accessibles à partir d'un point d'accès **LSAP** (*Link Service Access Point* ou point d'accès au service de liaison). Ces points sont respectivement appelés **DSAP** pour la machine destination (*Destination Service Access Point*) et **SSAP** pour la machine source (*Source Service Access Point*). La figure 16.17 illustre ces notions.

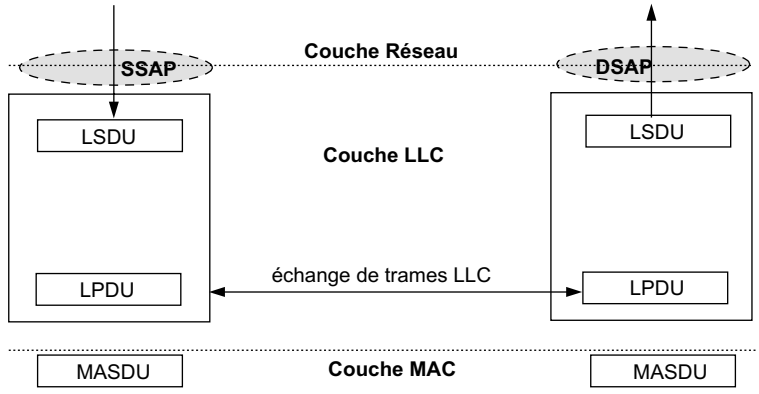


Figure 16.17 Notions de point d'accès selon le modèle OSI.

9. Voir chapitre 4 « Notion de protocole ».

10. La couche LLC est très peu utilisée dans les réseaux locaux. Mais l'encapsulation LLC (LLC1) est utilisée dans de nombreux autres environnements.

© Dunod – La photocopie non autorisée est un délit

Les unités de données délivrées par ou à la couche supérieure forment des **LSDU** (*Link Service Data Unit*), celles-ci transmettent à la couche liaison les informations nécessaires à l'envoi des données (adresses MAC source et destination, niveau de priorité, données...). Les sous-couches LLC s'échangent des **LPDU** (*Link Protocol Data Unit*) dont le format est similaire à celui des trames d'HDLC (figure 16.18).

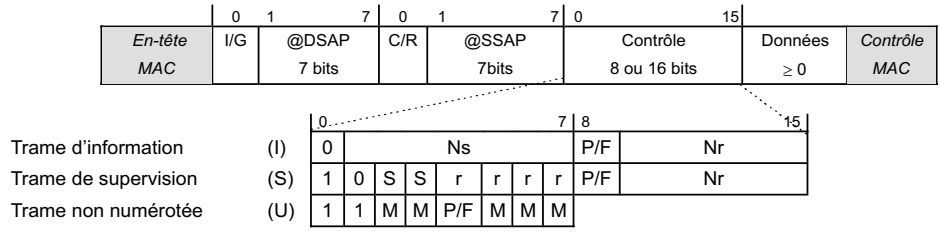


Figure 16.18 Le format général des trames LLC.

Les adresses DSAP et SSAP sont codées sur 7 bits (128 points d'accès). La notion d'adresse LSAP autorise la cohabitation de protocoles différents sur une même carte adaptateur (adresse MAC). Certaines valeurs sont réservées, la figure 16.19 fournit quelques exemples d'adresses LSAP.

LSAP	Service identifié
0X'00'	Null SAP
0X'02'	LLC Management
0X'06'	Internet ARPA
0X'AA'	SNAP
0X'F0'	NETBIOS
0X'FE'	ISO

Figure 16.19 Exemples d'adresses LSAP.

Le bit I/G indique s'il s'agit d'une adresse DSAP individuelle (I=0) ou de groupe (G=1). Tous les bits du champ adresse à 1 correspondent à l'adresse de diffusion générale (*broadcast*).

Le bit C/R distingue une trame de commande (C/R=0) ou de réponse (C/R=1), identifiant ainsi l'initiateur des échanges. À l'instar du champ Adresse de LAP-B, il sert à distinguer le bit P du bit F. À l'instar d'HDLC, le champ Contrôle, sur 8 ou 16 bits (compteurs sur 3 ou 7 bits), identifie le type de trame (I, S, U). Les bits « r » sont réservés pour un usage ultérieur.

La couche LLC offre, selon les besoins, trois types de services : LLC1, LLC2 et LLC3.

Les services de la couche LLC

➤ Le service LLC de type 1

Le service LLC1 est un service en mode datagramme. Il n'y a, par conséquent, ni acquittement, ni contrôle de séquencement, ni contrôle de flux et de reprise sur erreur. La couche MAC réalise un contrôle d'erreur, mais n'effectue pas de reprise sur erreur, toute trame erronée est purement et simplement éliminée. C'est le service le plus simple et pratiquement le seul utilisé dans les réseaux locaux. Le service rendu aux couches supérieures est limité, c'est à cette dernière de prendre en

compte les lacunes du service LLC1. Généralement, dans les réseaux locaux, c'est la couche transport qui assure ce rôle. LLC1 ne met en œuvre que deux primitives :

– L_Data. request (@Source, @Destination, LSDU, Priorité) ;
– L_Data.indication (@Source, @Destination, LSDU, Priorité).

Les adresses source (@Source) et destination (@Destination) sont constituées de l'association du LSAP source ou destination et de l'adresse MAC source ou destination. Ces valeurs sont nécessaires pour construire la trame MAC. Le champ Priorité n'est exploité que si la sous-couche MAC offre ce service.

LLC1 utilise la trame de type UI (*Unumbered Information*, champ de contrôle à 0x03) représentée figure 16.20.

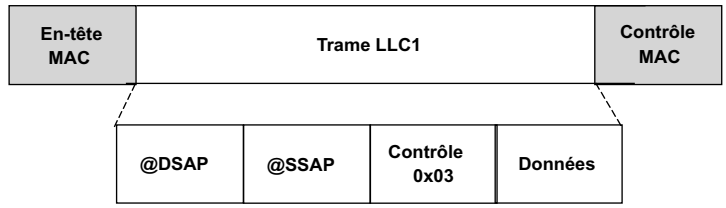


Figure 16.20 Le format de la trame LLC1.

➤ Le service LLC de type 2

Le service LLC2 est un service en mode connecté similaire à HDLC (LAP-B). Il assure l'acquittement, le contrôle de flux, le contrôle de séquencement et la reprise sur erreur. Une connexion est identifiée par l'association de l'adresse LSAP et de l'adresse MAC de la station (figure 16.21).

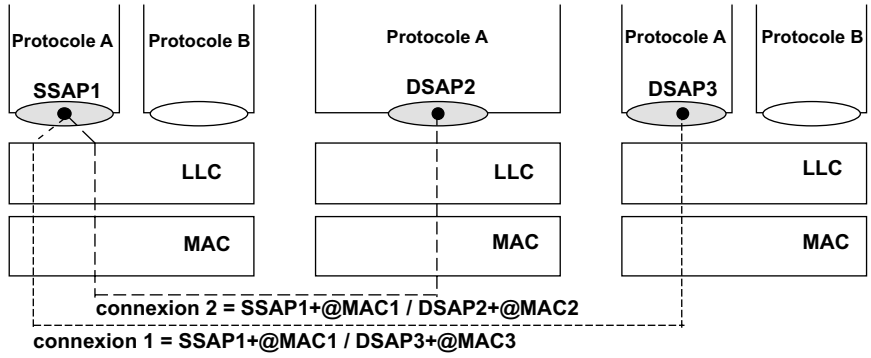


Figure 16.21 Mode connecté de LLC2.

LLC2 est un service en mode connecté, un échange de données ne peut avoir lieu qu'au sein d'une connexion et, par conséquent, ce mode interdit la diffusion.

➤ Le service LLC de type 3

Intermédiaire entre le service LLC1, simple mais non sécurisé, et le service LLC2 complexe mais qui certifie la délivrance des données, LLC3 implémente un service sans connexion (simplicité)

© Dunod – La photocopie non autorisée est un délit

mais avec acquittement (sécurisation des échanges) ; c'est un service de datagrammes acquittés. Si l'acquittement n'est pas arrivé à l'échéance du temporisateur, il n'y a pas de reprise, la perte est signalée aux couches supérieures. Ce sont elles qui décideront de l'éventuelle retransmission de la trame perdue ou d'une nouvelle trame contenant les valeurs actualisées du processus en cours.

Destiné aux systèmes temps réel (processus industriel), ce service, par sa simplicité, autorise son implémentation sur des systèmes simples (capteurs...). Le protocole prévoit un mécanisme de *polling*, le capteur n'envoie des données que lorsqu'il y est invité, ce qui limite les mécanismes à implémenter dans celui-ci.

*La sous-couche SNAP (*SubNetwork Access Protocol*)*

L'encapsulation LLC présente deux inconvénients : d'une part, elle n'identifie pas tous les protocoles et en particulier le protocole ARP (*Address Resolution Protocol*) de la pile TCP/IP et, d'autre part, en introduisant un en-tête de 3 octets, elle détruit l'alignement de la trame sur des mots machines grévant ainsi les performances. D'où la définition d'une encapsulation supplémentaire réalisée par une sous-couche spécifique : la sous-couche **SNAP** (*SubNetwork Access Protocol*). Celle-ci introduit un champ d'identification supplémentaire **PIH** (*Protocol Identifier Header*). La figure 16.22 représente l'encapsulation SNAP pour une trame MAC IEEE 802.3 (Ethernet). Les différents champs de la trame IEEE 802.3 seront expliqués lors de l'étude de ce type de réseau. L'encapsulation SNAP est identifiée par les champs DSAP et SSAP qui contiennent la valeur 0xAA.

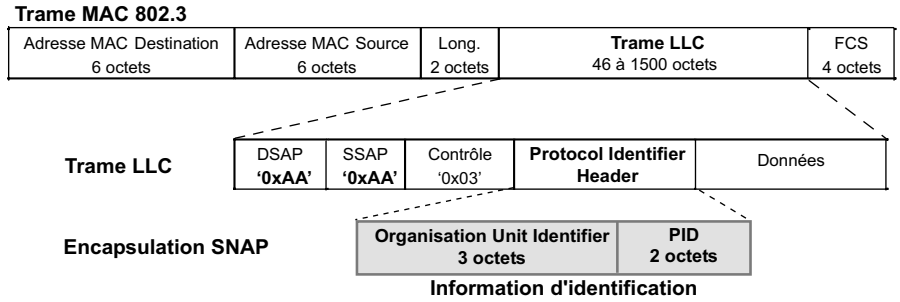


Figure 16.22 L'encapsulation SNAP.

Le **PIH** (*Protocol Identifier Header*) est divisé en deux champs : le champ **OUI** (*Organization Unit Identifier*) et le champ **PID** (*Protocol Identifier*). La valeur « 0 » du champ OUI indique que le champ PID est codé de la même façon que le champ Ethertype de la trame Ethernet.

L'encapsulation SNAP est essentiellement utilisée dans l'environnement Token Ring et dans les modes d'encapsulation utilisés par les protocoles haut débit (Frame Relay, RFC 1490 et ATM, RFC 1483).

Les interfaces de programmation NDIS et ODI

Afin d'éviter d'avoir à développer des piles protocolaires spécifiques à telle ou telle carte, les fabricants de cartes réseaux (**NIC**, *Network Interface Card*) et les éditeurs de logiciels ont introduit, entre les couches logicielles et la carte transporteur, une couche d'abstraction. Cette couche, **NDIS** pour *Network Data Interface Specification* d'origine Microsoft et 3COM ou **ODI** pour *Open Data link Interface* de Novell n'est pas une couche au sens OSI du terme puisqu'elle ne rend aucun service. Elle masque aux couches supérieures les différentes implémentations des cartes (figure 16.23).

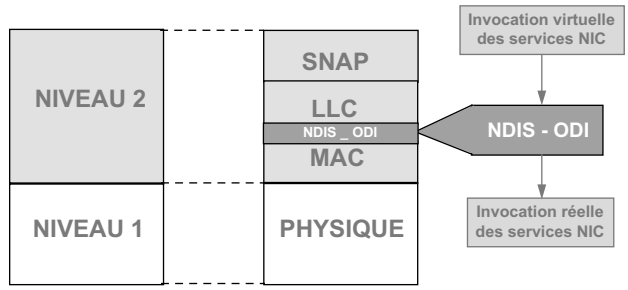


Figure 16.23 Les interfaces de programmation.

Outre l'indépendance des piles vis-à-vis des cartes, NDIS et ODI autorisent le chargement et l'utilisation simultanée de plusieurs protocoles réseaux sur une même interface physique.

16.3 ÉTUDE SUCCINCTE DES PRINCIPALES IMPLÉMENTATIONS

16.3.1 L'anneau à jeton, IEEE 802.5

Généralités

Publiée en 1985, la norme IEEE 802.5, plus connue sous le nom de Token Ring, fut implémentée par IBM dès 1986. Dans ce type de réseau, chaque station est reliée à sa suivante et à sa précédente par un support unidirectionnel (figure 16.24).

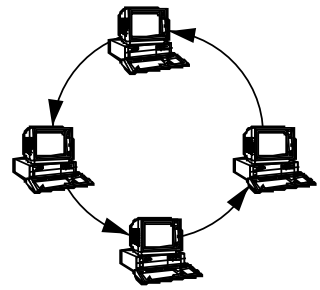


Figure 16.24 Principe de l'anneau.

Afin de centraliser la gestion de la rupture de l'anneau, le Token Ring adopte une topologie physique en étoile. Les stations sont reliées à des concentrateurs (**MAU**, *Multiple Access Unit*) comme le montre la figure 16.25.

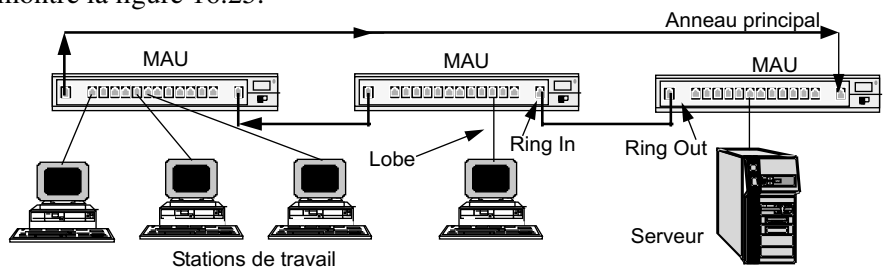


Figure 16.25 La topologie physique du réseau Token Ring.

© Dunod – La photocopie non autorisée est un délit

Principe général du jeton sur anneau

Le droit d'émettre est matérialisé par une trame particulière « le jeton ou *token* ». Celui-ci circule en permanence sur le réseau. Une station qui reçoit un jeton libre peut envoyer une ou plusieurs trames, elle devient station maître. Si elle n'a rien à émettre, elle se contente de répéter le jeton, elle est dite : station répéteur. Dans un tel système, les informations (trames) transitent par toutes les stations actives.

Le jeton ne contient pas l'adresse d'un destinataire, le destinataire est la station qui suit physiquement celle qui le détient (jeton non adressé). Le mécanisme du jeton est illustré par la figure 16.26.

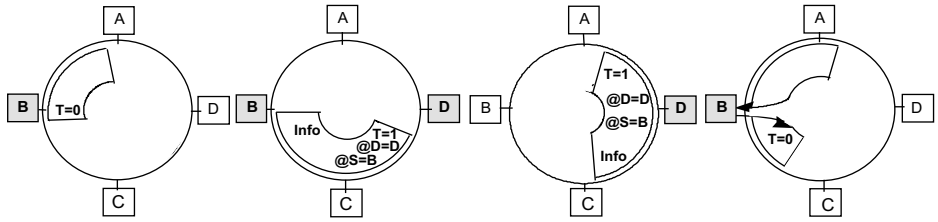


Figure 16.26 Principe du jeton.

Sur le premier schéma de la figure 16.26, la station B, qui a des données à émettre, reçoit un jeton libre. Le bit **T** (*Token*) indique si le jeton est disponible (T=0) ou indisponible (T=1). La station B ayant des données à émettre, acquiert le jeton, elle le marque occupé (T=1), et émet, à la suite du jeton, son message (@destination, @source, informations), elle devient, momentanément, le maître de l'anneau. Pour éviter qu'une station ne monopolise l'anneau, le temps de détention du droit d'émission est limité. Ce temps est, par défaut, d'environ 10 ms.

La station C lit le jeton, celui-ci est marqué occupé, elle lit l'adresse destination. Ne reconnaissant pas son adresse, le destinataire du message, elle ne fait que régénérer le message (fonction répéteur). La station D procède de même, elle reconnaît son adresse et recopie, au vol, le message. La station B reçoit alors l'en-tête du message qu'elle a émis. Elle l'ôte de l'anneau (ne le retransmet pas), et dès qu'elle a reconnu son adresse (@source) elle génère un jeton libre sur le support (T=0).

Dans la version de base, à 4 Mbit/s, un seul jeton circule en permanence sur le support (système à trame unique). Pour faire évoluer le débit à 16 Mbit/s et améliorer l'efficacité, lorsque la station maître a terminé d'émettre son message, elle génère un jeton (système à trames multiples ou protocole **ETR**, *Early Token Release*). De ce fait, plusieurs messages d'origines différentes mais un seul jeton libre peuvent circuler en permanence sur le réseau. La station maître reçoit toujours les bits qu'elle a émis. Ces bits ne sont pas répétés, la station élimine tous les bits jusqu'au délimiteur de fin de trame. Elle reprend après son rôle de répéteur.

La gestion de l'anneau

La trame 802.5 utilise deux formats de trames, les trames dites LLC pour le transport d'information et les trames dites MAC pour la gestion de l'anneau. Dans une trame MAC, le champ d'information est vide. La trame 802.5 est représentée figure 16.27.

Quatre octets spécifiques de la trame MAC 802.5 distinguent les différentes fonctions et permettent la gestion de l'anneau. Ce sont : l'octet de contrôle d'accès (*Access Control*), l'octet de contrôle de trame (*Frame Control*), l'octet de fin de trame (*End Delimiter*) et enfin, l'octet d'état de la trame (*Frame Status*).



Figure 16.27 La trame IEEE 802.5.

La distribution du droit à parole est assurée par les bits de l'octet de contrôle d'accès. Le bit **T** (*Token*) indique l'état du jeton. À zéro (T = 0), le jeton est libre et la station qui le détient peut transmettre un message. À un (T = 1), le jeton est occupé et un message suit. Le bit **M** : le bit M (*Moniteur*) est toujours à zéro dans un jeton libre et dans le message émis par la station maître. Il est positionné à 1 par une station particulière : le moniteur. Cette station a pour rôle de surveiller qu'un message ne boucle pas sur le réseau (trame orpheline). À cette fin, quand le moniteur voit passer un message, il examine la valeur du bit M. S'il est à 0, il le passe à 1. S'il est à 1, c'est que le message boucle, il aurait dû être retiré par la station émettrice. Le moniteur va dans ce cas, suppléer la station défaillante et réinitialiser l'anneau.

Les réseaux 802.5 offrent une certaine qualité de service en permettant de gérer huit niveaux de priorité. Lorsqu'une station veut émettre, elle attend le jeton. Si celui-ci est occupé, elle le réserve en positionnant les bits **RRR** (niveau de réservation). Si les bits sont déjà positionnés, la station n'en modifie la valeur que si le niveau requis est supérieur à celui de la réservation déjà effectuée. La station qui purge l'anneau (celle qui détenait précédemment le jeton), émet un jeton de la priorité (PPP) égale à la demande de réservation mémorisée (RRR). Une station ne peut prendre le jeton que si les données qu'elle a à émettre ont une priorité au moins égale à PPP.

L'octet de contrôle de trame (**FC**, *Frame Control*) du réseau 802.5 définit le type de trame qui circule sur l'anneau. Les deux premiers bits distinguent les trames d'information (trames LLC) des trames de gestion de l'anneau (trames MAC).

Le positionnement à 1 du bit **I** de l'octet délimiteur de fin de trame (**ED**, *End Delimiter*) informe le destinataire qu'une trame de même origine suit celle reçue, à 0 il indique que la trame est unique ou la dernière d'un envoi. Le bit **E** positionné à 0 par l'émetteur est basculé à 1 par la première station qui détecte une erreur ; il n'est plus modifié par la suite. Le protocole IEEE 802.5 utilise le codage Manchester différentiel. Les symboles J et K ne sont ni des 1 ni des 0, ce sont des éléments binaires sans transition au milieu du temps bit (violation de la loi de codage Manchester différentiel).

L'octet d'état de la trame (**FS**, *Frame Status*) est le dernier octet de la trame. Non protégées par le FCS, ses informations sont dupliquées. Les bits « r r » sont réservés à un usage ultérieur. Le bit **A** (*Address*) est positionné à 1 par la station qui a reconnu sa propre adresse dans le champ adresse destination. Cette station, si elle a correctement recopié la trame (accusé de réception), positionne à 1 le bit **C** (*Copy*).

D'origine IBM, le routage par la source (*Source Routing*) est un mode de fonctionnement spécifique des ponts[11] dans l'environnement Token Ring. Ces ponts, éléments d'acheminement de niveau 2, n'entretiennent aucune table d'acheminement. Ils se contentent de router les trames selon les indications contenues dans le champ d'informations de routage (**RI**, *Routing Information*) de la trame Token Ring.

© Dunod – La photocopie non autorisée est un délit

11. Voir chapitre 18.

16.3.2 Le jeton adressé ou Token Bus, IEEE 802.4

Généralités

Réseau du monde industriel, le Token Bus est aujourd'hui le seul réseau sur support filaire qui utilise un canal large bande (figure 16.28). Conçu pour fonctionner en milieu industriel, le Token Bus utilise du câble coaxial (CATV de 75 Ω), les débits possibles sont 1, 5 et 10 Mbit/s.

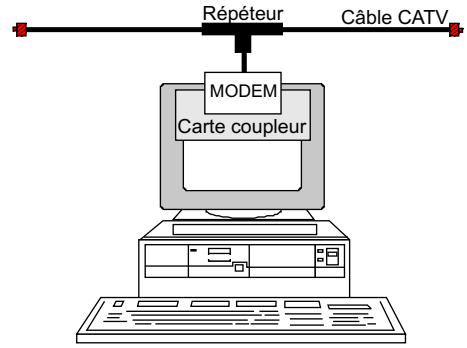


Figure 16.28 Le niveau physique du IEEE 802.4.

Le protocole IEEE 802.4 est mis en œuvre dans le réseau **MAP** (*Manufacturing Automation Protocol*).

Fonctionnement du jeton sur bus

D'une topologie physique en bus, le Token Bus est un réseau à diffusion dans lequel le droit à parole est matérialisé par un jeton qui adresse explicitement une station. Le jeton (jeton adressé), circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique).

Dans le système, représenté figure 16.29, toutes les stations en fonctionnement sur le réseau perçoivent le message (bus), mais seule, celle dont l'adresse est contenue dans le jeton considère l'avoir reçu (jeton adressé).

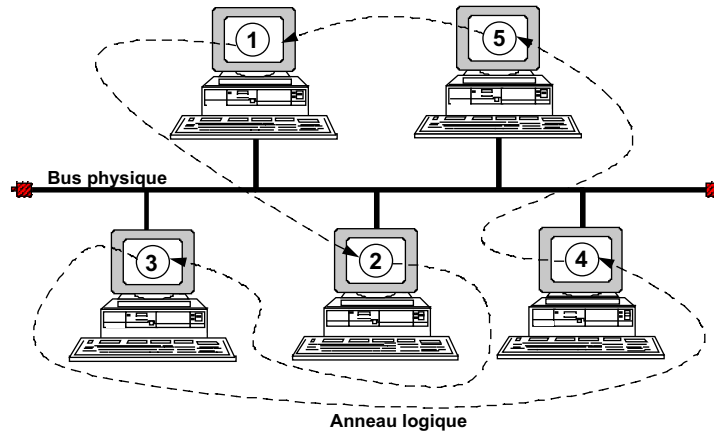


Figure 16.29 Principe du bus à jeton.

Si elle n'a rien à émettre, elle transfère immédiatement le jeton à la station suivante (adresse de la station suivante), sinon elle émet ses données puis génère un jeton à destination de la station suivante.

Cet algorithme impose que chaque station connaisse l'adresse de celle qui la suit sur l'anneau (**NS**, *Next Station address*) et de celle qui la précède (**PS**, *Previous Station address*). Se pose alors le problème de l'apprentissage, de l'insertion et du retrait d'une station.

La gestion de l'anneau

La perte du jeton ou l'initialisation de l'anneau est traitée de manière identique. La procédure d'initialisation ou de réinitialisation est déclenchée par détection d'inactivité sur le support (*timer* d'inactivité remis à zéro à chaque détection d'activité). La station qui détecte l'inactivité passe en procédure d'appel du jeton (trame *claim token*).

Cette station émet alors la trame *claim token* dont la longueur est une fonction de son adresse, puis, elle passe en écoute. Si elle détecte une activité elle abandonne, sinon elle réitère. Lorsque le silence persiste, elle se considère comme propriétaire du jeton et entreprend la procédure d'insertion pour reconfigurer l'anneau. Notons que cette procédure donne le jeton à la station de plus grande adresse (temps d'émission le plus long).

Une station ne peut s'insérer dans l'anneau que si elle y est invitée par la station dont elle doit devenir le successeur sur l'anneau. À cet effet, la station qui détient le jeton déclenche périodiquement une procédure de réveil. La procédure de réveil est déclenchée tous les N passages de jeton. N compris dans l'intervalle [16, 255] est un paramètre défini par l'administrateur du réseau. La figure 16.30 illustre le mécanisme d'insertion.

La station 5 (que nous supposerons d'adresse 5 notée : @5) attend pour s'insérer de recevoir une invitation à le faire. Celle-ci est matérialisée par une trame particulière « *solicit successor* » dont l'adresse source et destination définissent l'intervalle d'insertion. Ce message (étape 1) invite les stations, dont l'adresse est comprise entre celle de la station origine de l'invitation et sa suivante actuelle, à se manifester. Une réponse est attendue pendant un *time slot*.

La station 5, détectant que son adresse (@5) est dans l'intervalle d'insertion, répond par le message « *set successor* » et met à jour ses variables NS et PS (étape 2). La station 4 apprend ainsi que son nouveau successeur est la station 5 et lui envoie le jeton (étape 3). La station 5 transmet alors le jeton à sa suivante (@6) qui apprend ainsi que la station 5 est sa nouvelle précédente (étape 4).

Si plusieurs stations sont comprises dans l'intervalle d'insertion, elles répondent simultanément provoquant ainsi une collision sur le bus. La station origine de la trame d'insertion détecte la collision et met en œuvre un algorithme de résolution des contentions. Pour cela, elle émet une trame, *resolve contention*, cette trame définit un temps d'attente de 4 time slots.

Ne peut (ou ne peuvent) répondre pendant le premier intervalle de temps que la (ou les) station(s) dont les deux premiers bits d'adresse sont 00, pendant le second celles dont les deux premiers bits d'adresse sont 01, puis 10 enfin 11. Dès qu'une station a répondu, les autres ne répondent plus. La procédure d'insertion ne permet l'insertion que d'une seule station à la fois. Si de nouvelles collisions se produisent le mécanisme est repris, mais avec les deux bits suivants de l'adresse et ainsi de suite. Pour limiter le risque de collisions, seules les stations ayant participé à la collision précédente peuvent répondre à la trame *resolve contention*.

© Dunod – La photocopie non autorisée est un délit

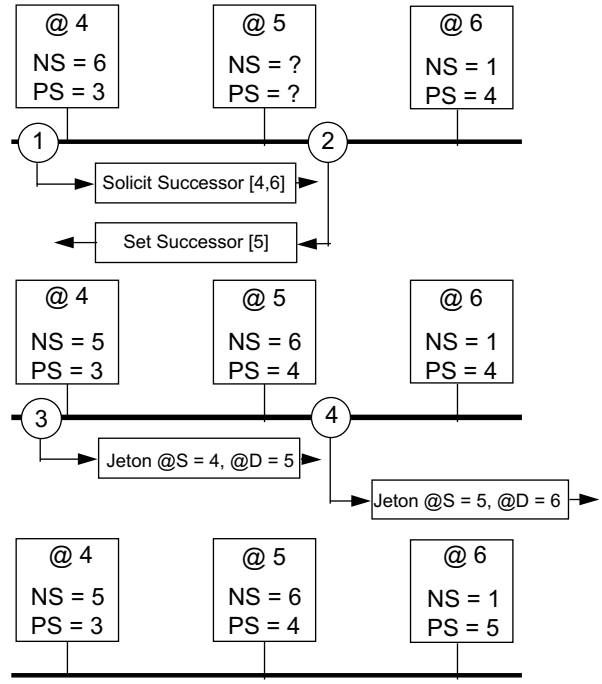


Figure 16.30 L'insertion d'une station.

Une station qui désire se retirer de l'anneau envoie, lorsqu'elle dispose du jeton, une trame *set successor* à sa précédente et le jeton à sa suivante, avec l'adresse source de sa précédente. Chaque station peut ainsi mettre ses variables à jour et la continuité de l'anneau est préservée (retrait normal d'une station).

Le réseau Token Bus est utilisé en environnement industriel, il autorise le temps réel à condition d'inhiber le mécanisme d'insertion de stations.

16.3.3 Le réseau 100 VG AnyLAN, 802.12

Généralités

D'origine HP et AT&T et normalisé par le groupe de travail IEEE 802.12, le 100 VG AnyLAN[12] implémente un nouveau protocole d'accès fondé sur la scrutation (*polling*). Les trames peuvent, selon la configuration, être au format Ethernet ou Token Ring d'où l'appellation d'AnyLAN. Se contentant de simples paires torsadées de qualité vocale (**VG**, *Voice Grade*), le 100 VG AnyLAN est défini pour un débit de 100 Mbit/s et un accès déterministe. Il admet du trafic de type isochrone.

Le réseau 100 VG AnyLAN, en raison de son protocole d'accès, utilise au maximum la bande passante (bande utile de 80 % contre 40 à 50 % pour l'Ethernet). Concurrent malheureux de l'Ethernet 100 Mbit/s, le 802.12 est resté très confidentiel. Seule, la description de sa méthode d'accès justifie son étude.

12. Le 100 VG LAN est une proposition commune d'Heweltt Packard, IBM et d'AT&T.

Le DPAM (Demand Priority Access Method)

Les stations sont raccordées à un concentrateur intelligent (hub) selon une topologie physique en étoile et pouvant ainsi réutiliser les câblages Ethernet ou Token Ring qu'il avait vocation à remplacer. Lorsqu'une station a des données à émettre, elle formule une requête au hub, qui lui alloue ou non le support (**DPAM**).

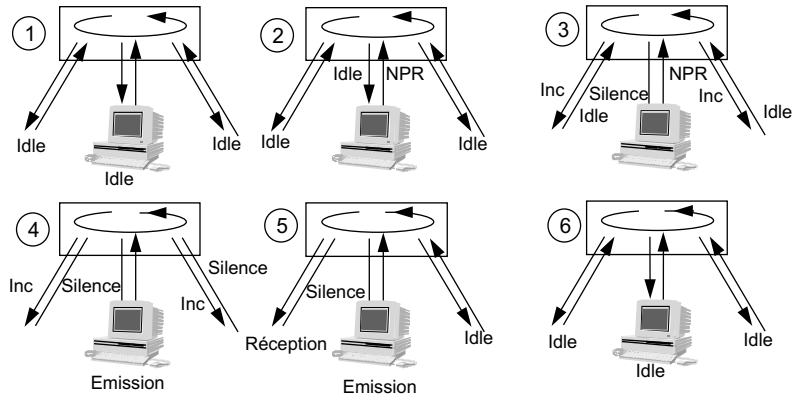


Figure 16.31 Principe du DPAM.

Les schémas de la figure 16.31 illustrent succinctement le principe de DPAM :

1. Le hub informe les stations et celles-ci informent le hub de leur disponibilité (émission du signal *Idle*).
2. La station ayant des données à émettre le signale au hub en lui envoyant une requête selon le niveau de priorité des données. Ici, ce sont des données de priorité normale, signal **NPR** (*Normal Priority Request*).
3. Le hub scrute en permanence ses différents ports (*Round robin*). Durant cette phase de *polling*, le hub détecte la demande de la station. Il informe les autres stations qui lui sont raccordées de se mettre en état de recevoir (signal *Incoming*, **INC**) et cesse son émission de Idle vers la station demanderesse (silence).
4. Les stations signalent au hub qu'elles sont prêtes à recevoir en cessant leur émission de Idle. La station demanderesse interprète la non-réception de Idle comme une autorisation d'émettre, elle transmet sa trame.
5. Le hub, à réception de cette dernière, examine l'adresse destination et retransmet la trame sur le seul port intéressé. Ce processus nécessite l'implémentation d'un protocole d'apprentissage d'adresses. Le hub reprend, vers les autres stations, l'émission de Idle.
6. À la fin du cycle, après émission et réception de la trame toutes les stations et le hub émettent les signaux Idle.

© Dunod – La photocopie non autorisée est un délit

16.4 LES RÉSEAUX LOCAUX ATM[13]

16.4.1 Généralités

Le nombre de réseaux locaux et d'applications exploitant les technologies LAN et la pile de protocoles TCP/IP font que l'introduction d'ATM dans ces environnements n'est envisageable que si cela n'induit que peu de modifications de l'existant. Or, pour tirer pleinement parti de toutes les potentialités d'ATM (garantie de qualité de service de bout en bout), il faut introduire cette technologie jusqu'au poste de travail de l'utilisateur final. Cette solution n'est envisageable que si l'environnement de travail ne s'en trouve pas modifié, or les normes ATM et LAN diffèrent.

Masquer aux applications la couche ATM implique de résoudre de nombreux problèmes comme la diffusion (ATM offre un service en mode connecté) et l'adressage, à plat dans les réseaux locaux (IEEE) et hiérarchique de type E.164 (UIT-T) ou NSAP (ISO) dans ATM.

L'aspect mode non connecté

L'émulation d'un service sans connexion peut être obtenue en spécialisant un ou plusieurs nœuds du réseau dans la diffusion des messages. Toutes les stations du réseau sont connectées *via* un circuit virtuel permanent à l'un de ces nœuds : le serveur sans connexion (**CLS**, *ConnectionLess Server*). Les différents serveurs sans connexion du réseau sont reliés entre eux par un faisceau de circuits virtuels permanents. Lorsqu'une station envoie des données, celles-ci sont adressées au serveur sans connexion, celui-ci prend en charge, pour le compte de la station source, l'acheminement et la diffusion du message aux destinataires.

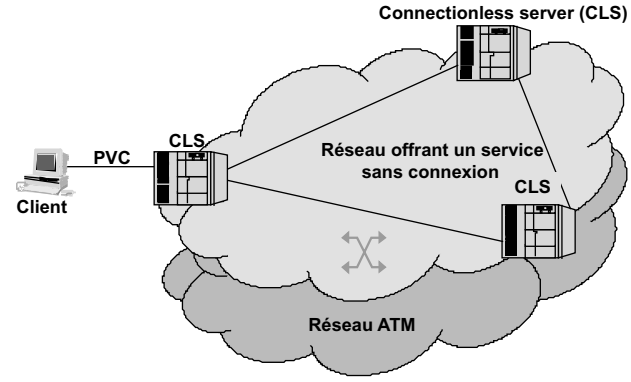


Figure 16.32 Principe du mode non connecté sur ATM.

Dans une telle architecture (figure 16.32), l'établissement d'un lien, spécifique, entre la source et le destinataire est devenu inutile (émulation du mode non connecté), tous les messages *unicats* ou *broadcasts* transitent par le serveur sans connexion qui devient vite le goulet d'étranglement du réseau.

13. Les techniques LAN ATM sont aujourd'hui obsolètes, cependant l'étude des solutions adoptées pour émuler, sur un réseau en mode connecté, un réseau en mode diffusion justifie largement l'étude de ces réseaux.

L'aspect protocolaire

Les réseaux locaux utilisent essentiellement le protocole IP du DoD. Traditionnellement, la communication entre stations d'un réseau local s'effectue après mise en correspondance, par le protocole **ARP** (*Address Resolution Protocol*), de l'adresse réseau IP et de l'adresse MAC. Dans les réseaux LAN ATM, ce sont les adresses IP et ATM qui doivent être mises en correspondance. Deux solutions ont été envisagées pour résoudre le problème d'adressage IP/ATM, (figure 16.33) :

– l'IETF (*Internet Engineering Task Force*) propose la mise en œuvre d'une pile TCP/IP particulière qui effectue directement la mise en relation d'adresses IP avec des adresses ATM (RFC 1577, *Classical IP and ARP over ATM*) ;

– l'ATM Forum quant à lui préconise l'insertion, entre les services ATM et une pile IP traditionnelle, d'une couche interface chargée d'émuler les services d'un réseau local (*LAN Emulation*). Cette couche présente, à la couche IP, une adresse MAC qu'elle met en relation avec l'adresse ATM de la station (double résolution d'adresses).

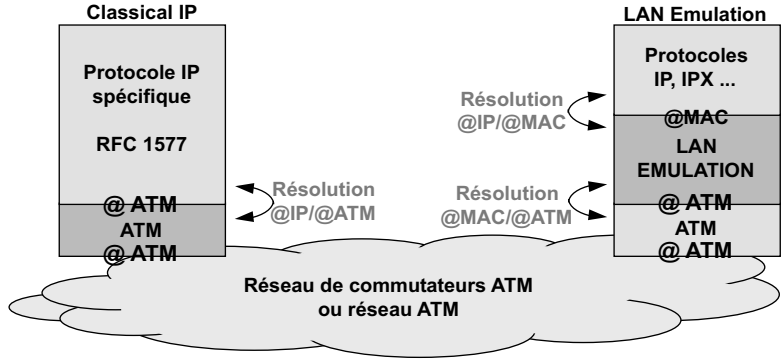


Figure 16.33 Les piles protocolaires sur les LAN ATM.

La compatibilité complète de l'implémentation d'IP sur ATM est l'avantage majeur de ces deux approches. Toutefois :

– seules les communications entre machines d'un même réseau logique peuvent communiquer directement et bénéficier de la garantie de service d'ATM ;

– le temps d'établissement des circuits virtuels pénalise les performances lors de transfert de données de faible volume ;

– tous les paquets entre deux systèmes partagent le même circuit virtuel, ce qui rend impossible de garantir à un flux spécifique une qualité de service données.

16.4.2 « *Classical IP* » ou « *IP over ATM* »

Principes généraux

Classical IP (**CLIP**) ou mode natif définit un réseau IP comme un sous-réseau logique (**LIS**, *Logical IP Subnetwork*) de manière similaire à un réseau IP traditionnel. Un LIS est un ensemble de machines IP connectées à un réseau ATM (figure 16.34) partageant un même préfixe d'adresse IP.

© Dunod – La photocopie non autorisée est un délit

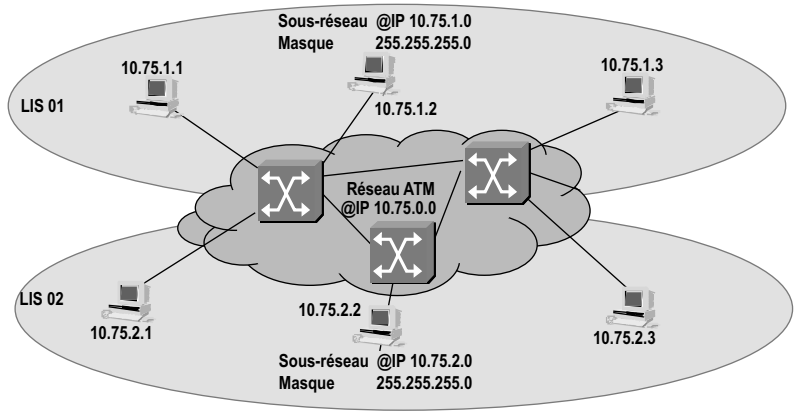


Figure 16.34 Principe du Classical IP.

Les stations d'un même sous-réseau (LIS) communiquent directement entre elles après avoir établi un circuit virtuel. Les stations de deux sous-réseaux différents communiquent *via* un routeur.

La communication intra-LIS

Pour communiquer, les stations doivent établir un circuit virtuel, ce qui nécessite que la station source connaisse l'adresse ATM du destinataire. La fonction de résolution d'adresses (mise en correspondance de l'adresse IP avec l'adresse ATM de la station) est assurée par un serveur d'adresses (serveur ATMARP) qui, sur sollicitation d'une requête **ATMARP** (*ATM Address Resolution Protocol*), retourne au client l'adresse ATM correspondante. Chaque réseau logique (LIS) possède son propre serveur ATMARP (figure 16.35).

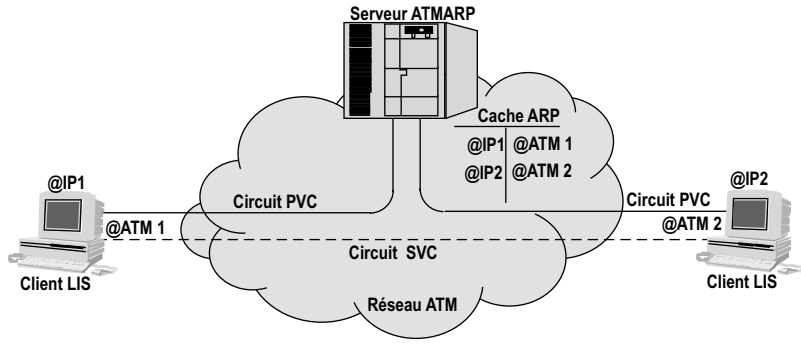


Figure 16.35 Principe d'un serveur ATMARP.

La communication inter-LIS

La communication entre stations de LIS différents transite par un ou plusieurs routeurs intermédiaires (figure 16.36). La mise en relation s'effectue en deux temps : la station source établit un circuit virtuel (SVC) avec le routeur, ce dernier à son tour établit un circuit avec la station destinataire ou un autre routeur. Le routeur entretenant un grand nombre de SVC constitue un goulet d'étranglement.

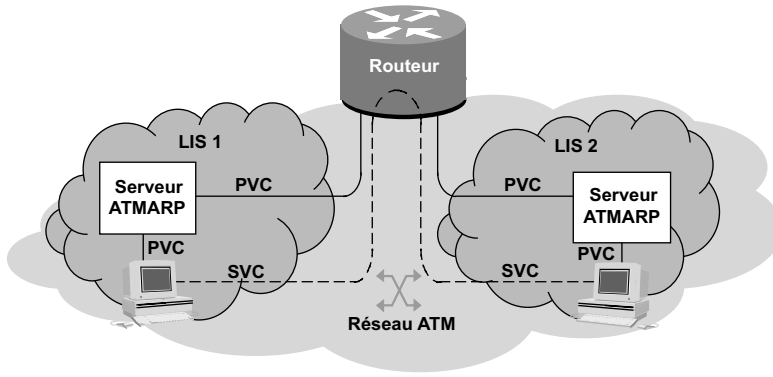


Figure 16.36 Principe de la communication inter-LIS.

Le format des données (RFC 1 483)

Classical IP utilise AAL5 et la RFC 1 483 pour l'encapsulation des données. Dans la figure 16.37, le paquet IP subit une double encapsulation : LLC (*Logical Link Control*) et SNAP (*SubNetwork Access Protocol*) déjà décrite précédemment. C'est cette trame qui est remise à l'AAL5, la MTU est fixée à 9 180 octets.

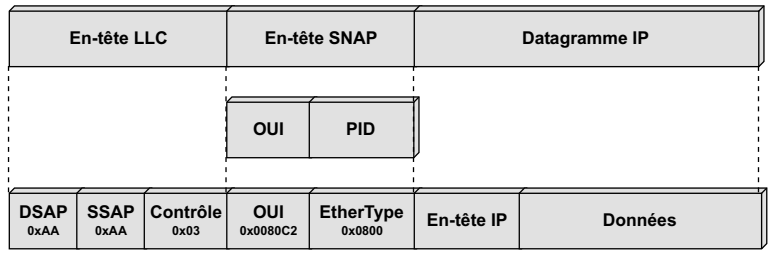


Figure 16.37 Le format d'encapsulation RFC 1483.

16.4.3 *LAN Emulation*

Généralités

Utilisant une pile IP spécifique, *Classical IP* ne peut communiquer avec les LAN traditionnels (*Legacy LAN*). N'implémentant pas de serveur de diffusion, il ne peut assurer un trafic de *multicast* ou de *broadcast*. *LAN Emulation* pallie ses défauts en introduisant entre les services ATM et les protocoles réseaux une couche spécifique émulant, vis-à-vis des protocoles supérieurs, les fonctions d'un LAN traditionnel (figure 16.38).

L'interface LAN Emulation (**LUNI**, *LAN emulation User to Network Interface*) d'une station cliente (**LEC**, *LAN Emulation Client*) fournit un service MAC en mode non connecté aux couches supérieures. Cette interface a deux adresses, une adresse MAC vue des couches supérieures et une adresse ATM vue du réseau ATM. Le LEC utilise l'AAL5 pour le transfert des données et la SAAL (*Signaling* AAL) pour la signalisation (signalisation Q.2931), et en particulier pour l'établissement et la libération des circuits virtuels commutés (SVC).

© Dunod – La photocopie non autorisée est un délit

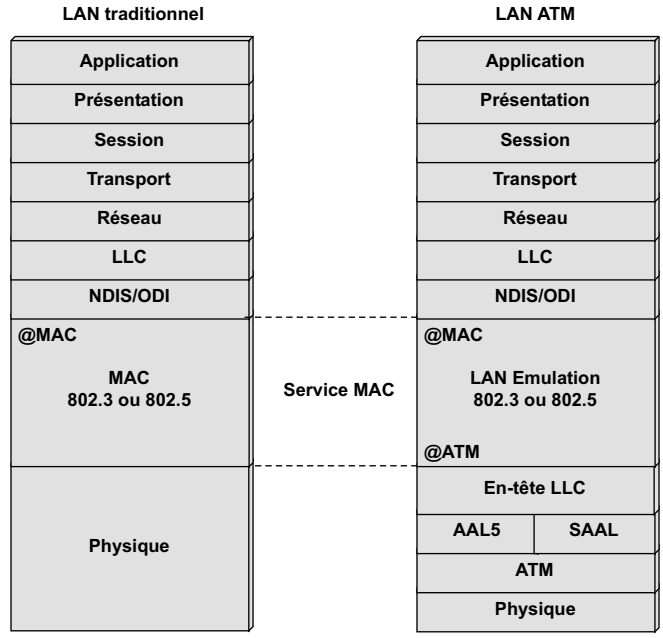


Figure 16.38 L'architecture d'un LAN traditionnel et d'un LAN ATM.

Chaque LEC entretient un cache ARP (correspondance entre les adresses ATM et MAC des stations connues). Le LEC peut être configuré pour délivrer des trames MAC au format 802.3 ou 802.5, le champ FCS de la trame MAC n'est pas utilisé. Tous les LEC d'un même réseau émulé[14] (**ELAN**, *Emulated LAN*) doivent utiliser le même format de trames MAC. Un LEC ne peut appartenir qu'à un seul ELAN. Si un système d'extrémité doit être connecté à plusieurs ELAN, il possédera un LEC par ELAN rejoint et une interface physique ou logique par LEC.

Les composants d'un LAN ATM (ELAN)

Les différents nœuds d'un réseau local émulé (ELAN, *Emulated LAN*) constituent un réseau virtuel. Un réseau ATM peut comporter plusieurs ELAN (figure 16.39). Chaque ELAN est identifié par un nom (ELAN-ID). La fonction LEC (*LAN Emulation Client*) est présente dans tous les nœuds d'un ELAN. Les différents services d'un ELAN sont offerts par :

– le **LES** (*LAN Emulation Server*), similaire au serveur ATMARP du *Classical IP*, il assure la mise en relation d'une adresse MAC et d'une adresse ATM. Cette fonction est généralement localisée dans un commutateur ATM. Il y a un LES par ELAN ;
– le **BUS** (*Broadcast and Unknown Server*) fournit les services de diffusion aux trames MAC de diffusion (*broadcast* ou *multicast*). Il est aussi chargé de la résolution d'adresses pour les LEC non connus du LES (diffusion d'une requête LE-ARP). Les fonctions du BUS sont réalisées par le même commutateur que celui qui héberge les fonctions LES. Il y a un serveur BUS par

14. Ne pas confondre les termes ELAN et LANE. LANE *(LAN Emulation*) est la technique mise en œuvre sur ATM pour émuler, sur ce dernier, un réseau local (ELAN, *Emulated LAN*).

ELAN. Chaque LEC entretient une connexion permanente avec le serveur BUS. Si le LAN émule un réseau Token Ring, le BUS émule l'anneau en assurant le passage des trames (jeton compris) de système terminal à système terminal selon un ordre préétabli ;

– enfin, le **LECS** (*LAN Emulation Configuration Server*) fournit un service d'autoconfiguration de type « *plug and play* ». Sur la requête d'un LEC, le LECS affecte le LEC à un ELAN en lui fournissant l'adresse du LES pour qu'il puisse s'enregistrer auprès de ce dernier. Le LECS est commun à tous les ELAN d'un même réseau ATM.

Les échanges inter-ELAN doivent transiter par un pont ou un routeur. La figure 16.39 décrit la topologie générale d'un LAN ATM.

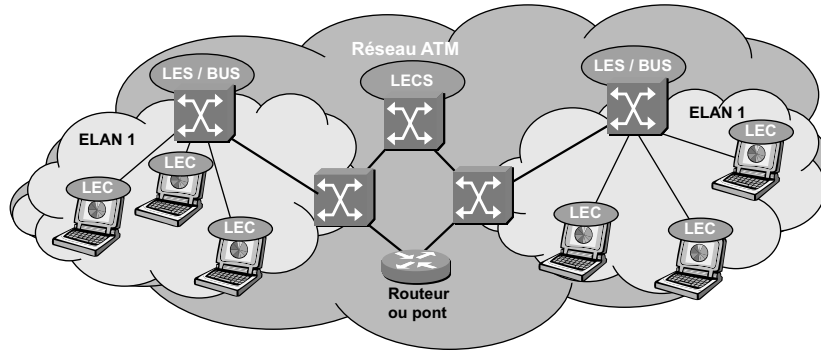


Figure 16.39 La topologie d'un LAN ATM.

*Le fonctionnement des ELAN (*Emulated *LAN)*

Pour transférer des données entre deux clients, il faut établir une connexion (*Data Direct VCC*) entre les clients. Pour cela, le LEC source doit disposer de certaines informations qui lui ont été fournies, à la configuration du système, par l'administrateur. Il s'agit notamment de sa propre adresse ATM et de l'identifiant de son ELAN de rattachement (ELAN-ID). D'autres informations lui sont fournies par le **LES** (*LAN Emulation Server*) de son ELAN auprès duquel il doit s'enregistrer (résolution d'adresses) et obtenir l'adresse ATM du destinataire. Cette procédure comprend les étapes suivantes :

– **Initialisation du LEC** (LAN *Emulation Client*) ; dans cette phase le LEC obtient près du LECS (LAN *Emulation Configuration Server*) l'adresse ATM du LES (LAN *Emulation Server*).

– **Enregistrement auprès du LES** (LAN *Emulation Server*), une fois l'adresse du LES connue, le LEC établit une connexion bidirectionnelle en point à point (*Control Direct VCC*) avec son LES. Ce dernier lui attribue un identifiant sur deux octets (LEC-ID, *LEC-Identifier*), et lui indique le type de réseau émulé (Ethernet, Token Ring) et la taille maximale des trames de données (MTU). Le LEC s'enregistre alors auprès du LES en lui fournissant son adresse MAC.

– **Connexion au BUS** (*Broadcast Unknown Server*) le LEC doit auparavant obtenir son adresse auprès du LES. Le LEC émet, vers le LES, une requête LE-ARP (LAN *Emulation* ARP) pour l'adresse de diffusion « FFFFFFFFFFFF ». L'adresse ATM du BUS obtenue, le LEC ouvre une connexion point à point bidirectionnelle avec le BUS (*Multicast Send VCC*), le BUS en retour ouvre une connexion unidirectionnelle en point à multipoint avec le LEC (*Multicast Forward VCC* ou *Multicast Distribute VCC*).

© Dunod – La photocopie non autorisée est un délit

La figure 16.40 récapitule toutes les connexions ouvertes durant les différentes phases d'adhésion d'un LEC à un ELAN.

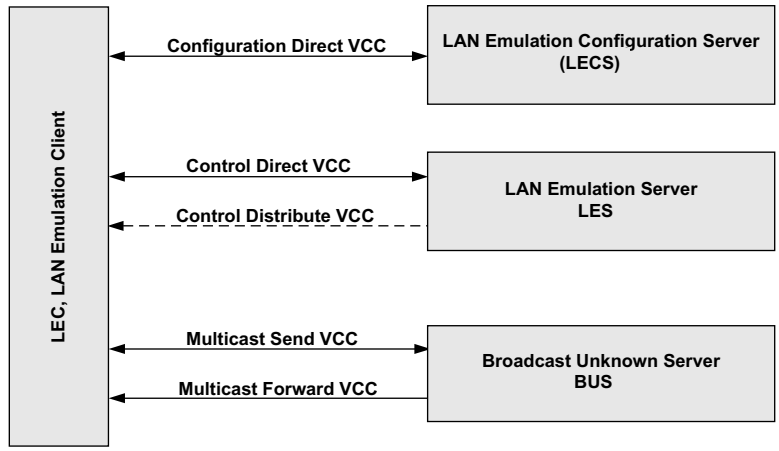


Figure 16.40 Les liens entre le LEC et les différents serveurs de l'ELAN.

L'interconnexion de réseaux LANE (MPOA)

Défini par l'ATM Forum, **MPOA** (*MultiProtocol Over ATM*) permet aux protocoles de niveau 3 comme IP, IPX, Appletalk, etc., d'exploiter les possibilités d'ATM (débit, qualité de service...). MPOA autorise, sans transiter par un routeur, une communication directe entre deux systèmes d'extrémité n'appartenant pas au même réseau logique virtuel (VLAN ou subnet différent). La figure 16.41 illustre les techniques LANE et MPOA.

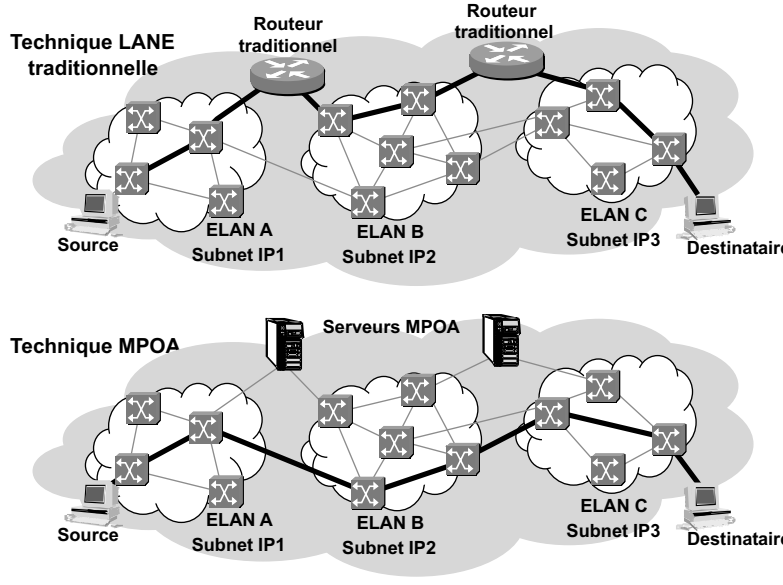


Figure 16.41 Principe de MPOA.

Dans la technique LANE traditionnelle, tout le flux de données transite par le routeur. Tandis que, dans l'approche MPOA, une fois le flux identifié (couple @IP source/@IP destination), un circuit virtuel commuté (VCC) est établi entre les deux équipements d'extrémité.

MPOA exploite la technologie LANE (LAN *Emulation*) et pallie ses limites en offrant une émulation transparente des protocoles réseaux s'exécutant au-dessus d'ATM. MPOA assure une connectivité de niveau 3 de bout en bout entre les systèmes d'extrémité, qu'ils soient directement raccordés à une infrastructure ATM ou à un sous-système de technologie antérieure.

L'avantage primordial de l'approche MPOA réside dans le fait que chaque système intégrant une interface MPOA peut établir des connexions ATM directes (sans intermédiaire) de type *unicast*, *multicast* et *broadcast*. La figure 16.42 présente l'architecture d'un réseau MPOA.

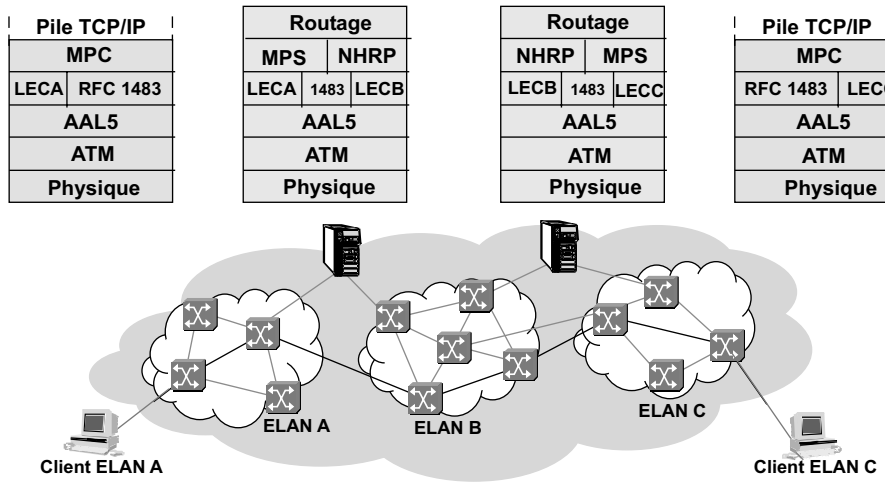


Figure 16.42 L'architecture d'une interconnexion MPOA.

À l'instar de LANE, MPOA fonctionne selon le modèle client/serveur. Il comporte deux éléments :

– le client (*MPOA client*, **MPC**), élément logiciel résident dans l'équipement terminal ou le commutateur de bordure[15] (*Edge device*) raccordé à ATM. Le client MPC inclut les services de la RFC 1483 pour assurer un transfert de données hors LEC ;
– le serveur (*MPOA server*, **MPS**), extension logicielle résidente dans les routeurs interréseaux.

MPOA ne fonctionne que sur LANE2. La communication entre MPC (MPOA *Client*) et MPS (MPOA *Serveur*) s'effectue *via* les LAN Emulation Clients (LEC). La communication entre serveurs MPOA (MPS) utilise le protocole NHRP (*Next Hop Routing Protocol*).

15. C'est par exemple le cas d'un commutateur Ethernet disposant d'un raccordement ATM.

© Dunod – La photocopie non autorisée est un délit

16.5 LES RÉSEAUX MÉTROPOLITAINS

16.5.1 Généralités

À l'origine, les réseaux métropolitains (**MAN**, *Metropolitan Area Network*) étaient essentiellement destinés à l'interconnexion de réseaux locaux d'entreprise. Fédérateurs de réseaux, ils offraient, au regard du débit des composantes locales, des débits élevés ($\geqslant$ 100 Mbit/s), et couvraient des distances importantes ($\geqslant$ 100 km). Devant le besoin croissant de débit, ils ont été utilisés en lieu et place des LAN traditionnels. Ces réseaux pouvaient donc à la fois être considéré comme des réseaux locaux (LAN), s'ils étaient utilisés essentiellement pour leur débit (100 Mbit/s ou plus) ou comme réseaux métropolitains s'ils l'étaient pour leurs caractéristiques de distance et les possibilités d'interconnexion de LAN.

Deux technologies ont longtemps dominé ce secteur : **FDDI** (*Fiber Distributed Data Interface*) et **DQBD** (*Distributed Queue Dual Bus*). Ces techniques sont aujourd'hui obsolètes face au Gigabit Ethernet dans les composantes locales et du 10 voire 40 Gigabit Ethernet dans les boucles locales.

16.5.2 FDDI (*Fiber Distributed Data Interface*)

Généralités

D'origine ANSI (ANSI X3T9.5), la technique FDDI a été normalisée par l'ISO (ISO 9314). FDDI est un réseau en anneau optique sur fibre optique multimode. L'anneau est en fait un double anneau, ce qui permet une autocicatrisation du réseau en cas de défaillance d'un lien ou d'un nœud (figure 16.43). Le débit nominal est de 100 Mbit/s pour une distance maximale de 100 km. FDDI supporte jusqu'à 1 000 stations, distantes l'une de l'autre de moins de 2 km.

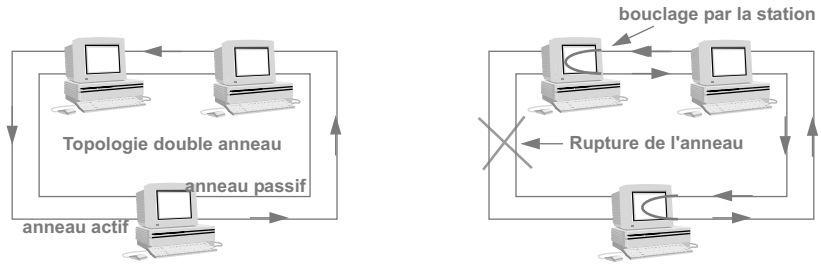


Figure 16.43 La reconfiguration rapide de l'anneau.

Une version de FDDI sur paire torsadée (**TPDDI**, *Twisted Pair Distributed Data Interface*) autorise des débits de 100 Mbits sur 100 m.

La méthode d'accès est similaire à celle du réseau IEEE 802.5 version 16 Mbit/s (**ETR**, *Early Token Release*). Pour accéder au support, une station doit posséder le jeton. Elle émet ses données puis génère un nouveau jeton. Chaque station retire de l'anneau les données qu'elle y a déposées. Plusieurs trames de données, issues de stations différentes, peuvent circuler sur l'anneau, mais il n'y a qu'un seul jeton libre à la fois.

En définissant deux types de données : les données urgentes à contrainte de débit (classe synchrone) et les données sporadiques, sans contrainte particulière de débit (classe asynchrone), FDDI introduit aussi une notion réduite de la qualité de service. Lorsqu'une station possède le jeton, elle

peut toujours émettre des données synchrones (données prioritaires) et, si et seulement si, le jeton est en avance (jeton temporisé), elle peut alors émettre des données asynchrones.

La méthode d'accès : le jeton temporisé

Pour garantir une certaine bande passante à chaque station, FDDI implémente une technique d'accès originale. Le jeton est dit temporisé : à l'initialisation de l'anneau une autonégociation détermine, en fonction des contraintes de chaque station, un temps maximal au bout duquel une station doit disposer du jeton (protocole déterministe), fixant aussi, pour garantir ce délai d'accès aux autres stations, un temps maximal d'émission (données de la classe synchrone). Le mécanisme du jeton temporisé (*Timed Token Protocol*) est contrôlé par trois variables d'état (figure 16.44) :

- **TTRT** (*Target Token Rotation Time*) : cette variable indique le temps maximal au bout duquel une station doit recevoir le jeton. La valeur de TTRT est négociée lors de l'initialisation de l'anneau. Chaque station propose, en fonction de ses contraintes de débit, une valeur maximale admissible de TTRT. C'est la plus faible valeur qui est retenue, celle de la station qui a les plus fortes contraintes de trafic. Chaque station dispose d'un temps d'émission défini (*Ts*), réservé à l'émission de données de la classe synchrone, tel que la somme de ces temps soit inférieure à TTRT (TTRT > [*Ts* • *N*] où *N* représente le nombre de stations actives).
- **TRT** (*Token Rotation Timer*) : ce *timer* est initialisé à la valeur de TTRT à chaque réception d'un jeton, puis il décroît linéairement jusqu'à l'arrivée effective du jeton. Si le jeton arrive avant l'expiration du TRT, la station peut émettre des données asynchrones pendant le temps restant (THT) et des données synchrones pendant le temps d'émission qui lui est imparti (*Ts*). Si le jeton arrive alors que TRT est nul, elle ne peut émettre que des données synchrones pendant le temps *Ts*. TRT ne mesure pas le temps de rotation du jeton, mais l'avance de celui-ci.
- **THT** (*Token Holding Timer*) : ce temporisateur mesure le temps d'émission de données de la classe asynchrone. Quand le jeton arrive en avance, THT est initialisé à la valeur actuelle du TRT (avance du jeton), et TRT est réinitialisé à TTRT. La station peut alors émettre des données de la classe asynchrone durant le temps THT et des données de la classe synchrone durant le temps *Ts*.

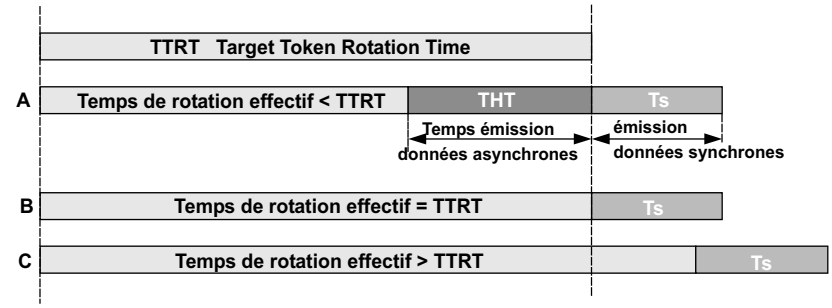


Figure 16.44 Les variables de gestion des temps d'émission.

© Dunod – La photocopie non autorisée est un délit

La figure 16.44 représente ces variables dans différents cas, les valeurs sont celles vues d'une station. En **A**, le temps de rotation effectif du jeton est plus petit que TTRT, la station émet des données de la classe synchrone pendant *Ts* (les données synchrones sont toujours émises en premier) et de la classe asynchrone pendant THT (la figure matérialise des temps d'émission et non l'ordre d'émission). En **B** et **C** le temps de rotation effectif est égal ou plus grand que TTRT, la station ne peut émettre que des données synchrones.

L'évolution de FDDI : FDDI-II

FDDI offre une bande passante minimale aux données de la classe synchrone mais ne garantit pas une récurrence temporelle entre les différentes émissions. De ce fait, FDDI n'est pas susceptible d'assurer des transferts de données de type isochrone (voix, vidéo). Pour pallier cette limitation, FDDI-II multiplexe sur le support une voie asynchrone et synchrone (fonctionnement en mode paquet) et une voie isochrone (fonctionnement en mode circuit). La figure 16.45 présente l'architecture générale du réseau FDDI-II.

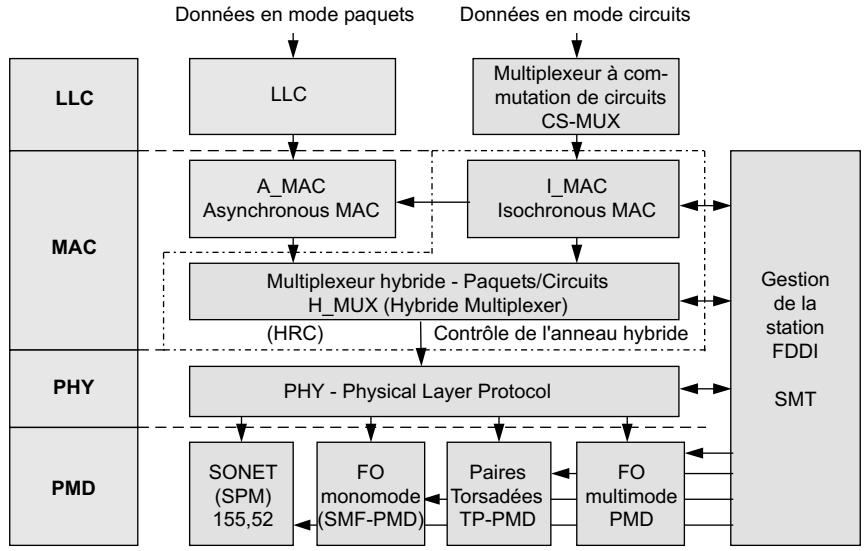


Figure 16.45 L'architecture du réseau FDDI-II.

Si le trafic généré est du type paquet, la station FDDI-II fonctionne en mode de base. Lorsque du trafic paquet et du trafic isochrone sont multiplexés sur le support, elle fonctionne en mode hybride. Une station maître (*Cycle master*) génère une trame de 12 500 bits toutes les 125 μs.

FDDI-I a toujours eu du mal à se positionner entre les LAN et le MAN. La version 2 arrivée trop tard n'a connu aucun succès.

16.5.3 DQDB (*Distributed Queue Dual Bus*)

Généralités

Issu des laboratoires de l'université de Western Australia et soutenu par les télécommunications australiennes (Telecom Australia), le réseau QPSX (*Queue Packet Dual Bus*) a été normalisé par

l'IEEE et l'ISO (IEEE 802.6, ISO 8802.6) comme réseau métropolitain (MAN) sous le nom de **DQDB**.

Développé parallèlement à **ATM** (*Asynchronous Transfer Mode*), DQDB en utilise le format (cellule de 53 octets dont 48 de charge utile). Parfois considéré comme une technologie pré-ATM, il permet le transfert de données isochrones et asynchrones (mode connecté et non connecté). Les débits disponibles sont de 45, 155 et 622 Mbit/s.

DQDB utilise un double bus unidirectionnel (figure 16.46). Sur chaque bus, une tête de bus (**HoB**, *Head of Bus*) génère, toutes les 125 μs, une trame (trame DQDB) contenant *n slots* ou cellules de 53 octets. Le nombre de slots par trame (*n*) dépend du débit du réseau. Le premier bit de chaque *slot* (bit *Busy*) indique l'état du slot (libre ou occupé).

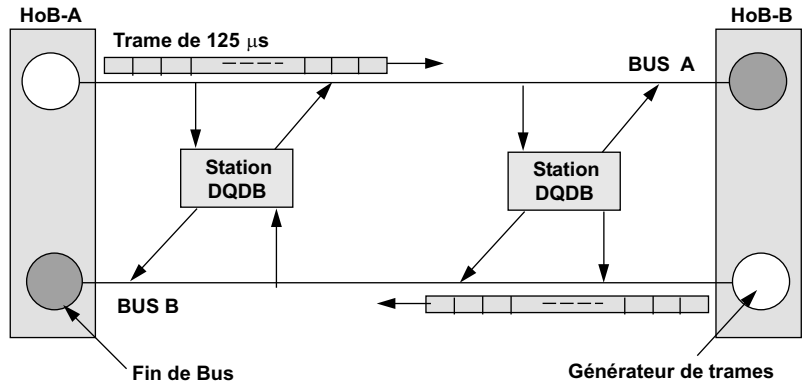


Figure 16.46 Principe général du réseau DQDB.

Chaque station, qui a des données à émettre, les dépose dans un *slot* vide attribué de manière statistique pour le transfert de données asynchrones ou selon un préarbitrage, pour les données isochrones. Une station lit ou écrit au vol les données (fonction « OU logique ») dans une cellule ; elle ne les retire pas, la cellule les contenant s'évanouit en fin de bus (fonction d'absorption). Les stations sont à l'écoute des deux bus (bus A et bus B). L'émission n'a lieu que sur un seul bus en fonction de la position physique de la station avec laquelle elles veulent communiquer. Les messages de diffusion (*broadcast*) sont émis sur les deux bus.

L'architecture générale de DQDB

DQDB offre trois types de service : transfert asynchrone en mode connecté et non connecté et le transfert isochrone. La couche MAC comprend un ensemble de fonctions spécifiques à chaque type de transfert (figure 16.47) :

– **MCF** (*MAC Convergence Function*) offre un service asynchrone sans connexion (service de type datagramme) qui est particulièrement adapté aux transferts en mode rafales (transfert de données entre ordinateurs) ;

– **COF** (*Connection Oriented Function*), ce service (comme le précédent) est dédié aux transferts asynchrones mais en mode connecté. Un circuit virtuel (mode orienté connexion) est établi préalablement à l'échange de données. Ce type de service est essentiellement destiné aux applications de type conversationnel ;

© Dunod – La photocopie non autorisée est un délit

– **ICF** (*Isochronous Convergence Function*) offre un service de transfert de type isochrone qui garantit un débit constant et une récurrence temporelle parfaite entre les blocs de données transportés. Ce service est destiné aux applications de type voix et vidéo (flux isochrone).

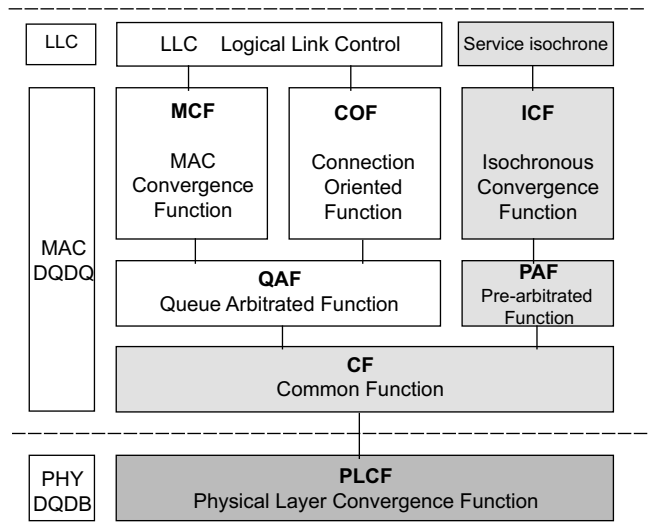


Figure 16.47 L'architecture du réseau DQDB.

L'accès au support partagé est géré par deux entités : l'une prend en charge le trafic isochrone (**PAF**, *Pre-Arbitrated Function*) et l'autre le trafic asynchrone (**QAF**, *Queue Arbitrated Function*).

Le service SMDS et CBDS

D'origine Bellcore, la proposition **SMDS** (*Switched Multimegabits Data Service*) reprise en Europe sous l'appellation **CBDS** (*Connectionless Broadand Data Service*) offre un service d'interconnexion de réseaux en mode non connecté. S'appuyant sur l'AAL5 d'ATM, SDMS offre une interface utilisateur similaire à celle de DQDB. Il a souvent été perçu comme une solution d'accès provisoire aux réseaux ATM. Cette solution a surtout été mise en œuvre pour l'interconnexion des réseaux locaux.

16.6 LES CANAUX HAUTS DÉBITS

D'abord définis comme de simples interfaces haut débit entre calculateurs et périphériques, les canaux hauts débits se sont rapprochés des réseaux de diffusion avec l'introduction de commutateurs qui ont autorisé les relations multiples entre périphériques à haut débit ou stations de travail. Les principales solutions d'interconnexion de cette catégorie sont les interfaces **HiPPI** et **Fibre Channel**.

16.6.1 HiPPI

L'interface **HiPPI** (*High Performance Parallel Interface*), normalisée par l'ANSI (ANSI X3.183, X3.222), est un canal de transmission haut débit (800 Mbit/s) entre un calculateur et ses périphériques. HiPPI définit un mode de transmission unidirectionnelle en parallèle sur un support cuivre (paires torsadées, une paire par bit) en mode connecté. Deux interfaces HiPPI sont nécessaires pour réaliser une communication *full duplex*. L'interface d'origine (800 Mbit/s) utilise un câble 50 paires dont 32 pour la transmission de données (mot de 32 bits), les paires restantes (18 bits) servent à la signalisation (figure 16.48), la distance maximale est de 25 m. Un débit de 1,6 Gbit/s peut être obtenu par l'utilisation simultanée de deux câbles de 50 paires (mots de 64 bits).

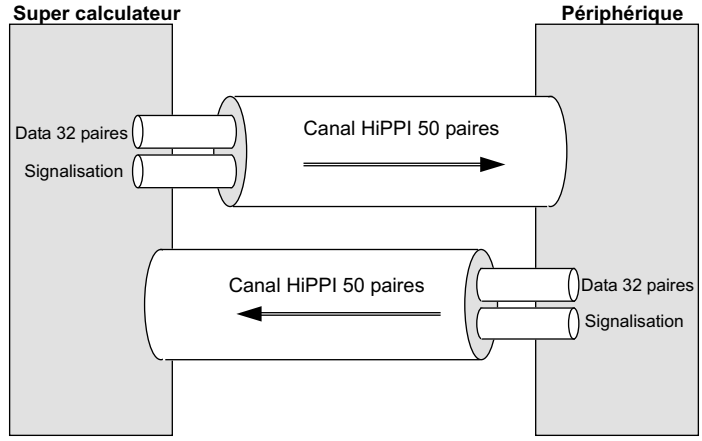


Figure 16.48 Principe des canaux HiPPI.

La transmission se fait en mode paquet par rafale. HiPPI fournit les mécanismes nécessaires au contrôle d'erreur (bit de parité), au contrôle de flux et à l'adressage des différents périphériques. L'efficacité de la synchronisation est garantie par un codage des signaux du type 20B/24B. L'introduction d'un commutateur de type *crossbar* (HiPPI-SC, *Crossbar Switch*) a permis le partage d'un même canal par plusieurs périphériques ou calculateurs, une seule interface est alors nécessaire pour chaque élément raccordé au réseau HiPPI ainsi formé.

Compte tenu de la limitation à 25 m, une interface optique a été définie (*Serial HiPPI*) dont la portée est alors de 1 km pour la fibre multimode et de 10 km pour la fibre monomode.

16.6.2 *Fibre Channel Standard*

Évolution des canaux sur fibre optique, **FCS** (*Fibre Channel Standard*) définit une interconnexion à haut débit en mode série autour d'un commutateur spécifique appelé la « *Fabric* » (figure 16.49).

Le commutateur principal (*Fabric*) assure les fonctions de routage (adressage sur 24 bits du type hiérarchique), de contrôle d'erreur et de contrôle de flux. Il supporte les protocoles de haut niveau comme IP (*Internet Protocol*), les interfaces IPI (*Intelligent Peripherical Interface 3*), SCSI (*Small Computer System Interface*) et HiPPI.

© Dunod – La photocopie non autorisée est un délit

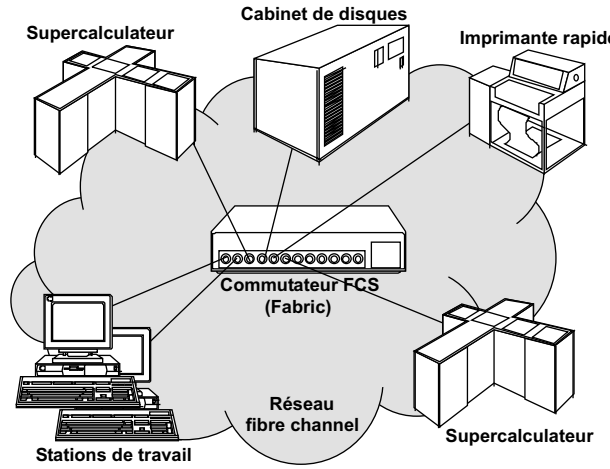


Figure 16.49 Principe du FCS (Fibre Channel Standard).

16.7 CONCLUSION

Les réseaux locaux constituent aujourd'hui le moyen d'accès aux systèmes d'information le plus utilisé, mais la plupart des réalisations présentées dans ce chapitre sont aujourd'hui considérées comme obsolètes. Malgré la supériorité des méthodes d'accès contrôlé, le marché a choisi les solutions à contention. Les réseaux locaux sont aujourd'hui dominés par les réseaux de types Ethernet et ses évolutions, en particulier la migration des environnements à contention vers des environnements commutés.

EXERCICES

Exercice 16.1 Adressage MAC, type d'adresse

1. Quel est le format de l'adresse MAC et la signification de chacun des quatre champs ?
2. Quels sont les types d'adresse MAC auxquels une station doit répondre ?
3. À quel type d'adresse correspond l'adresse MAC 01-00-5E-AB-CD-EF, cette adresse peut-elle être présente dans le champ Adresse source ?
4. Déduisez-en un type d'application possible.

Exercice 16.2 Notation canonique et non canonique

Écrivez l'adresse MAC de *broadcast* généralisé en notation canonique et non canonique.

Exercice 16.3 Comparaison des topologies et méthodes d'accès

Établissez un tableau comparatif (avantages, inconvénients) des différentes topologies et des différentes méthodes d'accès utilisées dans les réseaux locaux.

Exercice 16.4 Longueur virtuelle de l'anneau 802.5

Quelle est l'influence sur la longueur virtuelle de l'anneau à jeton (802.5) de l'insertion d'une nouvelle station si le coefficient de vélocité du câble utilisé est de 2/3 ?

Exercice 16.5 Efficacité du protocole 802.5 à 100 Mbit/s

Compte tenu des résultats de l'exercice précédent, les concepteurs imaginent utiliser le protocole 802.5. Quel sera alors le débit maximal d'information ?

Exercice 16.6 Détermination du temps d'accès

Un réseau 802.5 à 4 Mbit/s comporte 50 stations, la distance moyenne entre stations est de 50 m. La vitesse de propagation étant de 200 m/μs, on demande :

1. Quel est le temps maximum au bout duquel une station est assurée de disposer du jeton ?
2. Quel est, vu d'une station, le débit du réseau ?
3. Peut-on effectuer un calcul similaire pour les réseaux CSMA/CD ?

Exercice 16.7 Adresses auxquelles répond une station

Sur un même segment physique votre administrateur réseau a défini deux sous-réseaux :

SR1 : 10.75.0.0/16

© Dunod – La photocopie non autorisée est un délit

SR2 : 10.203.0.0/16

De même, deux services de diffusion vidéo sont supportés sur ce réseau (un par sous-réseau), les adresses d'abonnement à chacun de ces services sont respectivement :

Serveur 1 du SR1 : 224.75.161.12

Serveur 2 du SR1 : 224.203.161.12

On vous demande :

1. pour une des stations de chacun de ces sous-réseaux de compléter le tableau de la figure 16.50 ;
2. de commenter le résultat et d'en tirer les conséquences au point de vue des performances de ces deux stations.

Adresses	Type d'adresse	Sous-réseau 1	Sous-réseau 2
	Unicast	10.75.18.30	10.203.125.7
I	Groupe *Multicast*	224.75.161.12	224.203.161.12
P	Diffusion limitée		
	Diffusion dirigée		
M	*Unicast*	00-01-02-03-05	00-01-02-04-06
A	*Broadcast*		
C	*Multicast*		

Figure 16.50 Les différentes adresses d'une station.

Exercice 16.8 FDDI et Token Ring

Comparez les caractéristiques physiques et fonctionnelles des réseaux Token Ring et FDDI.

Exercice 16.9 Données de la classe Isochrone

Est-il envisageable d'émettre des données Isochrone sur un réseau FDDI-I ?

Exercice 16.10 Rotation des données sur le réseau FDDI

Supposons un réseau FDDI ne comportant que quatre stations. Représentez la circulation des données sur l'anneau en admettant que :

– avant l'échange seul le jeton circule sur l'anneau ;
– la station 1 acquiert le jeton et transmet des données à la station 3 ;
– la station 2 acquiert le jeton et transmet des données à la station 4.

On considérera que la trame est très petite devant la taille de l'anneau.

Chapitre **17**

Ethernet et ses évolutions sans fil

17.1 INTRODUCTION

Les protocoles à contention ont pour origine la méthode d'accès radio Aloha du réseau radio de l'université d'Hawaï (1970). Une station qui avait un message à transmettre l'émettait sans se préoccuper des autres stations. Si le message était pollué par une autre émission (collision), il était retransmis. Cette méthode, très simple à implémenter, est d'autant moins efficace que le nombre de stations augmente. La méthode dite **CSMA/CD** (*Carrier Sense Multiple Access*, *Collision Detection*) dérive de cette approche. D'abord baptisé Alto Aloha, l'Ethernet[1] (réseau dans l'Ether) a été développé chez Xerox par Robert Metcalfe dans les laboratoires d'Alto (**Alto Aloha Network**) en 1973. Cette première version sur câble coaxial offrait un débit de 3 Mbit/s. Associant Digital, Intel et Xerox (**DIX**), Bob Metcalfe fit évoluer sa version vers 10 Mbit/s (Ethernet DIX, 1980). Les spécifications définitives (Ethernet v2, 1982) ont été reprises par l'IEEE pour donner naissance aux spécifications IEEE 802.3 10Base5 (1985), puis par l'ISO (ISO 8802.3) en 1989. Aujourd'hui cette technique domine largement le marché, et fait un retour aux sources avec le développement de la norme 802.11 (réseaux sans fil).

17.2 LES CARACTÉRISTIQUES GÉNÉRALES DES RÉSEAUX ETHERNET/802.3

17.2.1 Le principe du CSMA/CD

Le principe de base du CSMA/CD repose sur la **diffusion** des messages à l'ensemble des stations du réseau (réseau à diffusion). Lorsqu'une station désire émettre, elle écoute le réseau, si aucun message n'est en cours de diffusion (aucune activité électrique sur le support) elle émet, sinon, elle diffère son émission jusqu'à ce que le support soit libre (attente active).

1. Ethernet est une marque déposée par Xerox. Ce nom, passé dans le langage commun, s'écrit toujours avec une majuscule.

Cette méthode ne peut garantir que deux stations décèleront le silence en même temps et qu'elles n'émettront pas en même temps leur message. Dans cette hypothèse, chaque message est pollué par l'autre (collision) et devient inexploitable. Il est alors inutile de poursuivre l'émission. Aussi, lorsqu'une station détecte une collision, elle cesse ses émissions.

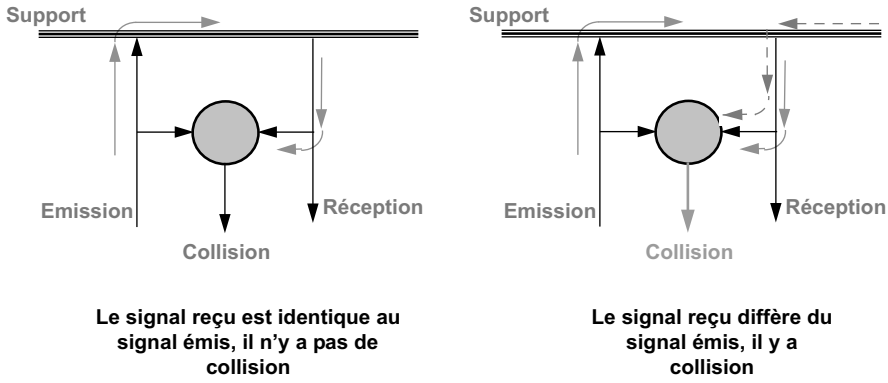


Figure 17.1 Principe de la détection de collision.

Pour détecter les collisions (figure 17.1), chaque station, durant l'émission de son message, écoute le support. Si elle décèle une perturbation, les niveaux électriques sur le support ne correspondent pas à ceux qu'elle génère, elle arrête son émission et arme un temporisateur. À l'échéance de ce dernier, la station écoute de nouveau le support, s'il est libre, elle retransmet le message tout en surveillant son émission (détection de collision). Afin d'éviter d'avoir à remonter l'information de trame perdue aux couches supérieures, c'est la couche MAC qui réalise la reprise sur détection de collision. La figure 17.2 illustre ce mécanisme.

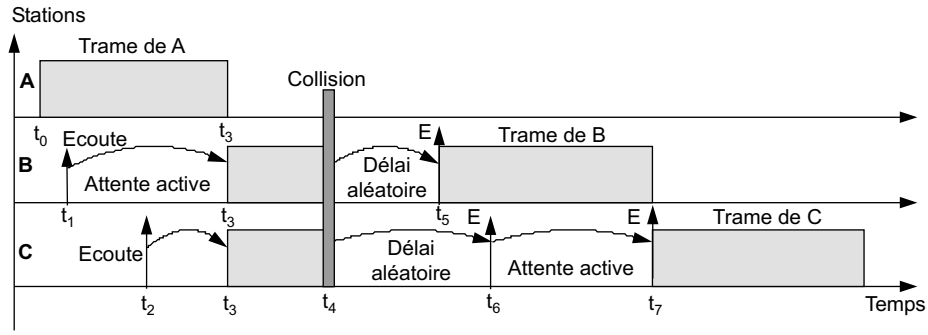


Figure 17.2 Principe du CSMA/CD.

La station *A* diffuse son message (t_0 à t_3). En t_1, La station *B*, avant d'émettre, se met à l'écoute. Le support est occupé, elle diffère son émission, mais reste à l'écoute (attente active). De même *C*, en t_2, se porte à l'écoute et retarde son émission. En t_3, *A* cesse d'émettre, *B* et *C* détectent le silence, ils émettent en même temps. En t_4, chacune des stations détecte que son message est altéré, la collision est détectée. *B* et *C* cessent leur émission et déclenchent une temporisation aléatoire (§ 17.2.3). En t_5, le *timer* de *B* arrive à échéance. Le canal étant libre, *B* émet. En t_6, *C* détecte le support occupé, il diffère son émission jusqu'au temps t_7.

17.2.2 La fenêtre de collision

La fenêtre de collision correspond au temps minimal pendant lequel une station doit émettre pour détecter la collision la plus tardive que son message est susceptible de subir. Considérons (figure 17.3) les deux stations les plus éloignées du réseau : *A* et *B*. En 1, *A* émet, tant que le message de *A* n'est pas parvenu à *B*, cette dernière suppose le support libre (2). *B* émet alors un message juste au moment où le premier bit du message de *A* lui parvient (3). La station *B* détecte instantanément la collision et cesse son émission (3). Pour que *A* puisse détecter que son message a subi une collision, il est nécessaire que le petit message de *B* lui parvienne et qu'il soit encore en émission à cet instant (4). Ce temps minimal d'émission s'appelle fenêtre de collision, *Time Slot* ou encore tranche canal. C'est aussi la période de vulnérabilité d'un message, c'est-à-dire l'intervalle de temps pendant lequel une collision peut se produire.

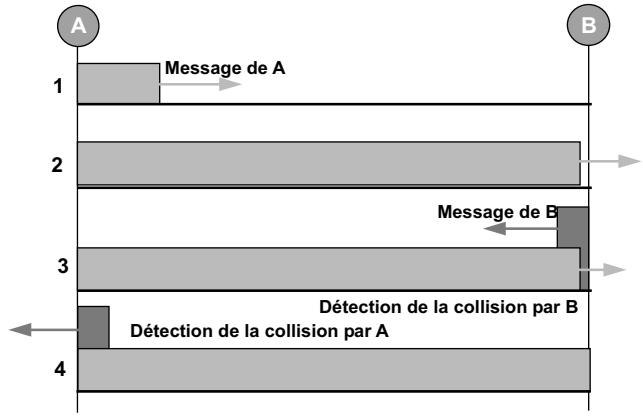


Figure 17.3 La fenêtre de collision.

Ce temps minimal d'émission correspond à deux fois le temps de propagation d'une trame sur la plus grande distance du réseau (2 500 m), traversée des répéteurs ou autres organes d'interconnexion des brins compris. Fixé à 51,2 μs, ce temps correspond, pour un débit de 10 Mbit/s, à l'émission de 512 bits, soit 64 octets. En cas de message de longueur inférieure, une séquence de bourrage (*Padding*) est insérée derrière les données utiles. Un pointeur de longueur des données utiles, sur deux octets, permet au récepteur d'extraire les données utiles de l'ensemble des données du champ information (données utiles + bourrage). La figure 17.4 illustre la structure générale de la trame 802.3.

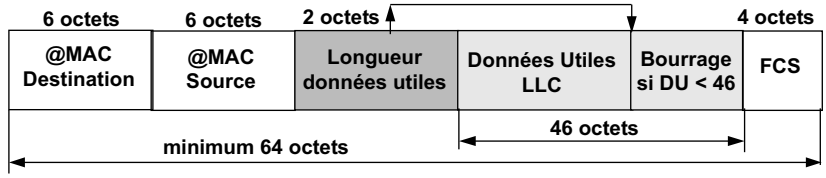


Figure 17.4 La structure générale d'une trame 802.3.

La signification du champ « Longueur des données utiles », diffère selon que la trame est au format Ethernet v2 ou au format IEEE 802.3, rendant ces deux types de réseaux CSMA/CD incom-

© Dunod – La photocopie non autorisée est un délit

patibles (§ 17.2.5). Dans la version Ethernet v2, ce champ identifie le protocole supérieur, c'est à ce dernier que revient la tâche d'extraire les données utiles du champ Données.

Dans l'exemple de la figure 17.3, la station ***B*** a cessé son émission immédiatement après avoir détecté la collision, son message est donc très court. Pour être certain que ***A*** détecte la collision, le message qui lui arrive doit avoir une taille minimale, aussi pour garantir la détection de collision par ***A***, ***B*** émet une séquence de brouillage de 32 bits à 1 (3,2 μs) appelée *jam interval*.

Les évolutions récentes d'Ethernet vers des débits plus élevés soulèvent le problème du maintien de cette fenêtre à 51,2 μs. Par exemple, à 100 Mbit/s, la trame minimale devient de 640 octets, c'est-à-dire que compte tenu des données de bourrage l'augmentation du débit, vu des applications, serait quasiment nulle pour les petits messages. Dans ces conditions, et pour assurer la compatibilité entre les différentes versions, la trame minimale de 64 octets a été maintenue. Si le débit croît, la fenêtre de collision décroît dans les mêmes proportions, et par conséquent la distance maximale entre deux stations (diamètre du réseau). La figure 17.5 illustre cette relation.

Débit	Fenêtre de collision	Diamètre du réseau
10 Mbit/s	51,2 μs	2 500 m
100 Mbit/s	5,12 μs	250 m
1 000 Mbit/s	0,512 μs	25 m

Figure 17.5 La relation débit et le diamètre du réseau.

17.2.3 L'algorithme du BEB

Le **BEB** (*Binary Exponentiel Backoff*) ou encore algorithme de ralentissement exponentiel, détermine le délai aléatoire d'attente avant qu'une station ne tente, après collision, une nouvelle émission (figure 17.6). Ainsi, après une collision, une station ne peut émettre qu'après un délai défini par :

$$T = K \cdot TimeSlot$$

K est un nombre aléatoire entier généré par l'émetteur et compris dans l'intervalle :

$$K = [0,\ 2^n - 1] \text{ avec } n \leqslant 10$$

où n représente le nombre de collisions successives détectées par la station pour l'émission d'un même message. Après seize tentatives, l'émetteur abandonne l'émission.

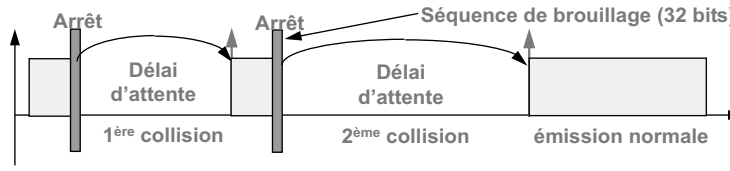


Figure 17.6 Principe du BEB.

Remarquons :

– que si deux stations entrent en collision, la probabilité pour qu'elles en subissent une seconde est de 0,5 (tirage de 0 ou 1) ;

– qu'il est, dans ces conditions, impossible de borner le temps d'attente avant l'émission d'un message. Le CSMA/CD est une méthode d'accès probabiliste et non déterministe. Ce protocole ne convient pas aux applications temps réel, ni aux transferts de flux isochrones (voix, vidéo).

17.2.4 Le silence inter-message (IFG, *InterFrame Gap*)

Une station avant d'émettre doit détecter une période de silence d'au moins 9,6 μs soit 96 bits (**IFG**, *InterFrame Gap*). Ce silence inter-message permet :

– d'une part, à l'électronique de bien discerner deux messages successifs,
– et, d'autre part, l'évanouissement d'éventuelles réflexions (écho), évitant ainsi de générer de fausses collisions (collision entre le message émis et l'écho du message précédent dite collision fantôme).

17.2.5 Le format des trames Ethernet/IEEE 802.3

La trame IEEE 802.3 est représentée en figure 17.7. Le codage est du type Manchester. Un préambule de 7 octets permet la synchronisation bit. La synchronisation caractère est assurée par le fanion de début de trame (**SFD,** *Start Frame Delimitor*), les deux bits à « 1 » marque le début de la trame. Les champs adresses (2 ou 6 octets) contiennent les adresses MAC destination et source. Un pointeur, sur 2 octets, indique la longueur utile du champ données. Le champ données est suivi d'un contrôle d'erreur de type CRC : le **FCS** (*Frame Check Sequence*) sur 4 octets.

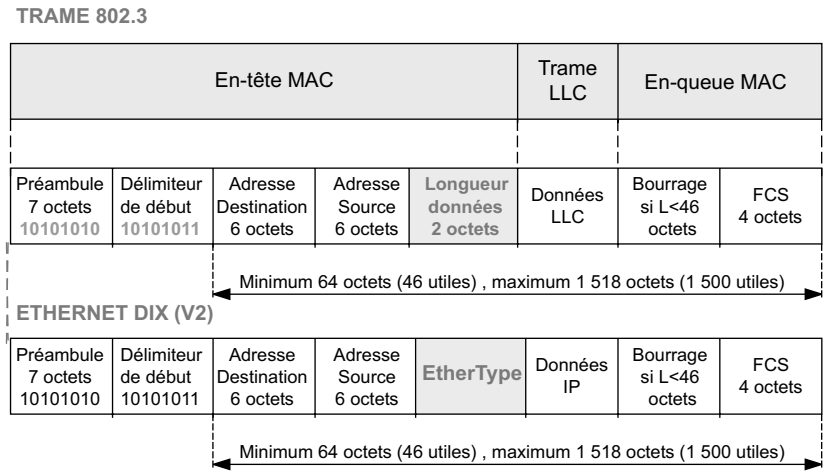


Figure 17.7 Le format de la trame Ethernet/IEEE 802.3.

La trame Ethernet DIX (Dec, Intel, Xerox) diffère de la trame IEEE 802.3, par le champ longueur de données. Celui-ci est remplacé par l'identifiant, sur deux octets, du protocole supérieur (Ethertype). C'est à ce dernier de gérer la longueur des données utiles. Par exemple, le protocole IP de TCP/IP est identifié par la valeur 2 048 (0x0800). Pour éviter toute ambiguïté, la longueur maximale utile d'une trame étant de 1 500 octets, les valeurs assignées à l'Ethertype sont toutes supérieures à 1 500. De ce fait, l'octet Type/Longueur permet de distinguer les deux versions.

© Dunod – La photocopie non autorisée est un délit

17.2.6 Les erreurs

Les collisions sont, sur un réseau CSMA/CD, la principale cause d'erreur. Lorsque le réseau est chargé, elles se multiplient provocant ainsi une réduction apparente du débit, cette réduction allant jusqu'à l'effondrement du réseau (figure 17.8).

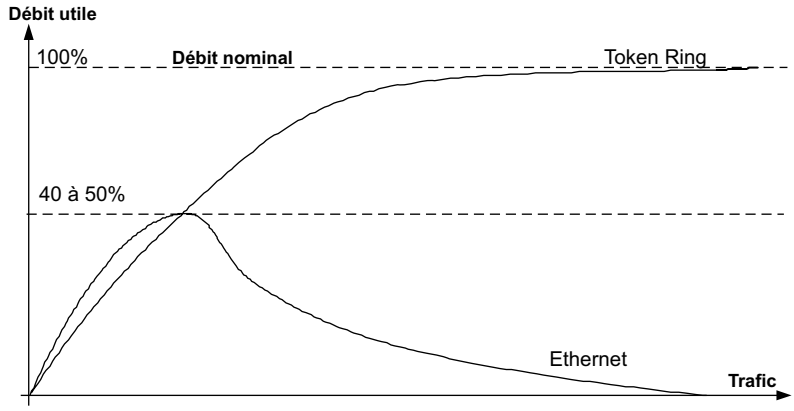


Figure 17.8 Courbe de comparaison Ethernet/Token Ring.

La figure 17.8 montre l'évolution des débits apparents, celui vu par les applications, en fonction de la charge des réseaux de type accès à contention (Ethernet, accès CSMA/CD) et à réservation (Token Ring, accès à jeton). Il est intéressant de constater qu'à faible charge, les réseaux de type Ethernet présentent, vis-à-vis des couches supérieures, une meilleure efficacité. En effet, dans un réseau Ethernet, si le trafic est faible, dès qu'une station veut émettre, elle émet. En Token Ring, même à faible charge, la station doit attendre le jeton.

Cependant, à forte charge dans le réseau Ethernet, les collisions se multiplient et le débit utile sur le support s'effondre, alors que dans le cas du réseau Token Ring, même si le débit effectif de chaque station diminue, le débit utile sur le support tend vers le débit nominal.

Les collisions se caractérisent par des trames de moins de 64 octets (*Runt*) et généralement non alignées sur un nombre d'octets (*Misaligned*). L'adaptateur peut présenter des dysfonctionnements et émettre des trames trop longues appelées *Jabert*.

Enfin, les erreurs de FCS proviennent d'un événement extérieur (parasites), d'un câblage défectueux ou encore de collisions tardives. Les collisions tardives (*Late collision*) peuvent se produire dans un réseau dont la longueur est supérieure à la norme, c'est-à-dire dont le temps de transit est supérieur au *Time Slot*.

17.3 LES DIFFÉRENTES VERSIONS D'ETHERNET

17.3.1 Présentation

Les réseaux de type Ethernet sont certainement ceux qui se sont le mieux adapté à l'évolution des besoins. D'abord en terme de débit en passant de 3 Mbit/s pour la première version expérimentale à 40 Gbit/s, ensuite en migrant d'un environnement à contention vers un environnement commuté. Initialement destiné aux applications en mode texte, Ethernet aujourd'hui supporte tout type de transfert : voix, données, vidéo. La figure 17.9 présente une synthèse de ces évolutions.

Année	Nom	Description succincte
1976	Alto Aloha Network	Réseau expérimental à 2,94 Mbit/s.
1980	Ethernet DIX	Pré-version de l'Ethernet sur coaxial épais à 10 Mbit/s.
1982	Ethernet v2	Version de base des réseaux Ethernet, repris par L'IEEE sous le nom de IEEE 802.3 10Base5 en 1985, puis en 1989 par l'ISO (ISO 8802.3).
1988	IEEE 802.3a ou 10Base2	Extension de la norme sur coaxial fin.
	IEEE 802.b ou 10BROAD36	Version en large bande.
	IEEE 802.c	Définition des répéteurs pour prolonger le réseau.
	IEEE 802.e ou 1Base5	Reprise des spécifications du Starlan, version d'Ethernet sur paires torsadées.
1989	IEEE 802.d Ethernet FOIRL	Ethernet 10 Mbit/s sur fibre optique.
1990	IEEE 802.3i 10BaseT	Extension du réseau Starlan à 10 Mbit/s.
	IEEE 802.3h	Définition de l'administration (*Layer Management*).
1993	IEEE 802.3j 10BaseF	Redéfinition de FOIRL, apport d'une configuration en étoile avec répéteurs multiports.
1995	IEEE 802.3u Fast Ethernet	Définition des versions à 100 Mbit/s : 100BaseTx, 100BaseT4, 100BaseFx.
1998	IEEE 802.3x	Introduction du fonctionnement en *full duplex* et du contrôle de flux.
	IEEE 802.3z GigabitEthernet	Définition d'une version à 1 Gbit/s sur fibre optique (1000 BaseLX, BaseSX) et paires torsadées blindées (1000 BaseCX).
	IEEE 802.3ab 1000BaseT	Définition d'une version à 1 000 Mbit/s sur les infrastructures existantes (câble catégorie 5).
2002	IEEE 802.3ae	Version à 10 Gbit/s.
200x		Version à 40 Gbit/s.

Figure 17.9 La synthèse des évolutions des réseaux Ethernet.

17.3.2 L'Ethernet épais, IEEE 802.3 10Base5

Les appellations IEEE désignent d'abord le sous-comité (802.3), le type de modulation (bande de base ou large bande : *Broad band*) et le diamètre du réseau ou le type de support. La version 10Base5, (10 Mbit/s en bande de base sur câble coaxial d'une longueur maximale par segment de 500 m) utilise un codage Manchester. La figure 17.10 illustre cette version d'origine de l'Ethernet.

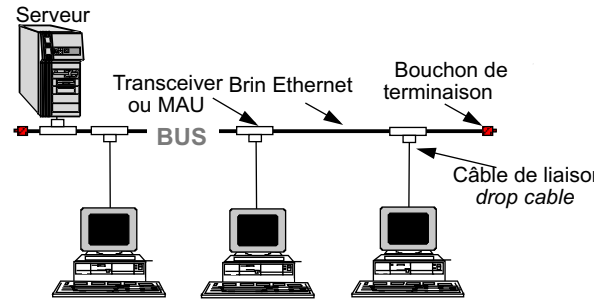


Figure 17.10 Le réseau Ethernet jaune.

© Dunod – La photocopie non autorisée est un délit

Chaque station est équipée d'une interface « Ethernet » (**NIC**, *Network Interface Card*) généralement appelée carte transporteur ou carte « Ethernet ». Cet équipement assure l'adaptation physique (niveaux électriques, encodage...) et gère l'algorithme CSMA/CD. Dans la version 10Base5, un connecteur DB15 (Cannon 15 broches) permet le raccordement du câble de liaison (*Drop cable*) au *transceiver* ou **MAU** (*Medium Attachment Unit* – unité d'attachement au support). Le MAU contient l'électronique d'émission et de réception, il assure la détection des collisions qu'il signale à la station (figure 17.1). Le *transceiver* se raccorde au coaxial par un système dit de prise vampire, le raccordement d'une nouvelle station peut être ainsi réalisé sans interrompre le trafic.

Le *drop cable,* d'une longueur maximale de 50 m*,* est constitué de paires torsadées (5 paires). Le câble coaxial est un câble épais de couleur jaune (Ethernet jaune) dont les principales caractéristiques sont : diamètre un demi-pouce, impédance 50 Ω, coefficient de vélocité 0,77. Un *transceiver* peut être connecté tous les 2,5 m avec un maximum de 100 stations actives par segment de 500 m. La longueur totale du réseau peut atteindre 2,5 km (5 segments). Il est recommandé de n'utiliser que des segments dont la longueur est un multiple impair de 23,4 m (longueur d'onde sur ce type de câble du signal à 10 MHz).

Cette version d'Ethernet n'est plus que très rarement utilisée. On la trouve encore les environnements compromis (rayonnement électromagnétique) ou lorsque l'on veut garantir la confidentialité des échanges (pas de rayonnement du câble coaxial), elle reste moins onéreuse qu'une solution sur fibre optique. Le câblage en bus étant moins volumineux qu'un câblage étoile, cette version trouve encore son utilité à chaque fois que des problèmes d'encombrement se posent.

17.3.3 L'Ethernet fin, IEEE 802.3 10Base2

Compte tenu des difficultés de câblage de la version 10Base5, une version économique a été définie sur du câble coaxial fin (*Thin Ethernet*). Dans cette version, les fonctions du transceiver sont remplies par la carte transporteur (MAU intégré à la carte). De ce fait, le bus coaxial est connecté directement sur la carte par l'intermédiaire d'un T vissé BNC (*Barrel Neck Connector*). La longueur maximale d'un segment est de 185 m et chaque segment peut accueillir un maximum de 30 stations. La figure 17.11 présente cette version du réseau Ethernet.

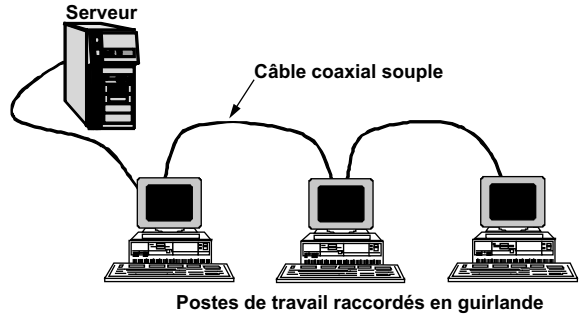


Figure 17.11 L'Ethernet fin.

Cette architecture physique de réseau a été très utilisée pour réaliser de petits réseaux d'une dizaine de machines.

17.3.4 L'Ethernet sur paires torsadées, IEEE 802.3 10BaseT

Origine

Compte tenu des difficultés du câblage coaxial, AT&T a imaginé de réutiliser le câblage téléphonique préexistant dans les immeubles de bureaux pour la réalisation de réseau. Le réseau devait alors passer d'une topologie physique et logique en bus à une topologie physique étoile, assurer la diffusion des messages (topologie logique en bus) et la détection des collisions. La solution adoptée par AT&T consiste simplement à émuler un bus dans un boîtier : le **hub**. Le hub est chargé d'une part de concentrer les connexions et d'autre part d'assurer la diffusion des messages (figure 17.12).

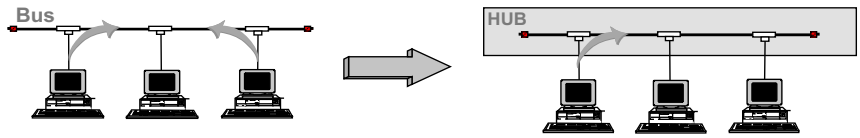


Figure 17.12 Le passage du bus à l'étoile.

La liaison hub/station est réalisée en paires torsadées (1 paire émission, 1 paire réception), ce qui impose deux contraintes : l'une de débit, l'autre de distance. Ce réseau fonctionne à 1 Mbit/s, les stations sont connectées sur des concentrateurs répéteurs (**hub**) et la distance entre le hub et une station est limitée à 250 m. Pour augmenter les capacités d'accueil et/ou de distance, les hubs peuvent être chaînés entre eux, cette cascade de hubs est illustrée par la figure 17.14 pour les réseaux Ethernet 10BaseT. Cette architecture (802.3 1Base5 ou Starlan), complètement obsolète, est à l'origine de la version à 10 Mbit/s (802.3 10BaseT, T pour *Twised pair*) qui en reprend les principes. La figure 17.13 illustre la réalisation des premiers câblages Ethernet sur paires téléphoniques. Ce mode de câblage utilisait un double brassage, un premier entre le hub et la ferme ressource téléphonique et un second entre la ferme ressource et la ferme distribution. Les premiers câblages dédiés réseau données sur paires torsadées ont repris ce double brassage, inutilisé aujourd'hui.

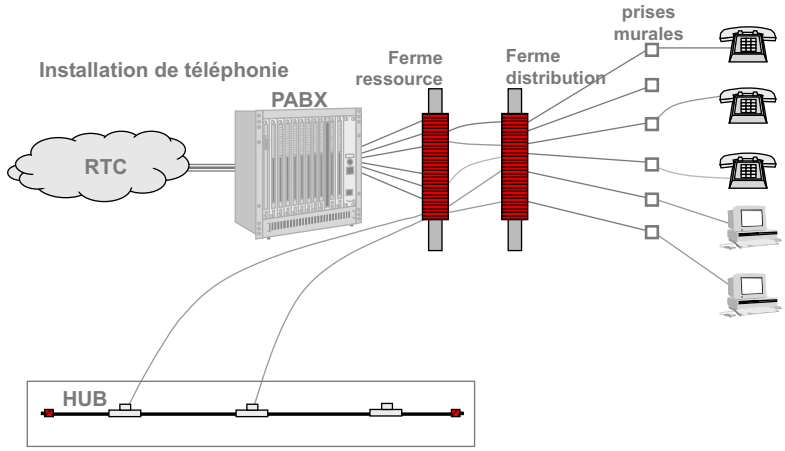


Figure 17.13 Principe des premiers câblages sur paires torsadées.

© Dunod – La photocopie non autorisée est un délit

L'Ethernet, 802.3 10BaseT

La version 10BaseT reprend les principes architecturaux du réseau Starlan, c'est un réseau en étoiles hiérarchisées (figure 17.14). Les hubs assurent :

– les fonctions de diffusion des messages (émulation de bus, deux stations connectées au même hub ne reçoivent le signal de l'autre que *via* le hub de tête) ;
– la détection des collisions (le hub diffuse un signal de collision vers les autres stations) ;
– la détection de stations bavardes (fonction *Jabber* : message d'une durée supérieure à 150 ms).

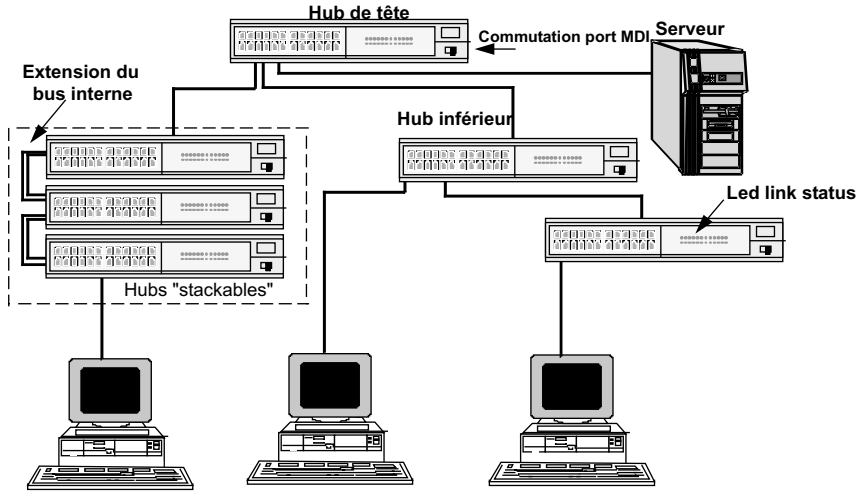


Figure 17.14 L'architecture du réseau 10BaseT.

En cas de collisions multiples (30), le hub segmente le réseau. Le débit est de 10 Mbit/s, la longueur d'un brin est limitée à 100 m (distance entre le hub et la station). Si l'atténuation est inférieure à 11,5 dB, cette longueur peut être portée à 150 m. Le nombre maximal de niveaux est fixé à trois.

C'est la fenêtre de collision qui limite le nombre de niveaux admissibles (distance et temps de traitement). Pour franchir la barrière des trois niveaux et autoriser un plus grand nombre de stations connectées, les hubs peuvent aussi être empilés par l'extension du bus interne (figure 17.14). Ces hubs, dits « *stackables* », sont vus par le système comme un seul niveau.

Un signal particulier, le *link status* (état de la ligne), permet, par la visualisation de diodes **LED** (*Light Emitting Diode*), de contrôler la continuité du lien entre le hub et la station (*Link integrity test function*). En l'absence d'émission, le hub et la carte réseau émettent, toutes les 16 ± 8 ms, une impulsion de test (**TP_IDL**, *Twisted Pair Idle Signal*), pour contrôler l'intégrité du lien (**LTP**, *Link Test Pulses*). En l'absence de données (données utilisateur ou signal LTP) le hub et la carte considèrent le lien défectueux, le voyant *link status* est alors positionné à « OFF » et le port du hub est inhibé.

Sur chaque hub, un interrupteur permet la commutation de la fonction d'un des ports (**MDI**, *Medium Dependent Interface*) en port de répétition vers un hub de niveau supérieur. Cette fonctionnalité autorise l'utilisation de câbles droits pour assurer les liaisons hub/hub et ainsi permettre de n'avoir qu'un seul type de jarretière de brassage en service. La figure 17.15 représente les différents cas de connexion d'un port 10BaseT.

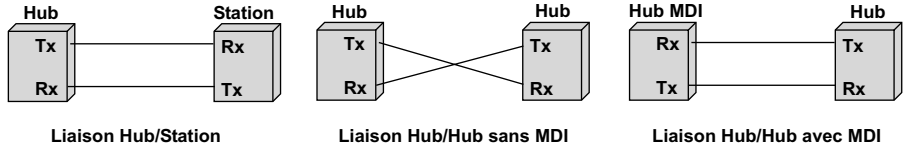


Figure 17.15 Raccordements hub/station et hub/hub.

17.3.5 L'Ethernet à 100 Mbit/s

Généralités

L'Ethernet 100 Mbit/s sur paires torsadées, ou ***Fast Ethernet***, est l'évolution naturelle de la version 10BaseT. La compatibilité avec la version 10BaseT est assurée par la reprise du protocole CSMA/CD et le maintien des tailles de trames (64 octets au minimum et 1 518 au maximum). De ce fait, la fenêtre de collision ou tranche canal est réduite à 5,12 μs (512 bits) et le silence entre deux trames successives (**IFG**, *Inter Frame Gap*) ne vaut plus que 0,96 μs (96 bits). La réduction de la fenêtre de collision par un facteur de 10 (de 51,2 μs à 5,12 μs) induit de fortes contraintes sur le temps de propagation du signal et, par conséquent, sur la distance maximale entre les deux stations les plus éloignées du réseau. La commutation étudiée au chapitre 18 permet de s'affranchir partiellement des limitations de distance.

La mixité et l'auto-négociation

Pour permettre l'évolution des réseaux en douceur, les concepteurs ont imaginé des hubs dont chacun des ports pouvait indifféremment fonctionner à 10 ou à 100 Mbit/. Afin de faciliter les tâches d'administration, selon les équipements en vis-à-vis, les ports s'auto-configurent à 10 ou 100 Mbit/s. À cet effet, les équipements 100 Mbit/s remplacent le signal de *link status* du 10BaseT par un mot de 16 bits (*Link Code Word*, voir § 17.3.6) décrivant les caractéristiques de l'équipement. Les cartes réseaux 100 Mbit/s sont dotés des mêmes fonctionnalités. Le port et la carte s'auto-configurent sur le plus grand dénominateur commun. Ainsi à un hub 100 Mbit/s, il est possible de connecter des équipements 10 ou 100 Mbit/s, de même une carte 100 Mbit/s peut être raccordée à un hub 10 Mbit/s, ces cartes ou ces hubs sont dits 10/100 Mbit/s. Dans la pratique, l'auto-négociation peut conduire à un fonctionnement perturbé du réseau. Le dialogue est mal compris, ce qui occasionne un fonctionnement à 10 Mbits, alors que les deux composants sont à 100 Mbit/s ou un basculement incessant de 10 à 100 Mbit/s, il est souvent préférable de verrouiller l'équipement terminal sur 10 ou 100 Mbit/s selon les équipements utilisés.

Deux types de hubs ont été définis (figure 17.16). Les hubs de classe 1, pratiquement les seuls utilisés permettent l'auto-négociation et donc la mixité des équipements. Ces hubs recevant un signal à 100 Mbit/s doivent être capables de le retransmettre à des équipements à 10 Mbit/s ; cette fonctionnalité impose une mémorisation de la trame reçue (éventuelle différence de débit des ports entrée et sortie) et un transcodage physique de la trame 4B/5B en entrée pour le 100BaseTX et

© Dunod – La photocopie non autorisée est un délit

Manchester en sortie pour le 10BaseT par exemple (figure 17.17). Les hubs de classe 2 destinés à relier des segments de même type n'implémentent aucune fonction d'auto-configuration. Plus rapide, car ils n'ont aucune fonction de modification de codage à réaliser, ils autorisent un niveau de cascade. Cependant ce lien inter-hub ne doit pas dépasser 5 m (**IRL**, *Inter Repeater Link*). Ce nombre de niveaux est sans grande influence sur les distances mais autorise plus de stations.

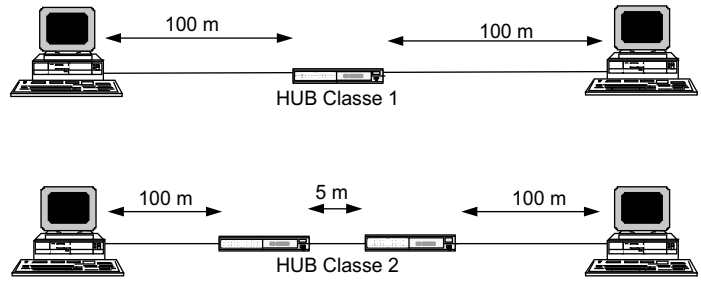


Figure 17.16 La topologie des réseaux 802.3 100BaseT.

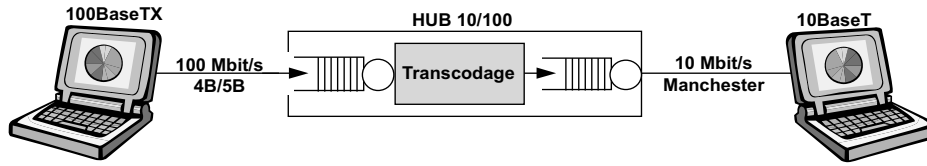


Figure 17.17 Hub autosense passage de 100 Mbit/s à 10 Mbit/s.

Les différentes implémentations

La norme 100BaseT prévoit trois supports différents (figure 17.18). Le 100BaseT4, utilise les quatre paires torsadées des câbles de catégorie 3, 4 et 5. Trois paires sont utilisées pour la transmission de données, le quatrième pour gérer la détection de collisions. Les données sont codées 8B/6T (8 bits sur trois temps d'horloge), ce qui ramène la fréquence d'horloge à 25 MHz (12,5 MHz sur le support). Cette version est restée très confidentielle, une version 100BaseT2 a aussi été définie.

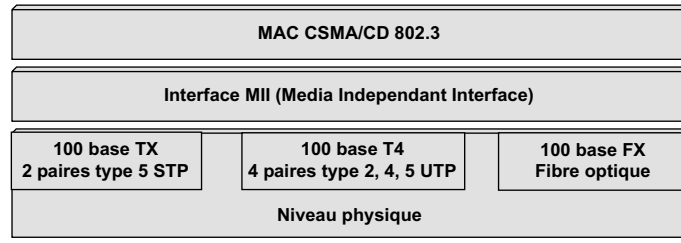


Figure 17.18 L'architecture générale de Fast Ethernet.

La version 100BaseTX utilise le même câble et les mêmes paires que le 10BaseT (UTP/FTP catégorie 5). Le codage Manchester est abandonné au profit du codage 4B/5B (16 symboles parmi 32) ce qui limite la signalisation à 125 bauds sur le support contre 200 si le codage Manchester avait été conservé. Une version sur fibre optique (100BaseFX), identique au niveau physique à FDDI, porte la dimension du réseau à 412 m.

17.3.6 Le Gigabit Ethernet

Généralités

En portant le débit à 1 Gbit/s, la version d'Ethernet dite Gigabit Ethernet (**GbE**) introduit selon le type de concentrateur (hub) utilisé et, en environnement partagé, deux modes de fonctionnement : le mode dit unidirectionnel ou *half duplex* et le mode bidirectionnel ou *full duplex*. Dans les deux cas une seule station peut être raccordée à un port. Cependant le GbE s'est essentiellement développé en mode commuté (voir chapitre 8). L'architecture générale du Gigabit est représentée figure 17.19.

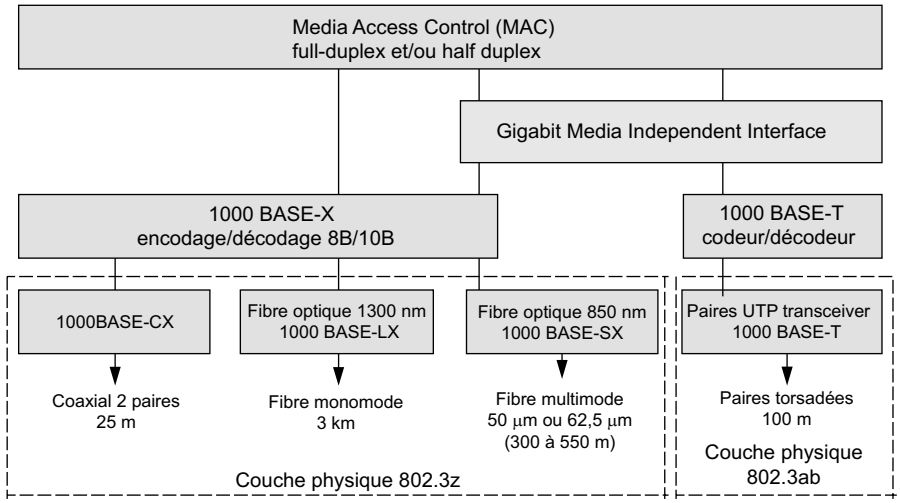


Figure 17.19 L'architecture du Gigabit Ethernet.

Le Gigabit Ethernet en mode partagé

En mode partagé *half duplex,* une taille minimale de trame de 512 bits non seulement réduit de façon drastique le diamètre du réseau, mais n'assure pas un délai suffisant pour garantir la détection de collision (512 nanoseconde). Pour cela deux techniques ont été introduites.

La première dite *carrier extention* a pour principal objectif de garantir la compatibilité avec les versions antérieures en particulier, elle maintient une trame minimale de 512 bits, aussi, pour permettre la détection de collision, la station émettrice poursuit son émission après le FCS de la trame en réalisant un « post-bourrage » par l'émission de symboles dit symboles d'extension (figure 17.20).

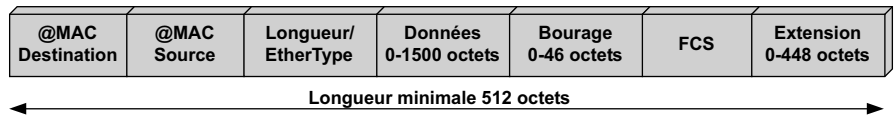


Figure 17.20 L'extension de porteuse.

Ainsi, si le concentrateur doit retransmettre la trame sur un port 10 ou 100 Mbit, il pourra cesser sa retransmission dès l'émission de FCS. En réception, un récepteur Gigabit doit, lui, même si la trame comporte des symboles d'extension, attendre la réception correcte des 512 premiers octets

© Dunod – La photocopie non autorisée est un délit

de la trame avant de la transmettre aux couches supérieures (période de vulnérabilité ou collision de la trame). Cette technique autorise un réseau de 200 m de diamètre (100 m entre station et hub).

Une taille minimale de trame de 512 octets conduit, lors du transfert de petits volumes d'information, à un bourrage important (*carrier extension*), et donc à un gaspillage de la bande passante. Pour y remédier, le Gigabit implémente une fonction de groupage de trames (*Frame bursting*). L'émission de rafales de trame est limitée par un paramètre configurable par l'administrateur (*Burst time*), donc la valeur maximale autorise l'émission de 8 ko (figure 17.21). Les silences inter-trames (IFG) sont remplis par des symboles d'extension.

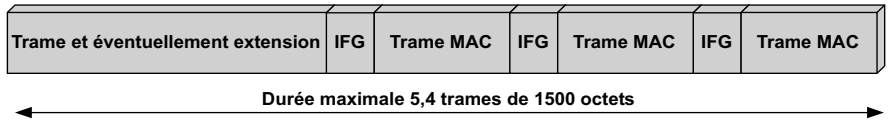


Figure 17.21 Principe du groupage de trames.

En mode *full duplex*, la station n'intervient pas dans la gestion des collisions, celle-ci est intégralement assurée par le hub. Dans ces conditions, la taille de la trame minimale peut rester à 512 bits (64 octets) et l'IFG (*Inter Frame Gap* ou silence inter-trames) à 96 bits. En mode partagé traditionnel, la détection de collision fait office de contrôle de flux, aussi, pour éviter la perte de trames par débordement des « *buffers* » du hub, notamment lors de la répétition de trames sur des ports de sortie dont le débit est inférieur à celui des ports d'entrée, il est nécessaire d'introduire un mécanisme de contrôle de flux entre la station et le hub. Ce mécanisme, du type XON/XOFF est aussi mis en œuvre dans les réseaux commutés (10-100-1000). Une trame **MAC Control** a été introduite (Ethertype = 0x8808) dont un sous-ensemble définit une trame dite trame « **Pause** » (code 0x0001). La trame Pause demande à la station source de suspendre ses émissions pendant un certain temps décompté en *Time Slot*. Une trame « *Pause* » avec un délai nul constitue une annulation de la trame précédente (reprise des émissions). La figure 17.22 fournit le format de la trame « *Pause* ».

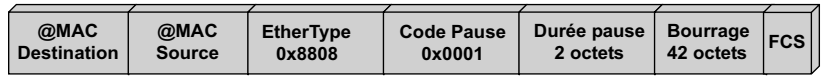


Figure 17.22 Le format de la trame Pause.

Le Gigabit Ethernet sur paires torsadées (IEEE 802.3 1000BaseT)

En *full duplex*, le Gigabit Ethernet utilise les quatre paires (figure 17.23), le débit n'est que de 250 Mbit/s sur chaque paire, ce mode de fonctionnement autorise la réutilisation des câblages 5e, mais conduit à la réalisation d'interfaces coûteuses.

En effet, le pas de torsades, différent d'une paire à l'autre, induit des délais de propagation inégaux (*Delay skew*) qu'il convient de corriger. La mise en œuvre d'une transmission *full duplex* est réalisée par la technique d'annulation d'écho et un circuit hybride permet le passage de 2 à 4 fils (figure 17.24). Le codage utilisé est du type PAM 5 (*Pulse Amplitude Modulation* à cinq niveaux –2, –1, 0, +1, +2) qui codent 2 bits de donnée et 1 bit de correction d'erreur en un temps d'horloge. La réalisation d'interface sur catégorie 6 est simplifiée, la transmission est unidirectionnelle, seul le *delay skew* est à corriger.

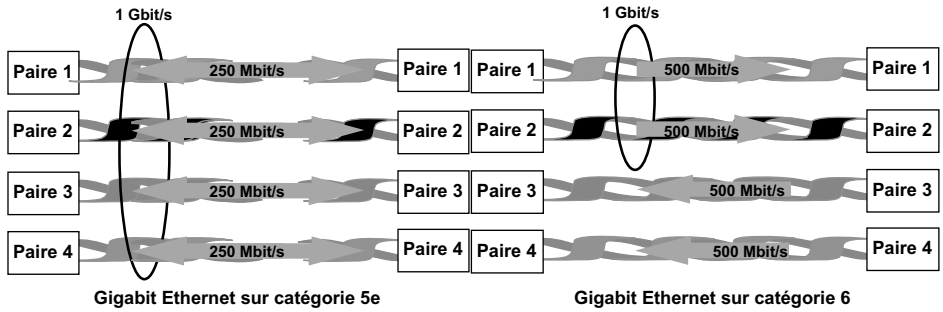


Figure 17.23 Gigabit Ethernet sur paires torsadées de catégorie 5 ou 6.

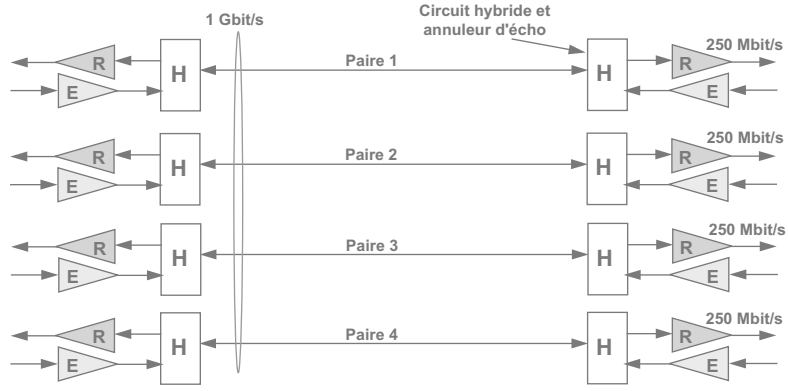


Figure 17.24 Principe d'une interface Gigabit sur catégorie 5e.

L'auto-négociation

Les équipements Gigabit Ethernet combinent généralement des ports 10, 100 et une ou plusieurs connexions à 1 Gbit/s. La figure 17.25 propose un exemple d'application du Gigabit Ethernet en tant que réseau fédérateur de réseaux à 100 ou 10 Mbit/s.

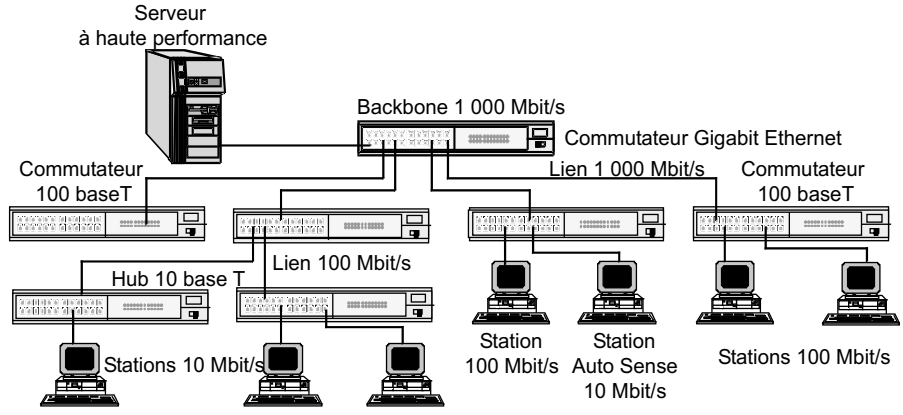


Figure 17.25 Exemple d'utilisation du Gigabit Ethernet.

© Dunod – La photocopie non autorisée est un délit

Le commutateur est utilisé en tant que *backbone* (*LAN in a box* ou *Collapsed backbone*). Le *backbone* est reporté sur le fond de panier du commutateur, qui remplit alors le rôle de multiplexage des connexions LAN.

Dans une telle configuration, il est important que chaque interface puisse déterminer quelle est la capacité de son vis-à-vis. À cet effet, la séquence d'impulsions (**NLP**, *Normal Link Pulse*) du « *link status* » du 10 base-T a été remplacée par une salve d'impulsions appelée **FLP** (*Fast Link Pulse*) annonçant les capacités de l'interface (figure 17.26). Introduit avec la version 802.3u d'Ethernet 100 Mbit/s, l'auto-négociation est, en principe, exécutée à chaque initialisation d'une voie. La négociation est unilatérale, chaque système acquitte le message de son vis-à-vis et annonce ses propres capacités, en principe c'est le niveau commun le plus élevé qui est retenu.

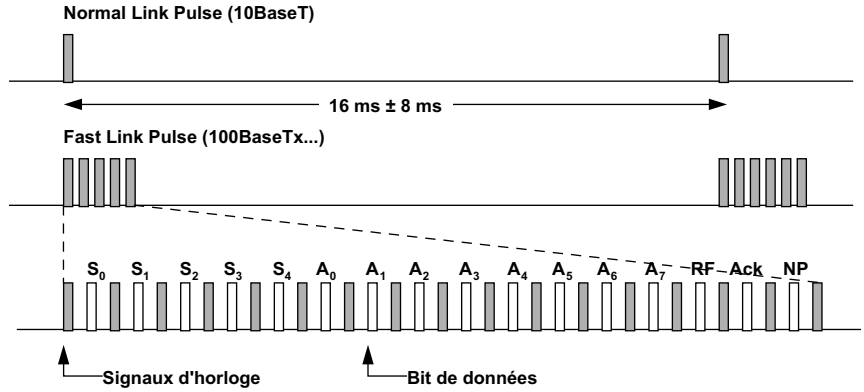


Figure 17.26 La structure du mot de 16 bits dit « Fast Link Pulse ».

Le FLP est composé d'une rafale de 33 impulsions dont 16 seulement sont significatives, il est émis à la même fréquence que le test de lien et donc interprété par une interface non compatible « *auto-sense* » comme un signal de *link status*. La figure 17.27 fournit la signification du mot de 16 bits dit **LCW** (*Link Code Word*) transporté par le signal FLP.

Mot	Bits	Signification	Valeur	Signification
Selector	S_0 à S_4	Type de carte	00010	803.3
Technology Ability	A_0 à A_7	Modes de fonctionnement disponibles (bit à 1)	A_0 A_1 A_2 A_3 A_4 A_5 A_6 A_7	10Base T– *Half duplex* 10Base T – *Full duplex* 100BaseTx – *Half duplex* 100BaseTx – *Full duplex* 100BaseT4 Pause 1000BaseT– *Half duplex* 1000BaseT– *Full duplex*
Autre	RF	Remote Fault	1	Erreur détectée
	ACK	Acknowledge	1	ACK de réception du mot LCW
	NP	Next Page	1	Mot à suivre

Figure 17.27 Codage des 16 bits du **LCW**.

En l'absence de signaux de négociation, il y a une possibilité d'auto-configuration par détection du type de codage des signaux reçus (100BaseTx et 100BaseT4). Ce mode de détection dit

« détection parallèle », est souvent à l'origine de quelques problèmes de dysfonctionnement des réseaux 100 Mbit/s.

17.3.7 Le 10 Gigabit Ethernet

Avec la publication IEEE 802.3ae, Ethernet multiplie encore le débit par 10. Le standard Ethernet 10 Gigabit (10 GE) est essentiellement destiné à une exploitation dans les dorsales de réseaux. Le Gigabit Ethernet et le 10 Gigabit sortent du LAN pour offrir des solutions d'encapsulation de niveau 2 aussi bien dans les MAN, les WAN et même sur la boucle locale (*Ethernet First Mile* ou IEEE 802.3ah).

Le 10 GE conserve la compatibilité avec les versions précédentes : définition du format de trame, taille minimale et maximale, contrôle de flux. Définit uniquement en mode *full duplex*, le 10 GE offre des interfaces LAN, MAN et WAN sur une distance de 40 km. En s'interfaçant avec des interfaces Sonet/SDH, le 10GE est susceptible de réaliser des liaisons de plusieurs milliers de kilomètres. Le nouveau standard Ethernet 10 Gigabit définit sept types de support différents en fonction des distances et réseaux cibles. La figure 17.28 illustre ces différentes architectures.

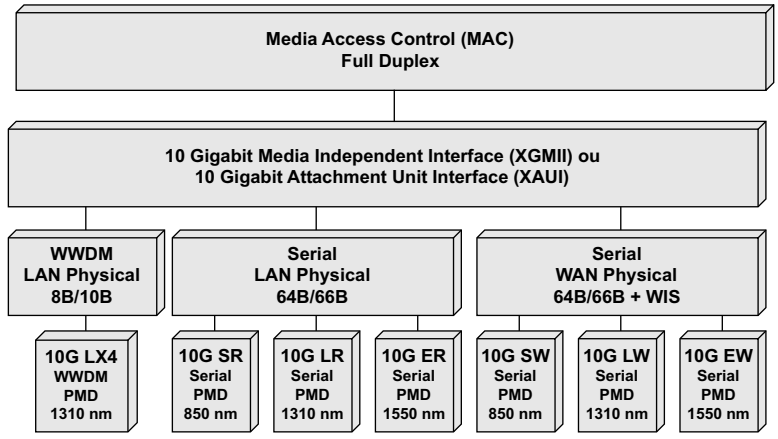


Figure 17.28 L'architecture générale du 10 GE

Les appellations 10G type S, L E se rapportent à la portée du système : S (*Short*), L (*Long*) et E (*Extralong*). Le 10GBASE-LX4, s'appuie sur une interface optique de multiplexage par division de longueur d'onde (**WWDM**, *Wide Wavelength Division Multiplexing*) et supporte une distance comprise entre 240 et 300 mètres sur fibre multimode. En utilisant une fibre nonomode, la distance peut être portée à 10 km.

Le 10GBASE-SR sur fibre multimode ne supporte que des distances allant de 26 à 82 mètres, selon le type de câble. Cette distance peut être portée à 300 m sur les nouvelles fibres multimodes à 2 000 MHz.

Le 10GBASE-LR et 10GBASE-ER, sur fibre monomode, portent les distances respectivement à 10 et 40 km.

10GBASE-SW, 10GBASE-LW et 10GBASE-EW destinés aux réseaux WAN sur interface SONET/SDH OC-192/STM-64 correspondent, respectivement, au niveau physique du 10GBASE-SR, 10GBASE-LR et 10GBASE-ER. Ils utilisent le même type de fibre et supportent les mêmes

© Dunod – La photocopie non autorisée est un délit

distances. L'interface **WIS** (*WAN Interface Sublayer*) réalise une adaptation du flux Ethernet aux *conteners* SONET/SDH. Cette interface n'autorise pas l'adaptation des débits et interdit donc l'injection d'affluents de débit plus faible.

Une version sur paires torsadées en cours de définition devrait autoriser des distances de 100 m sur câble UTP catégorie 6e. À l'instar du Gigabit sur catégorie 5, il utilise la technique *full duplex* avec annulation d'écho (utilisation des 4 paires). Le codage est du type **PAM 10** (*Pulse Amplitude Modulation* à 10 niveaux qui codent 3 bits) ce qui réduit la signalisation à 833 mégabauds sur chaque paire (4 paires × 833 MBaud × 3 bits/baud = 10 GB).

17.3.8 Le devenir d'Ethernet

Le succès d'Ethernet réside essentiellement dans son adaptabilité aux besoins. Les différentes versions ont su offrir aux utilisateurs les débits requis par les nouvelles applications. Les VLAN (*Virtual LAN*, voir chapitre 18) ont offert un service de sécurité que les versions 1GE et 10GE ont su prolonger à l'extérieur du LAN. Avec un débit maximal de 10 Gbit aujourd'hui et 40 voire 160 demain, Ethernet semble être la solution de transport de niveau 2 offrant ainsi un service de bout en bout sans rupture de technologie (figure 17.29). Associés à MPLS les réseaux de demain seront vraisemblablement Ethernet de bout en bout.

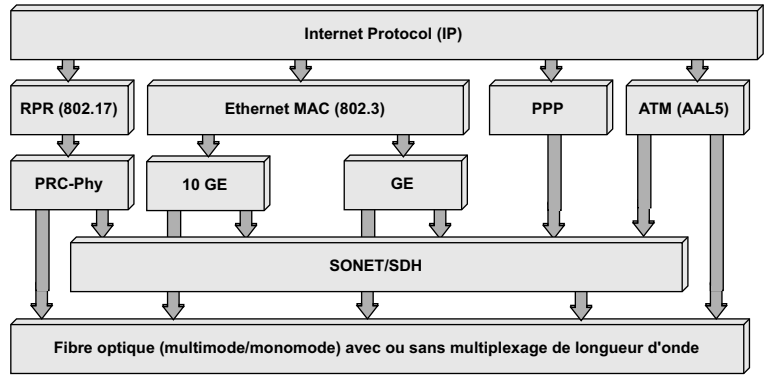


Figure 17.29 Les différentes solutions de tramage de niveau 2.

17.4 L'ETHERNET SANS FIL

17.4.1 Généralités

S'affranchissant d'une infrastructure câblée et autorisant la mobilité, les réseaux sans fil, sous des appellations génériques différentes, sont en plein essor. On distingue :

– les **WPAN** (*Wireless Personal Network*), de la simple liaison infrarouge à 100 kbit/s au Bluetooth à environ 1 Mbit/s, ces technologies peu coûteuses se développent rapidement. Elles sont essentiellement utilisées pour raccorder un périphérique informatique (imprimante...), un agenda électronique...

– les **WLAN** (*Wireless Local Area Network*), prolongent ou remplacent un réseau local traditionnel. Ces réseaux, objet de ce paragraphe, connaissent un développement important. Ils autorisent des débits allant de 2 à 54 Mbit/s et demain 100 Mbit/s voire plus ;
– les **WMAN** (*Wireless Metropolitain Area Network*) utilisés pour l'accès aux réseaux d'infrastructure (boucle locale radio), ils offrent des débits de plusieurs dizaines de Mbit/s ;
– enfin, les **WWAN** (*Wireless Wide Area Network*), recouvrent essentiellement les réseaux voix avec leurs extensions données (GSM, GPRS et UMTS), les débits sont relativement faibles de quelques dizaines de kbit/s (10 à 384 kbit/s).

La figure 17.30 présente une synthèse de ces principales technologies.

Nom	Fréquence	Débit (Mbit/s)	Portée (m)	Commentaires
Bluetooth	2,4 GHz	1 à 10	10-100	Utilisation personnelle
Wi-Fi (802.11b)	2,4 GHz	11	300	Liaison point à point à haut débit
Home RF	2,4 GHz	1,6 et 10	50	Domotique
IEEE 802.11g	2,4 GHz	54		Successeur du 802.11b
IEEE 802.11a	5 GHz	54		Idem
HiperLAN 2	5 GHz	54		Concurrent du 802.11a

Figure 17.30 Les principales solutions de réseaux sans fil.

17.4.2 La problématique de l'accès aux réseaux sans fil

Les techniques de partage du support hertzien relèvent du multiplexage fréquentiel (**FDMA**, *Frequency Division Multiple Access*) qui divise l'espace de fréquence en canaux, du multiplexage temporel (**TDMA**, *Time Division Multiple Access*) qui alloue toute la bande disponible durant un intervalle de temps prédéterminé, de la combinaison de ces deux techniques (**F/TDMA**) ou encore d'une technique de discernement de voies par attribution d'un code spécifique à chaque communication (**CDMA**, *Code Division Multiple Access*). La figure 17.31 illustre ces différentes techniques étudiées au chapitre 5.

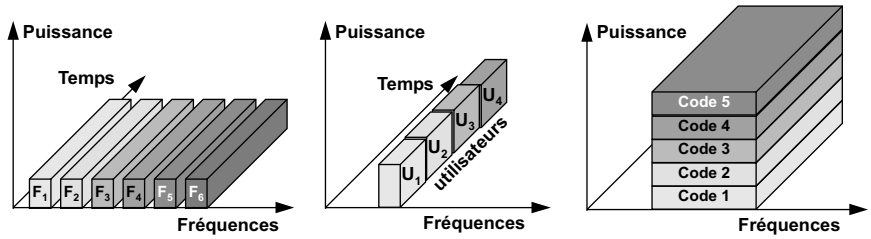


Figure 17.31 Les techniques de partage d'un support hertzien.

Cependant, dans les réseaux à diffusion tels que les réseaux locaux, tout le monde doit pouvoir écouter tout le monde, ce qui implique l'utilisation d'une fréquence unique[2]. Compte tenu que l'on

2. On pourrait imaginer un système où chaque station disposerait d'un ensemble de couples émetteur/récepteur, chaque couple utilisant une fréquence différente serait associé à une relation de type 1 à 1 avec les autres stations du réseau. Ce procédé est inconcevable car le nombre d'éléments récepteurs/émetteurs, pour chaque station, croît comme le carré du nombre de stations N (N–1).

© Dunod – La photocopie non autorisée est un délit

ne peut émettre et recevoir en même temps sur une même fréquence (éblouissement de l'antenne de réception par le signal émis), il n'est pas possible de contrôler que le signal émis n'est pas pollué par une autre émission. La détection de collision, telle que nous la connaissons dans le CSMA/CD, n'est pas réalisable, le canal radio monofréquence est un canal *half duplex*. Aussi, le premier système radio l'Aloha implémentait-il un mécanisme simple : une station qui désire émettre, émet. Le message devait être acquitté immédiatement. Si ce dernier était victime d'une collision, il n'était pas acquitté dans les temps et était retransmis.

Ce procédé est simple, mais lorsque le nombre de stations augmente, le débit efficace s'effondre rapidement. En découpant le temps en tranche canal (*Slot*) et en n'autorisant une station à n'émettre qu'au début d'une tranche, on diminue la probabilité de collision mais on complexifie le système par l'intégration d'un mécanisme de synchronisation (*Slotted Aloha*). Bien qu'inefficaces, les techniques Aloha restent à la base des modes d'accès à compétition.

Dans les réseaux sans fil, pour prévenir les collisions, avant d'émettre, une station écoute le support durant un temps supérieur au délai de propagation le plus long. Si le support est occupé, l'émission est différée, sinon la station poursuit son écoute pendant un intervalle de temps aléatoire et, si le support est toujours libre, émet. Cette technique dite **CSMA/CA** pour *Collision Avoidance* est illustrée figure 17.32.

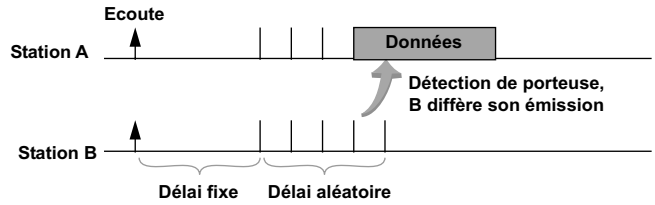


Figure 17.32 Principe du CSMA/CA.

17.4.3 L'architecture générale des réseaux sans fil

Les réseaux « ad-hoc »

Les réseaux « ad-hoc » s'affranchissent de toute infrastructure (figure 17.33). La communication a lieu directement de machine à machine. Une machine peut éventuellement servir de relais pour diffuser un message vers une station non vue (au sens électromagnétique du terme) par la station d'origine (routage). Les stations communicant en mode « ad-hoc » forment un réseau appelé **IBSS** (*Independant Basic Service Set*).

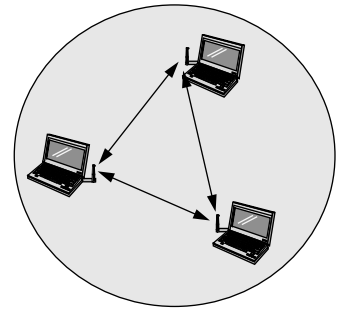


Figure 17.33 Microcellule « ad-hoc » ou IBSS.

Actuellement en mode « ad-hoc », les réseaux **Wi-Fi** (*Wireless Fidelity* ou IEEE 802.11) ne fonctionnent qu'en mode point à point, les réseaux de type Hiperlan implémentent une fonction de relais (« ad-hoc » multisaut) qui autorise la communication entre deux systèmes IBSS. Les protocoles de routage associés font l'objet de nombreuses recherches. Le principe[3] du routage reste cependant identique, lorsqu'une station veut en joindre une autre elle inonde le réseau, son message est répété par toutes les stations jusqu'à la station destination. Le destinataire acquitte le premier message reçu qui emprunte en retour la même voie qu'à l'aller. Chaque machine apprend ainsi la route pour joindre le destinataire (la route est construite à l'envers).

Les réseaux cellulaires

Les réseaux sans fil sont soit indépendants de toute infrastructure filaire, soit en prolongement de celle-ci. Cependant, quel que soit le mode choisi, les solutions adoptées doivent résoudre de nombreux problèmes :

- la bidirectionnalité de la communication, et le nombre de communications à établir en même temps ont conduit au concept de communication cellulaire. Une cellule est une zone dans laquelle les fréquences utilisées appartiennent à un même ensemble. Deux cellules adjacentes ne devront pas utiliser le même ensemble de fréquences (figure 17.34). La dimension limitée d'une cellule (portée radio) autorise la réutilisation des fréquences, la taille de la cellule étant généralement déterminée par le nombre de stations que peut accueillir une base fixe. De petites cellules entraînent une capacité d'accueil globalement plus importante ;
- l'accès multiple et le partage du support (politique d'accès) ;
- la localisation du mobile en déplacement (itinérance ou *Roaming*) ;
- la possibilité pour le mobile en déplacement de maintenir la communication en cours (*Hand over* ou *Handoff*) ;
- l'identification et la confidentialité des communications.

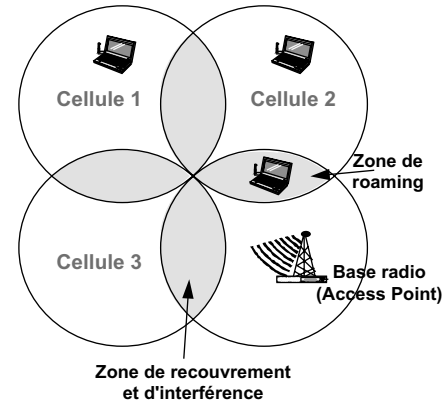


Figure 17.34 Principe d'un réseau cellulaire.

3. Ces techniques posent aujourd'hui de nombreux problèmes, en relation avec la sécurité (les messages sont stockés par les stations intermédiaires avant réémission) et la fiabilité (arrêt d'une station en cours de retransmission...).

© Dunod – La photocopie non autorisée est un délit

Une cellule est centrée autour de sa base radio (**AP**, *Access Point*). Lorsqu'un mobile quitte une cellule (**BSS**, *Basic Service Set*), pour maintenir la communication, il doit être accueilli par une autre cellule. Les techniques de gestion de la mobilité sont différentes selon que le mobile est un mobile voix (téléphone) ou un mobile données (station). Une communication téléphonique peut être interrompue quelques millisecondes sans nuire à l'intelligibilité de la conversation (temps de basculement d'une cellule vers une autre). Dans un service données, la moindre interruption provoque une erreur de transmission. Dans ces conditions, le basculement d'une cellule ne peut avoir lieu que dans la zone de recouvrement des cellules et en fin de transmission d'un paquet, on parle alors seulement de *roaming* et non plus de *hand over* (figure 17.34).

17.4.4 Les réseaux 802.11

L'architecture

Le réseau IEEE 802.11 est basé sur une architecture de type cellulaire (figure 17.35). Chaque cellule, **BSS** (*Basic Service Set*), est contrôlée par une base radio, (**AP**, *Access Point*). Un BSS est identifié par un **BSSID** (*Basic Service Set Identifier*), cet identifiant, sur 6 octets, correspond à l'adresse MAC du point d'accès. Le réseau peut comporter une ou plusieurs cellules autonomes ou être le prolongement d'un réseau Ethernet traditionnel. Dans ce dernier cas, les différents points d'accès sont reliés à un réseau de distribution qui fait office de *backbone* (**DS**, *Distribution System*). La liaison entre les différents AP peut être filaire ou radio (**WDS**, *Wireless Distribution System*). L'ensemble forme un seul réseau 802.11 désigné sous le terme de **ESS** (*Extended Service Set*). L'ESS est identifié par un *ESSID*, identifiant sur 32 octets qui sert de nom au réseau. La connaissance de l'ESSID est nécessaire pour se connecter au réseau. Les réseaux 802.3 et 802.11 sont interconnectés par un élément actif assurant l'adaptation des formats : le portail (pont à translation).

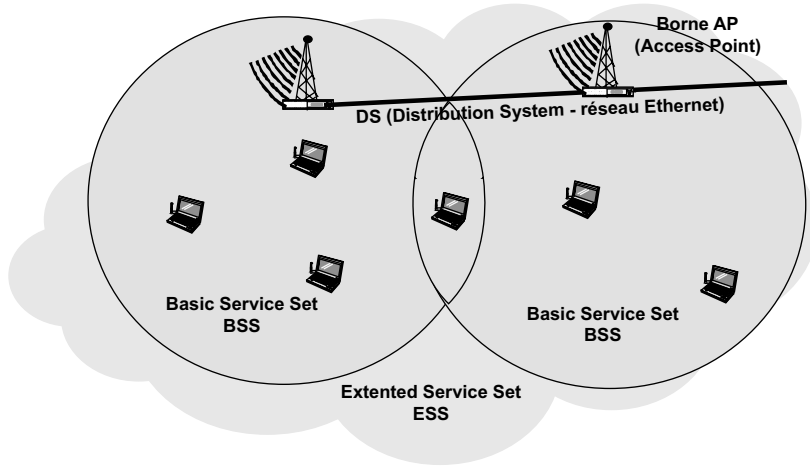


Figure 17.35 L'architecture matérielle du réseau IEEE 802.11.

Le niveau physique ou l'interface radio

➤ Généralités

Le niveau physique découpé en deux couches, l'une de convergence (**PLCP**, *Physical Layer Convergence Protocol*) et l'autre dépendant du type de modulation utilisé (**PMD**, *Physical Medium Dependent*), a pour objet la transmission des bits sur le support hertzien. Le support hertzien étant un support sujet aux perturbations : signaux parasites (bruit), aux interférences avec d'autres systèmes radios, à l'évanouissement dû aux multi-trajet (*fading*), les réseaux Wi-Fi utilisent des techniques de modulation présentant une bonne résistance à ces phénomènes perturbateurs comme les techniques d'étalement de spectre dans la bande des 2,4 GHz ou une modulation de type **OFDM** (*Orthogonal Frequency Division Multiplexing*) dans la bande des 5 GHz. La figure 17.36 présente les différentes implémentations des réseaux 802.11, les techniques IR (infrarouge) sont aujourd'hui obsolètes.

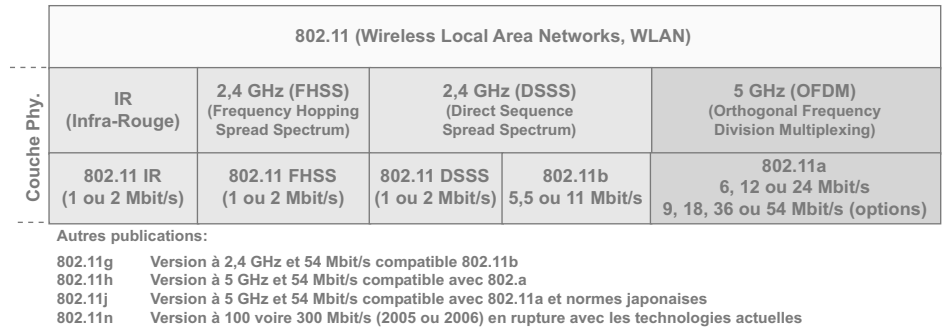


Figure 17.36 Synthèse des publications 802.11.

➤ Les techniques d'étalement de spectre

L'étalement à sauts de fréquence (FHSS)

Dans la technique d'étalement de spectre à sauts de fréquence (**FHSS**, *Frequency Hopping Spread Spectrum*), la bande des 2,4 GHz est divisée en sous-canaux de 1 MHz de largeur (figure 17.37). Cette technique se caractérise par des changements de fréquence parfaitement synchronisés (sauts de fréquence).

Pays	Bande de fréquences	Nombre de canaux
États-Unis (FCC)	2,400 - 2,485 GHz	79
Europe (ETSI)	2,400 - 2,485 GHz	79
Japon (MKK)	2,471 - 2,497 GHz	23
France (ANF)	2.4465 - 2,4835 GHz	35

Figure 17.37 Allocation des fréquences utilisées en 802.11 FHSS.

La synchronisation des sauts de fréquence est réalisée par l'émission périodique d'une trame de synchronisation dite « trame balise (*Beacon frame*) » qui identifie la séquence et fixe la durée de chaque saut. Pour s'insérer dans un réseau, une station doit attendre cette trame balise pour identifier la séquence de sauts (figure 17.38). Les schémas de sauts de fréquence sont déterminés pour minimiser le risque que deux systèmes utilisent à un moment donné la même fréquence.

© Dunod – La photocopie non autorisée est un délit

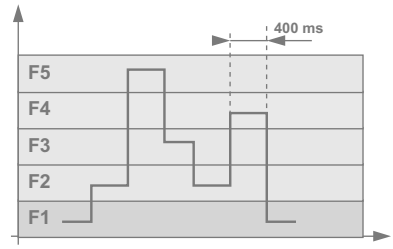


Figure 17.38 Exemple de séquence pseudo-aléatoire de sauts de fréquence.

La porteuse est modulée en phase (**PSK**, *Phase Shift Keying*) selon le mode **BPSK** (*Binary PSK*) qui code deux états (bit = 0 → $\varphi = 0$; bit à 1 → $\varphi = \pi$) ou le mode **QPSK** (*Quadrature PSK*) qui code quatre états (symbole 00 → $\varphi = 0$; 11 → $\varphi = \pi/2$; 01 → $\varphi = \pi$; 10 → $\varphi = \pi/2$), ce qui, compte tenu d'un canal limité à 1 MHz conduit à des débits respectifs de 1 et 2 Mbit/s. La version 802.11 FHSS n'est pratiquement plus utilisée aujourd'hui.

L'étalement à séquence directe

L'étalement de spectre à séquence directe (**DSSS**, *Direct Sequence Spread Spectrum*) autorise chaque canal à utiliser l'intégralité de la bande de fréquence allouée mais chaque communication utilise un code unique (**CDMA**, *Code Division Multiple Access*). En multipliant la séquence binaire à émettre par une autre séquence binaire dite **Barker** telle qu'à 1 bit du signal binaire corresponde *N* « bits » du signal émis. La nouvelle séquence ainsi constituée est dénommée *chip* (puce) ou *chipping code* (figure 17.39) Le nombre de transitions électriques est plus élevé et par conséquent le spectre plus large. En réception, le signal reçu est multiplié par la même séquence, on retrouve ainsi le signal binaire d'origine, cette opération « reconcentre » le spectre du signal d'origine, mais étale le spectre des éventuels signaux parasites, améliorant ainsi la résistance au bruit du signal d'origine (voir chapitre 5, § 5.2.4).

Dans les réseaux 802.11, la séquence d'étalement substitue à 1 bit à 1 la séquence « 1011 0111000 » et à 1 bit à 0 son complément soit « 01001000111 ». Ces séquences de Barker ne permettent que de coder deux états (0 ou 1). En codant plusieurs bits de données par *chip*, la technique dite du **CCK** (*Complementary Code Keying*) permet d'atteindre des débits plus élevés (802.11 HR, *High-Rate*). La figure 17.39 indique, en fonction des versions, le type de codage utilisé.

Technologie	Codage	Bits/symbole	Modulation	Débit Mbit/s
802.11b	11 bits (*Barker sequence*)	1	PSK	1
802.11b	11 bits (*Barker sequence*)	2	QPSK	2
802.11b	CCK	4	QPSK	5,5
802.11b	CCK	8	QPSK	11
802.11a	CCK	8	OFDM	54
802.11g	CCK	8	OFDM	54

Figure 17.39 Le codage et les différentes versions de 802.11.

Les versions 802.11b et g utilisent la bande des 2,4 GHz (2,412 à 2,484 GHz) divisée en 14 canaux de 22 MHz espacés de 5 MHz, de ce fait les canaux se recoupent partiellement (figure 17.40).

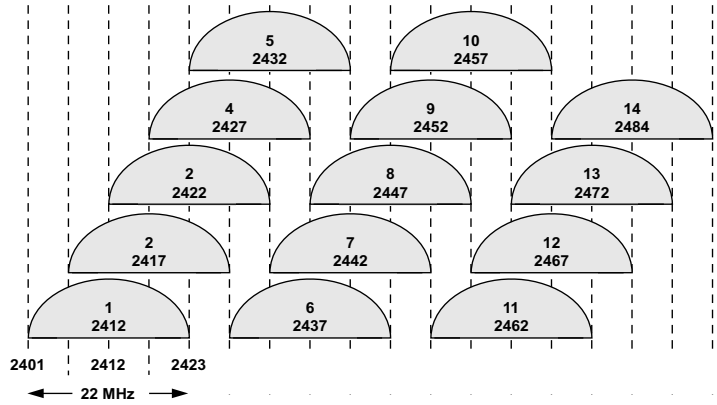


Figure 17.40 L'allocation à 802.11 des canaux de la bande ISM.

Aux États-Unis seuls les canaux 1 à 11 peuvent être utilisés, en France les 13 premiers canaux et au Japon seul le canal 14 est disponible. Le schéma de la figure 17.40 montre qu'en fait, pour qu'il n'y pas de chevauchement de fréquence, seuls trois canaux peuvent être utilisés simultanément pour former un réseau Wi-Fi.

➤ La modulation OFDM

La modulation **OFDM** (*Orthogonal Frequency Division Multiplexing*) ou encore **DMT** (*Discrete MultiTone modulation*) utilisée notamment dans les techniques **DSL** (*Digital Subscriber Line*) repose sur le principe du multiplexage fréquentiel. Le canal de transmission est découpé en sous-canaux, chaque sous-porteuse transporte *N* bits ou symboles. L'OFDM en répartissant le flux binaire sur *N* porteuses (figure 17.41), divise par *N* la rapidité de modulation de chaque porteuse réduisant ainsi les effets de l'interférence de symboles et optimisant l'utilisation du spectre radio-fréquence.

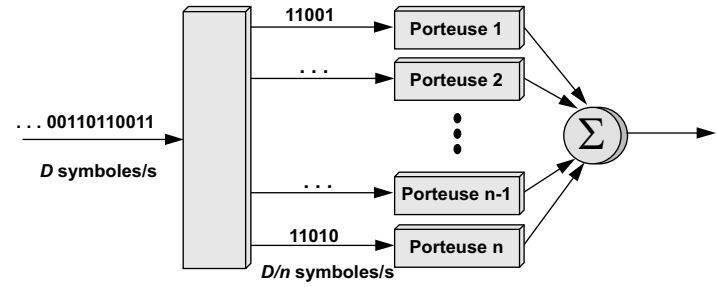


Figure 17.41 Principe de la modulation OFDM.

L'optimisation de l'occupation de l'espace fréquentiel conduit à définir des porteuses proches les une des autres, engendrant ainsi un risque d'interférence entre porteuses adjacentes (**ICI**, *Inter Carrier Interférence*). Aussi, pour minimiser ce risque, les sous-porteuses sont définies de telle manière que le maximum de puissance de leur spectre corresponde au minimum de puissance des porteuses voisines (porteuses dites orthogonales).

© Dunod – La photocopie non autorisée est un délit

L'utilisation de multiporteuses autorise aussi à adapter le débit aux conditions de propagation. En fonction des conditions de transmission (distance, perturbations...) le débit peut être réduit de 54 Mbit/s à 48, 36, 24, 12 et enfin 6 Mbit/s. Dans la bande des 5 GHz (802.11a), les canaux d'une largeur de 20 MHz sont espacés de 5 MHz, allant de 5 170 GHz pour le canal 34 à 5 320 GHz pour le canal 64 (figure 17.42). Chaque canal comporte 52 sous-canaux de 300 kHz, dont quatre sont utilisés pour la correction d'erreur. De même que pour le DSSS, le schéma montre qu'il est nécessaire d'avoir un écartement d'au moins quatre canaux pour éviter tout recouvrement de spectre.

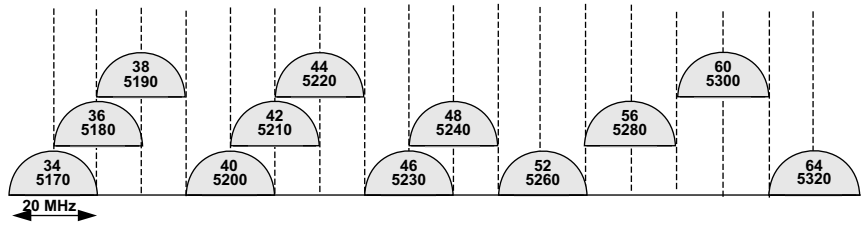


Figure 17.42 Les canaux disponibles et les fréquences dans la bande des 5 GHz.

La publication 802.11a implémente deux mécanismes destinés à choisir le meilleur canal de transmission et éviter les interférences : le **DCS** (*Dynamic Channel Selection*) et le **TPC** (*Transmit Power Control*).

➤ La portée des réseaux 802.11

La portée est, dans les systèmes radio mobiles, l'un des problèmes cruciaux. Accroître la zone géographique couverte impose qu'une borne d'accès ait plus de mobiles à gérer, divisant ainsi le débit total par le nombre de stations à gérer. Diminuer la puissance nécessite, pour couvrir une même zone géographique, l'utilisation de plusieurs cellules donc de fréquences. Enfin, en émission, la puissance nécessaire croît comme le carré de la portée ce qui, pour une station mobile, est consommateur d'énergie. Aussi, la norme 802.11 implémente-elle un mécanisme d'économie d'énergie.

Les réseaux Wi-Fi implémentent deux modes de fonctionnement. Le mode économie d'énergie (*Power save polling mode*) et le mode normal dit service continu (*Continuous aware mode*) qui est le mode de fonctionnement par défaut. La fonction de gestion de l'énergie ne peut être activée que dans le mode infrastructure. Lors de l'émission de données, une station qui met en œuvre le mode économie d'énergie en informe l'AP (*Access Point*). Celui-ci mémorise alors, pour cette station, toutes les trames qui lui sont destinées. Périodiquement l'AP émet dans la trame balise la liste des stations qui ont des données en attente (**TIM**, *Traffic Information Map*), cette période correspond à une période de réveil des stations en veille (synchronisation par la trame balise). La ou les stations concernées émettent alors une requête de demande de transfert de données (**PRF**, *Polling Request Frame*). Le transfert achevé, elles retournent en mode veille jusqu'à la prochaine période de réveil (figure 17.43).

Dans la figure 17.43, la première trame balise informe la station ***A*** qu'elle a des données en attente dans l'AP (*Access Point*). La station ***A*** se déclare prête à recevoir ces données (trame PRF). L'AP lui adresse ses données, en fin de réception la station ***A*** reprend le mode veille. La station ***B*** n'a pas de données en attente d'émission ni chez l'AP, ni chez elle, elle se remet en veille jusqu'à la prochaine trame balise. À la prochaine trame balise, c'est la station ***B*** qui a des données à émettre, elle les transmet à l'AP et revient au mode veille.

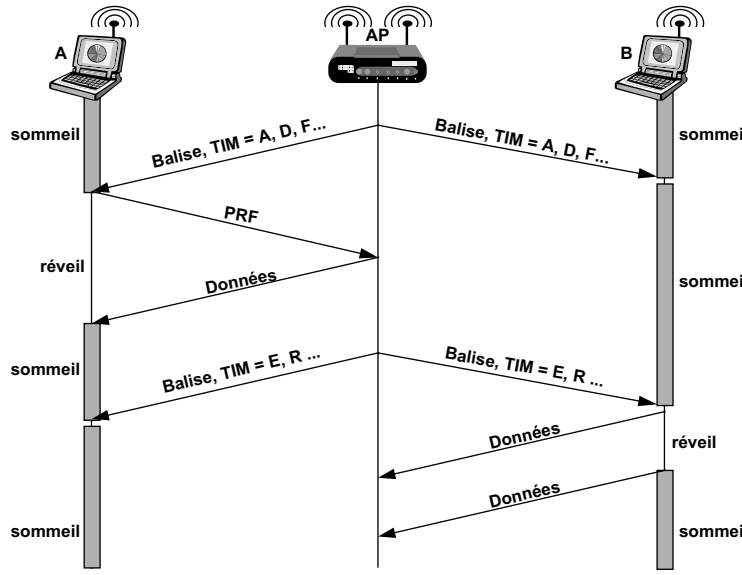


Figure 17.43 Principe du mode économie d'énergie.

Les stations sont informées de l'envoi de données *multicast* et *broadcast* par l'envoi d'une trame TIM particulière dite : **DTIM** (*Delivery Traffic Information Map*).

Enfin, la puissance d'émission est limitée non seulement par les problèmes en relation avec l'autonomie des systèmes mais aussi par les réglementations locales. Ainsi, en France à l'intérieur des bâtiments (*Indoor*), la puissance est limitée à 100 mW dans la bande 2,400–2,485 GHz et à l'extérieur (*Outdoor*) à 100 mW dans la bande 2,400–2,457 GHz et seulement 10 mW dans la bande 2,454–2,4835 GHz. La figure 17.44 indique la portée théorique des systèmes en fonction débit pour un émetteur émettant à la puissance maximale autorisée.

Débit (Mbit/s)	Portée (m)	
Toutes versions	*Indoor*	*Outdoor*
11	50	200
5	75	300
2	100	400
1	150	500
802.11a		
54	10	
48	17	
38	25	
24	30	
12	50	
6	70	

Figure 17.44 La zone de couverture des réseaux 802.11.

© Dunod – La photocopie non autorisée est un délit

On montre[4] aussi que l'atténuation d'une onde radio est d'autant plus importante que la fréquence de la porteuse est élevée. Aussi pour conserver de distances acceptables, les puissances admises pour la bande des 5 GHz sont plus élevées (figure 17.45).

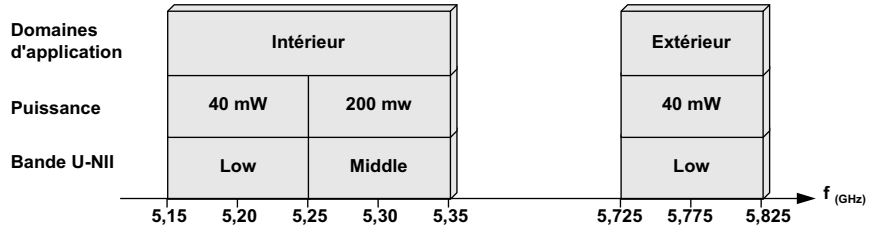


Figure 17.45 La puissance d'émission dans la bande des 5 GHz.

Cependant la portée est d'environ 30 % plus faible, ce qui, en cas d'évolution du réseau d'une solution à 2,4 vers une à 5 GHz, nécessite une nouvelle étude d'implantation du site, avec toutes les difficultés en relation avec les éventuels recouvrements de fréquence non seulement dans le plan horizontal, mais aussi dans le plan vertical (immeuble de bureau), alors que l'on ne dispose pas forcément de la maîtrise des fréquences utilisées par ses voisins (figure 17.46) !

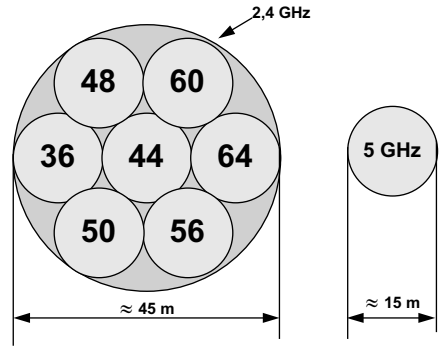


Figure 17.46 La comparaison d'une cellule 2,4 GHz et d'une cellule 5 GHz.

Le niveau MAC ou l'accès au support

➤ Généralités

La couche liaison de données est scindée en deux sous-couches, la couche LLC et la couche MAC. Seule la définition de la couche MAC nous intéresse ici. La couche MAC définit deux modes d'accès au canal, un mode d'accès par défaut qui organise un accès à compétition (**DCF**, *Distribution Coordination Function*) et un mode d'accès optionnel proche du mode à réservation (**PCF**, *Point Coordination Function*) avec un contrôle centralisé géré par le point d'accès. Ces modes d'accès mettent en œuvre un mécanisme d'accès au support contrôlé par l'utilisation de silences inter-trames (**IFS**, *InterFrame Spacing*) décrit figure 17.47. Ce mécanisme induit une prioritisation à l'émission d'une trame, ainsi un accusé de réception bénéficie d'un silence inter-trame plus court qu'une trame de données ordinaire.

4. L'atténuation est donnée, en milieu libre, par la relation : $A = 20 \log d \left[\frac{4\pi}{\lambda}\right]$
où λ est la longueur d'onde du signal et d la distance en mètres entre l'émetteur et le récepteur.

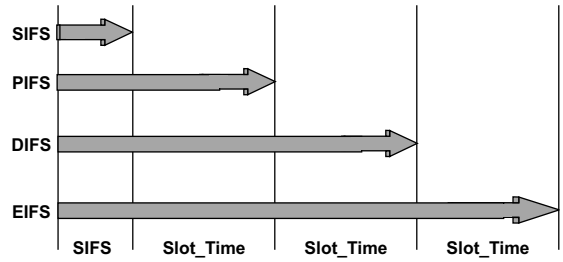


Figure 17.47 Les différents intervalles d'espacement entre trames (IFS).

Le *Short IFS* (**SIFS**) est le plus petit silence inter-message. Il donne une priorité absolue à certains messages et notamment aux acquittements. Sa valeur dépend de la version utilisée. Le *Point Coordination Function IFS* (**PIFS**) est utilisé par les bornes d'accès pour l'émission de données qui disposent ainsi d'un accès prioritaire par rapport à l'émission des stations toujours précédé, sauf pour les ACK, d'un silence inter-message plus important (*Distributed Coordination Function*, **DIFS**). Enfin, **EIFS** (*Extended IFS*) est utilisé pour toute retransmission après réception d'une trame incorrecte (CRC ou collision). Chaque IFS correspond à la valeur de son précédent augmentée du *Slot_Time* défini dans l'algorithme de *Backoff*.

➤ Le mode *Distributed Coordination Fonction* (DCF)

Mode de base

Le mode DCF implémente une fonction de contrôle de l'accès au support distribué dont le principe de base est très simple : une station voulant transmettre un message s'assure que le support est libre durant un certain temps fixe et prédéterminé (DIFS), puis poursuit cette écoute durant un temps aléatoire (fonction de *BackOff*) de *N Slot_Time*, si le support est toujours libre, la station émet. Chaque message transmis doit être acquitté immédiatement (sauf le trafic *multicast* et *broadcast* qui n'est pas acquitté), le destinataire, procède de même pour l'envoi de l'ACK, mais ne vérifie la disponibilité du support que durant un intervalle de temps réduit (SIFS). Le dialogue entre la station *A* et *B* de la figure 17.48 illustre le mécanisme

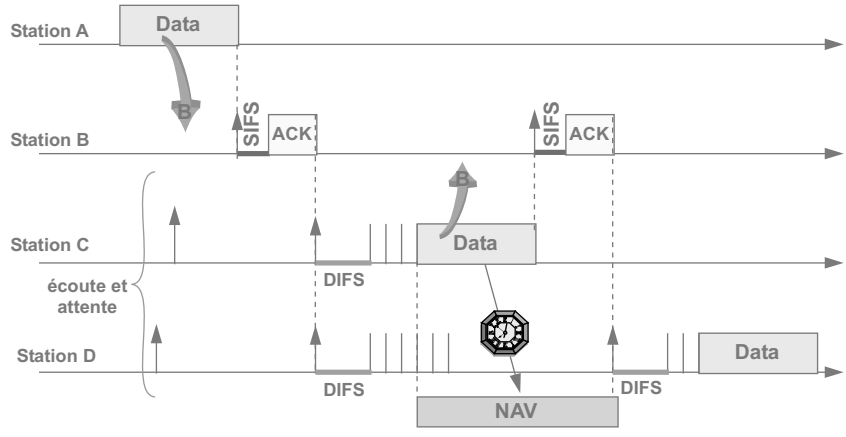


Figure 17.48 Principe de l'accès DCF, sans collision.

© Dunod – La photocopie non autorisée est un délit

Pour réduire la probabilité de collision, ce mécanisme est complété un mécanisme de réservation dit : *Virtual Carrier Sense*. Toute trame émise contient une information sur la durée totale du cycle de transmission (données + ACK). Ainsi toute station écoutant le support, à réception de cette information, positionne un temporisateur (**NAV**, *Network Allocation Vector*) et s'interdit toute émission durant cet intervalle de temps : dans la figure 17.48, le dialogue entre *C* et *B*, est entendu par *D* qui positionne son NAV, diffère son émission d'autant. À l'échéance de ce timer, *D* réinitialise un cycle d'acquisition du support (DIFS + *BackOff*).

Ce mécanisme tente de prévenir les collisions, mais ne garantit nullement que deux stations n'émettront pas en même temps. La collision ne pouvant être détectée par écoute du support, l'émission des données se poursuit, c'est la non-réception de l'ACK qui informe la station de l'état de collision. La station doit alors retransmettre le message dans son intégralité. Cependant, durant l'état de collision, les stations n'ont pu positionner leur NAV (message altéré), aussi, pour éviter des collisions multiples, le délai d'écoute du support est-il étendu (EIFS). La figure 17.49 illustre ce mécanisme.

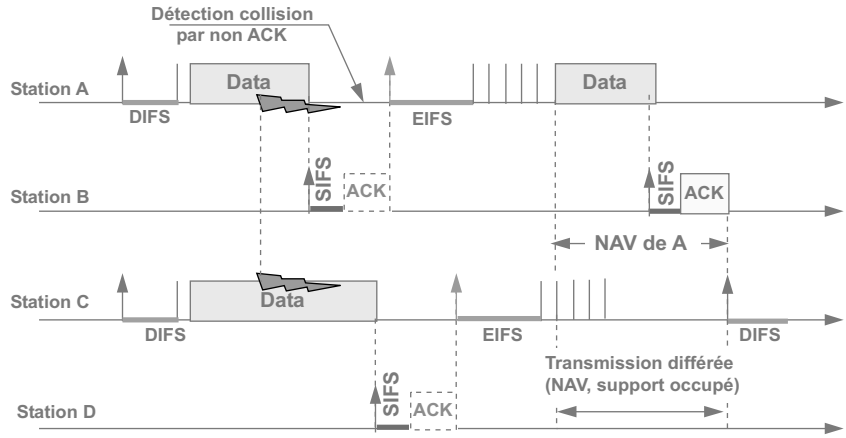


Figure 17.49 Principe de l'accès DCF, avec collision.

Problème de la station cachée

L'une des causes principale de collision provient du phénomène dit de la station cachée. Ainsi, figure 17.50, la station *B* est à portée radio de *A* et de *C*, mais *A* et *C* ne se voient pas (au sens électromagnétique du terme). Supposons que la station *A* doive transmettre des données à destination de la station *B*. Elle écoute le support, celui-ci est libre, elle émet. Cependant, dans le même temps, la station *C* désire aussi transmettre des données à *B* ou à une autre machine de la zone d'interférence. La station *C* est hors de portée radio de *A* (station cachée), elle n'entend pas le message de *A*, et considère le support libre, elle transmet ses données. Les données de *A* et de *C* sont polluées, il y a collision.

À cet effet, un mécanisme optionnel permet à la station *C* d'être informée de l'intention de *A*. À l'acquisition du support, la station *A* émet une trame très courte (**RTS**, *Request to Send*) ne contenant que l'information de réservation du support (**NAV**), à réception la station *B* acquitte cette trame (**CTS**, *Clear to Send*), la valeur du NAV de cette trame est décrémentée du temps déjà écoulé. Ainsi, la station *C*, à portée radio de *B*, est informée que le support est occupé par *A* (figure 17.51).

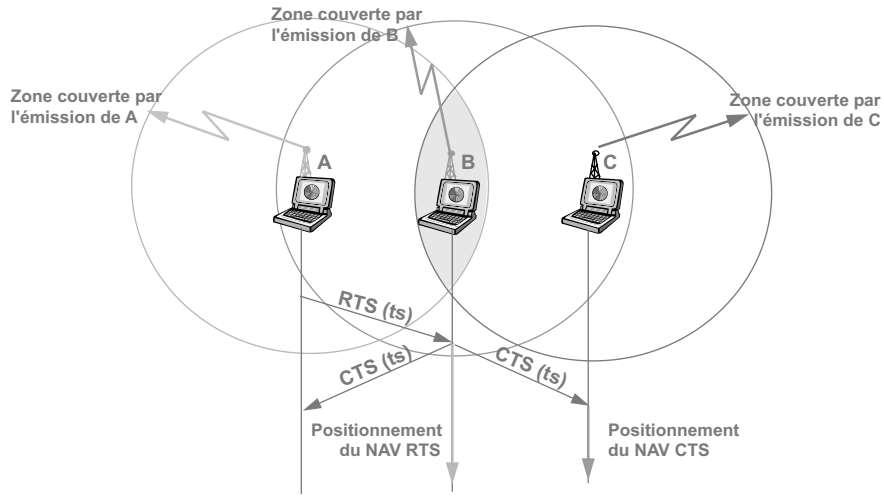


Figure 17.50 Problème de la station cachée.

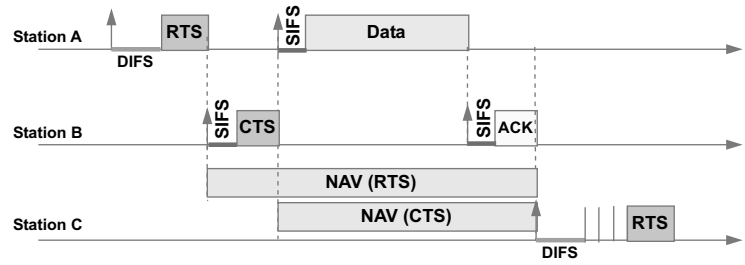


Figure 17.51 Principe de l'accès en mode RTS/CTS.

Ce mécanisme, optionnel, est très efficace. Les trames RTS/CTS sont courtes par conséquent, la probabilité de collision est alors faible. Malgré tout, si une collision se produisait, elle serait détectée beaucoup plus tôt que si elle affectait une trame de données. Cependant, si les trames de données à émettre sont de petite taille, le mécanisme RTS/CTS pénalise les performances, aussi, le standard autorise-t-il à ce que les trames inférieures à une certaine taille, fixée par l'administrateur (*RTS Theshold*, seuil RTS), soient transmises directement.

➤ Le mode *Point Coordination Function* (PCF)

Le mode DCF introduit un mode d'accès à compétition, l'acquisition du support n'est pas bornée et, par conséquent, ce mode de transmission ne convient pas aux données ayant des exigences temporelles strictes comme les flux multimédias (données isochrones). Aussi, la norme introduit-elle un mode d'accès optionnel : le **PCF**, *Point Coordination Function.* Ce mode définit un mécanisme de scrutation (*Polling*) géré par le point d'accès (AP). Cependant le mécanisme de *polling*, s'il borne l'accès, est consommateur de bande passante. Aussi, pour améliorer le rendement du PCF et assurer aux stations incompatibles avec ce mode de fonctionnement l'accès au support, le PCF divise le temps en deux périodes :

– la première période correspond à la mise en œuvre du mode PCF, elle est dite *Contention Free Period* (**CFP**) ;

© Dunod – La photocopie non autorisée est un délit

– la seconde période utilise la méthode d'accès de base (DCF), elle est dite *Contention Periode* (**CP**).

Dans la première période (CFP), les stations n'émettent leurs données que sur invitation explicite de l'AP auquel elles sont associées. Puis dans la seconde période, toutes les stations peuvent émettre leurs données en utilisant l'accès traditionnel à compétition du mode DCF. Les différentes périodes sont délimitées par des trames balises qui indiquent la durée de chaque phase. En mode PCF, une station « pollée » doit répondre dans un intervalle de temps prédéterminé (PIFS), sinon le point d'accès passe à la station suivante. À tout moment, le point d'accès peut mettre fin à la période de PCF et basculer en mode DCF par l'envoi d'une trame **CF-End** (*Contention Free End*).

Pour prendre en compte les exigences de QoS, la recommandation 802.11e introduit une amélioration du DCF (**EDCF**, *Enhanced DCF*) et du PCF (**EPCF**, *Enhanced PCF*). En mode EDCF, la durée d'attente DIFS devenue l'**AIFS** (*Arbitration IFS*) dépend du niveau de priorité de la trame à transmettre et, en mode EPCF, c'est l'AP qui définit, en fonction de la classe de priorité du flux, à chaque station les paramètres de trafic.

➤ L'association d'une station et d'un AP

En mode infrastructure, le mécanisme d'association permet à une station d'être prise en charge par un AP. Périodiquement, un AP diffuse une trame balise contenant le nom du réseau (SSID) et les caractéristiques de celui-ci (débit, BSSID du point d'accès et éventuellement le ESSID), une station possédant le même SSID (appartenant au même réseau) et désirant se connecter à ce réseau y répond par une trame *Probe request*, l'AP y répond (*Probe response*) et déclenche une phase d'authentification, ce mode d'association est dit passif. Dans l'association active, c'est la station qui prend l'initiative de la connexion en émettant des trames *Probe request* contenant le nom du réseau auquel elle veut se connecter.

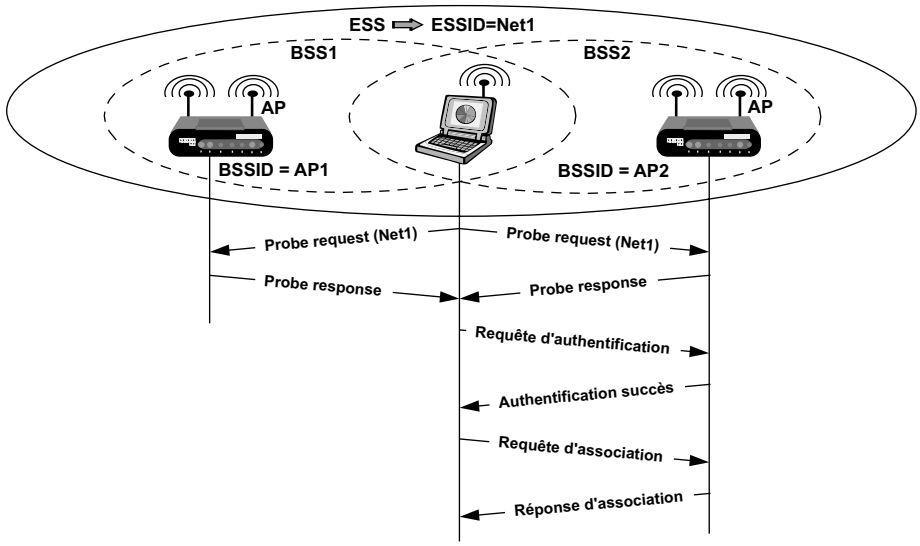


Figure 17.52 Le mécanisme d'association en mode actif.

La figure 17.52 illustre le scénario de rattachement d'une station à une cellule, le réseau est composé de 2 cellules. La station diffuse sa demande d'enregistrement (trame *Probe Request* en mode *broadcast*). Les AP y répondent (*Probe Response*), la station sélectionne alors l'un des AP (niveau du signal, taux d'erreur...) et émet une requête d'authentification (authentification ouverte). Dans ce mode d'authentification, si la station fournit le bon SSID, l'authentification est considérée comme positive. La station s'enregistre alors auprès de l'AP (association) en fournissant notamment ses caractéristiques et son adresse MAC.

Dans le mode dit « association fermée », l'AP envoi un défi à la station, si la réponse à celui-ci est correcte, la station est authentifiée et peut donc s'enregistrer. Le mécanisme d'association est reproduit à chaque fois qu'une station se déplace (*Roamming*) et veut s'enregistrer à un nouvel AP dont le signal est de meilleure qualité (requête de déassociation avec l'ancien AP, puis requête d'association avec le nouvel AP).

➤ Le mécanisme de fragmentation

Les transmissions hertziennes sont d'autant plus sensibles aux perturbations que la trame émise est grande. Aussi, pour améliorer la fiabilité des réseaux 802.11, la couche MAC implémente un mécanisme de fragmentation et de réassemblage. Ce mécanisme diminue la probabilité qu'une trame émise soit erronée, mais aussi améliore le rendement de transmission, en effet, la retransmission d'un fragment est moins coûteuse en bande passante que celle de l'intégralité de la trame d'origine. La figure 17.53 illustre le principe de la fragmentation, on remarquera que l'indication de durée contenue dans chaque fragment protège la séquence d'émission du fragment en cours, mais aussi celle du fragment suivant.

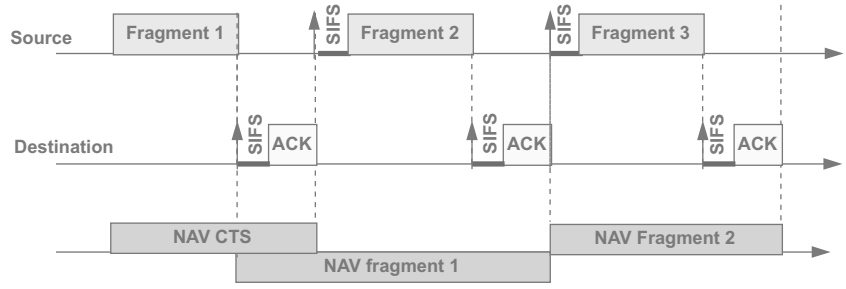


Figure 17.53 Le mécanisme de fragmentation.

➤ Les différentes trames MAC

Les réseaux Wi-Fi utilisent trois types de trames :

- les **trames de données**, utilisées pour transmettre les données utilisateur ;
- les **trames de contrôle** de l'accès au support (RTS, CTS, ACK) ;
- enfin les **trames de gestion** de l'interface Wi-Fi, comme les trames d'association...

Ces trames sont distinguées par le sous-champ **Type** (2 bits) et **Sous-Type** (4 bits) du champ Contrôle de la trame MAC (figure 17.55). La figure 17.54 fournit quelques exemples de codage des champs Type et Sous-Type.

© Dunod – La photocopie non autorisée est un délit

Type			Libellé
Codage (binaire)	Catégorie	Sous-Type (binaire)	
00	Gestion	0000	Requête d'association
		0001	Réponse d'association
		1000	Balise (*Beacon*)
		1011	Authentification
01	Contrôle	1011	RTS
		1100	CTS
		1101	ACK
10	Données	0000	Données utilisateur

Figure 17.54 Quelques exemples de type de trames 802.11.

La trame 802.11 comporte trois parties, un en-tête MAC (*MAC header*) de 30 octets, un champ Données variant de 0 à 2 312 octets et enfin le traditionnel champ de contrôle : le FCS (*Frame Check Sequence*). L'émission de la trame est toujours précédée par celle d'un préambule de synchronisation de 12 octets (format court) ou 16 octets (format long), suivi d'un en-tête ajouté par la couche de convergence (**PLCP**, *Physical Layer Convergence Protocol*). La figure 17.55 détaille chacun de ces champs.

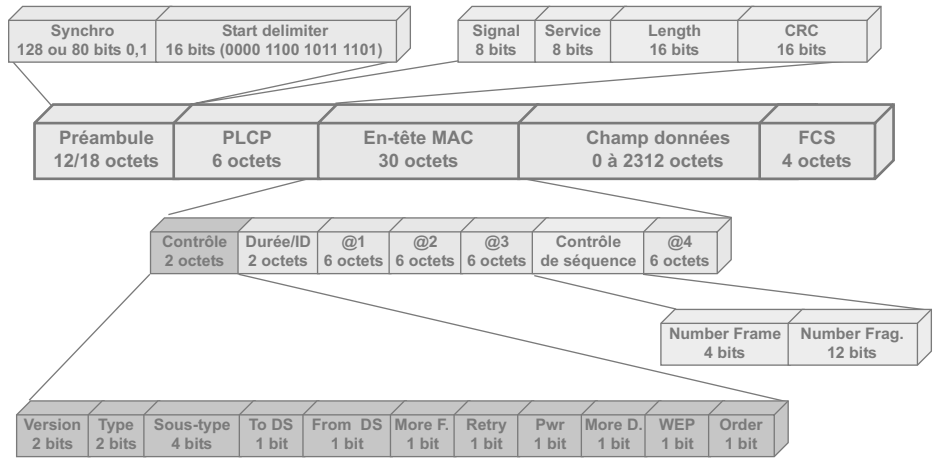


Figure 17.55 Trame MAC 802.11.

L'en-tête physique de convergence contient un ensemble d'information nécessaire au décodage de la trame et en particulier le champ **Signal** qui indique le débit d'émission de la trame, le champ **Length** qui fournit en octets la longueur de la trame. L'ensemble étant protégé par un CRC. Le champ **Service** est inutilisé (positionné à 0). Pour pouvoir être interprété par toutes les stations, l'en-tête PLCP est toujours émis au débit de 1 Mbit/s. Dans la version 802.11a et g, le préambule et l'en-tête OFDM, sont, pour les mêmes raisons, toujours émis à 6 Mbit/s, et insérés entre l'en-tête PLCP et l'en-tête MAC.

Le champ **Contrôle** sur 2 octets fournit les informations suivantes :

- **Version**, sur 2 bits, ce champ indique la version utilisée, actuellement ce champ est toujours positionné à 0 ;
- **Type** et **Sous-Type** distinguant les différentes trames, la signification de ces champs est indiquée dans la figure 17.54 ;
- **To Ds** et **From Ds**, ces champs utilisés uniquement en mode infrastructure (*Distribution system*, **Ds**), permettent d'indiquer (bit à 1) si la trame est destinée au point d'accès (*To Ds*) ou s'il provient du point d'accès (*From Ds*) ;
- **More Fragment**, ce champ indique (bit à 1) si 1 fragment suit celui en cours ou si la trame reçue est le dernier fragment (bit à 0). Lorsque la trame n'a pas été fragmentée, ce champ est évidemment à 0 ;
- **Retry**, ce champ à 1 indique que la transmission en cours est en fait une retransmission sur non réception d'ACK MAC ;
- **Pwr** (*Power*), ce champ à 1 indique qu'après cette trame, la station passe en mode économie d'énergie ;
- **More Data**, en mode économie d'énergie, ce bit est positionné par le point d'accès pour indiquer qu'il dispose encore de données à transmettre après la trame en cours. Ceci évite que la station ne passe en mode sommeil après réception de la trame en cours ;
- **WEP**, ce bit indique que le champ Données de la trame est chiffré avec l'algorithme du WEP ;
- Enfin, le champ **Order** indique que la trame reçue appartient à une classe de service où l'ordre des données doit être respecté (*Strictly Ordered Class Service*) et que par conséquent le point d'accès doit retransmettre les trames dans l'ordre dans lequel il les a reçues.

Le champ Durée/ID a deux significations. En mode économie d'énergie, dans les trames de *polling*, il identifie la station « pollée ». Dans toutes les autres trames, il indique la durée d'utilisation du canal, et permet le positionnement du NAV (*Network Allocation Vector*). Les champs Adresses peuvent contenir jusqu'à quatre adresses selon la position des bits *To Ds* et *From Ds* (figure 17.56), la quatrième adresse n'étant utilisée qu'en mode **WDS** (*Wireless Distribution System*).

Mode de fonctionnement	To Ds	From Ds	@1	@2	@3	@4
Mode ad-hoc	0	0	DA	SA	BSSID	0
Infrastructure message AP vers station	0	1	DA	AP	SA	0
Infrastructure message de la station vers l'AP	1	0	AP	SA	DA	0
Infrastructure message d'un AP vers un autre AP WDS	1	1	AP suivant	AP	DA	SA

DA (*Destination Address*) : adresse MAC Destination
SA (*Source Address*) : adresse MAC Source
AP (*Access Point*) : adresse MAC de l'AP (BSSID de la cellule)
RA (*Receive Address*)
TA (*Transmit Address*)
BSSID (*Basic Service Set Identifier*)
WDS (*Wireless Distribution System*)

Figure 17.56 L'utilisation des champs Adresses.

© Dunod – La photocopie non autorisée est un délit

Afin d'éliminer les trames dupliquées, trames retransmises sur temporisation, mais correctement reçues par le destinataire par exemple ACK corrompu, le sous-champ **Contrôle de séquence** assure la numérotation des trames émises (*Number frames*). Le second sous-champ (*Number fragment*) est utilisé par le destinataire pour assurer le réassemblage des différents fragments.

La figure 17.57 illustre le format des trames MAC les plus couramment utilisées. En fonction des différents types de trames, tous les champs ne sont pas présents.

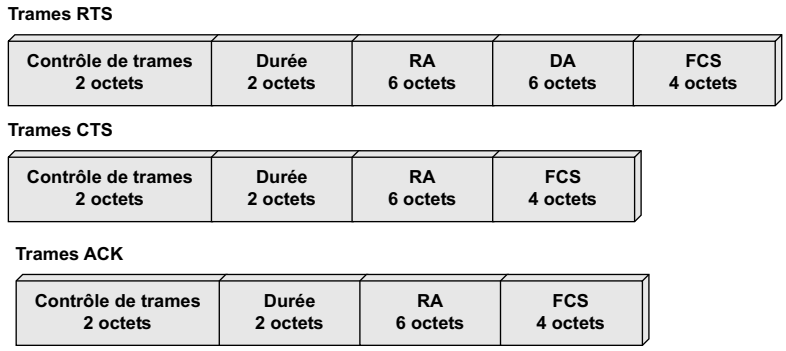


Figure 17.57 Exemples de trames de contrôle.

Dans la trame RTS, le champ **RA** indique l'adresse du destinataire final de la trame de données et le champ **TA** l'adresse source (adresse de la station qui transmet le RTS). Le champ Durée contient en μs la durée totale de l'échange (Données et CTS). Le champ Durée de la trame CTS correspond à celle annoncée par le RTS diminuée de la durée d'émission du CTS et du SIFS correspondant (Durée restante nécessaire à l'échange). Dans la trame ACK, le champ RA est la recopie du champ @2 de la trame précédente (adresse source).

➤ Notion de sécurité dans les réseaux Wi-Fi

Les ondes électromagnétiques se propagent indépendamment de tout support, elles peuvent être reçues par toute station à l'écoute, aussi se prémunir contre les écoutes clandestines est l'une des préoccupations majeures de tout système de transmission sans fil (faisceaux hertziens, téléphonie mobile...). La norme 802.11 prévoit la possibilité de chiffrer les données (**WEP**, *Wired Equivalent Privacy*), mais les nombreuses faiblesses du chiffrement RC4 ont conduit le comité 802.11 à éditer un nouveau standard (802.11i, **WPA**, *Wifi Protected Access*).

17.4.5 Les réseaux IEEE 802.15-1 (Bluetooth)

Généralités

Constituant une évolution du port série, les réseaux Bluetooth[5] ont pour objectif de supprimer toute liaison filaire entre divers équipements : téléphone portable et oreillette, ordinateur et ses périphériques... constituant ainsi un réseau personnel et non plus un réseau d'entreprise (**WPAM**,

5. Bluetooth, littéralement « dent bleue » fait référence au roi danois Harald Blatand II (910-986), qui aurait réussi à réunifier différents royaumes nordiques.

Wireless Personal Area Network). Les réseaux Bluetooth sont donc indépendants de toute infrastructure (réseau « ad-hoc ». Les différents modes d'utilisations visés permettent de limiter la puissance d'émission (faible portée, nombre d'hôtes à accueillir relativement réduit), les réseaux Bluetooth sont donc bien adaptés à un environnement de mobiles (faible consommation d'énergie). Le standard Bluetooth définit trois classes d'émetteur en fonction de la puissance et de la portée (figure 17.58).

Classe	Puissances (mW)	Portée (m)
I	100	100
II	2,5	15-20
III	1	10

Figure 17.58 Puissance et portée des interfaces Bluetooth.

L'organisation du réseau

Les réseaux Bluetooth fonctionnent dans une relation maître/esclave, un terminal Bluetooth, maître, distribue le droit à parole (*polling* des esclaves). L'accès au réseau est du type multiplexage temporel, le temps étant découpé en *slots* de 625 μs (1 600 slots/seconde). Un terminal, dit maître, synchronise le dialogue en distribuant le droit d'accès (*polling*). Le terminal interrogé (« pollé ») peut alors transmettre une trame durant un temps ne pouvant excéder 5 slot*s*. Le réseau formé par le maître et ses esclaves (au maximum 7 esclaves) se nomme un **piconet**. Pour permettre d'étendre les possibilités du réseau un esclave ou un maître d'un piconet peut être esclave dans un autre piconet (***scatternet***). La figure 17.59 représente les différents types de réseau Bluetooth.

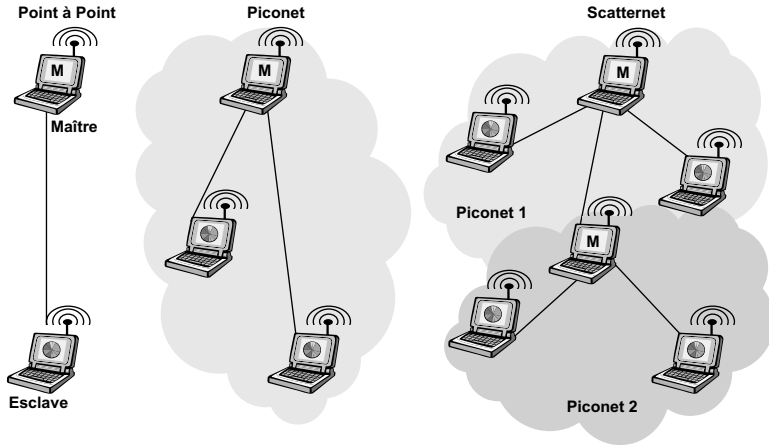


Figure 17.59 Les différents modes de relation d'un réseau Bluetooth.

L'architecture protocolaire

Les services offerts par les réseaux Bluetooth le sont *via* des profils prédéfinis au nombre de 13. Ces services comportent deux services de base : le **GAP** (*Generic Access Profile*) dont le rôle est

© Dunod – La photocopie non autorisée est un délit

de détecter les différents produits Bluetooth à portée radio et le **SDAP** (*Service Discovery Access Profile*) dont le rôle est de déterminer les différents services disponibles sur les matériels compatibles détectés par le GAP. Les services vont déterminer l'empilement protocolaire à utiliser (figure 17.60), citons :

– les services de téléphonie sans fil (*Cordless telephony profile*) ;
– les services de Fax (*Fax profile*) ;
– les périphériques séries (*Serial port profile*) ;
– les connexions à Internet ou aux réseaux locaux (*Dial Up networking profile* et *LAN access profile*) ;
– l'échange de fichiers (*File transfert profile*) et la synchronisation automatique de fichiers projets, agenda (*Synchronisation profile*)...

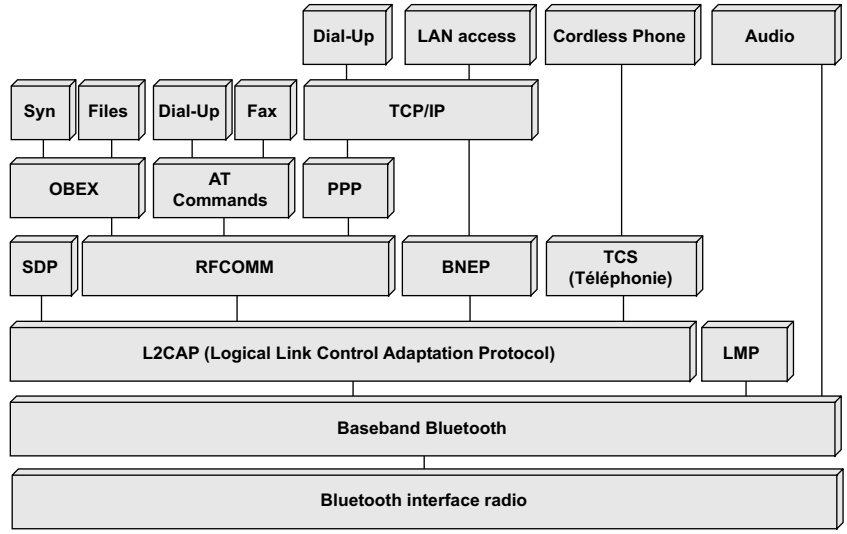


Figure 17.60 L'architecture protocolaire des réseaux Bluetooth.

Les différents services offerts par l'architecture Bluetooth permettent à un type de périphérique de se connecter aux réseaux sans avoir à modifier les applications qui en utilisent les services. Ainsi, par exemple la couche RFCOMM émule une interface V24/V28 (RS232C) pour les périphériques séries, en particulier elle gère les signaux TD, RD, RTS, CTS, DSR, DTR, RI de cette interface d'accès. L'autre couche de base de cette architecture, la couche **L2CAP** (*Logical Link Control Adaptations*) crée et gère les connexions logiques entre applications (canal). Un canal est défini par une source, un ou plusieurs destinataires, un protocole de niveau supérieur et une certaine qualité de service « négociée » à l'ouverture de la connexion. Le protocole **BNEP** (*Bluetooth Network Encapsulation Protocol*) offre aux applications IP une encapsulation plus efficace que celle offerte par RFCOMM.

La couche L2CAP réalise l'adaptation des données issues des applications (64 ko au maximum) à l'interface radio (2 745 bits), en assurant la segmentation/réassemblage et le multiplexage des données, plusieurs applications pouvant se partager la même connexion. Le protocole ***LMP*** *(Link*

Manager Protocol) assure la supervision des différentes connexions, l'authentification des appareils, la mise en veille.

Le protocole **SDP** (*Service Discovery Protocol*) est chargé de la découverte des services offerts par un périphérique et d'en déterminer les caractéristiques. **TCS** (*Telephony Control protocol Specification*) est l'interface téléphonique du modèle Bluetooth, il assure la signalisation téléphonique entre terminaux téléphoniques.

La couche physique

La couche physique correspond à l'interface radio, elle gère trois types de communication :

- Les communications synchrones ou **SCO** (*Synchronous Connection Oriented link*) qui autorisent un débit *full duplex* symétrique de 64 kbit/s avec une certaine garantie de qualité de service. Ce mode de mise en relation est essentiellement destiné au transport de la voix, un terminal esclave ne peut gérer que deux communications simultanées, le maître ne pouvant gérer, en même temps, que trois liens de ce type.
- Les communications asynchrones ou **ACL** (*Asynchronous Connection Less*) qui offrent un débit asymétrique de 723,2 kbit dans le canal descendant et 57,6 kbit/s pour le canal montant. Ce type de liaison permet de réaliser des accès Internet.
- Enfin des communications asynchrones (ACL) symétriques avec un débit de 433,9 kbit/s dans chaque sens.

À l'instar du 802.11, le Bluetooth utilise la bande comprise entre 2,402 et 2,480 GHz divisée en 79 canaux de 1 MHz, seuls 23 canaux sont disponibles en France (figure 17.61). L'utilisation d'une technique d'étalement de spectre à sauts de fréquence (**FHSS**, *Frequency Hopping Spread Spectrum*) augmente la résistance aux interférences et au bruit. Une séquence de sauts de fréquence comprend 79 (23 en France) séquences ou slots de 625 μs soit 1 600 slot/s. Un paquet peut être émis durant 1, 3 ou 5 slots. Un saut de fréquence ne peut être réalisé durant l'émission d'un paquet, une séquence de fréquence peut donc durer 1, 3 ou 5 slots.

Pays	Bande autorisée (GHz)	Canal	Fréquence centrale
États-Unis & Europe	2 400 – 2 483,5	k = 0 ... 78	2 402 + k GHz
Japon	2 471 – 2497	k = 0 ... 22	2 473 + k GHz
France	2 446,5 – 2 483,5	k = 0 ... 22	2 454 + k GHz
Espagne	2 445 – 2 475	k = 0 ... 22	2 449 + k GHz

Figure 17.61 La bande radio des réseaux Bluetooth.

Indépendamment du calcul des sauts de fréquence, le contrôleur Baseband assure le cryptage de bas niveau et gère les différents états du périphérique en mode économie d'énergie :

- *Active*, le périphérique est à l'écoute de tous les *slots*, il peut, sur invitation du maître émettre et recevoir des données.
- *Park*, la station est en veille, elle est connectée au piconet, mais ne participe à aucune communication.

© Dunod – La photocopie non autorisée est un délit

– *Sniff*, à des fins d'économie d'énergie, la station n'est à l'écoute que d'un certain type de *slots* (SCO...).
– *Hold*, la station n'accepte que les trames SCO (communication synchrone), elle refuse les trames ACL.

La couche MAC

La couche MAC gère l'accès au canal radio. Un terminal, dit maître, synchronise le dialogue en distribuant l'accès au support hertzien, le mode d'accès est déterministe. Lorsqu'un terminal rejoint un piconet, avant de communiquer, il doit reconnaître la séquence de sauts de fréquence.

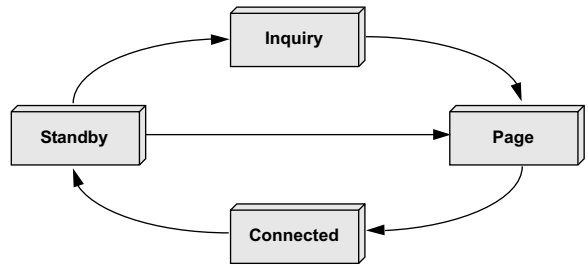


Figure 17.62 Les états d'une station Bluetooth.

Supposons un piconet existant, et une station voulant rejoindre ce dernier (figure 17.62). Avant l'établissement d'une connexion, la station est dans l'état « *Standby* ». Dans cet état, elle se réveille périodiquement (1,28 seconde) et écoute. À réception d'un message *Inquiry_Scan*, la station répond (message FHS), au maître, par un message contenant son adresse et son horloge (état *Inquiry*). Ayant alors identifié une nouvelle station candidate, le maître émet alors des messages « *Page* » à destination de la station. Celle-ci acquitte, immédiatement, par un message *Page_response*, le maître envoie un paquet contenant une adresse de membre du piconet (3 bits), sa propre adresse et son horloge. L'esclave synchronise son horloge sur celle du maître. Le maître et l'esclave passe alors en mode connecté.

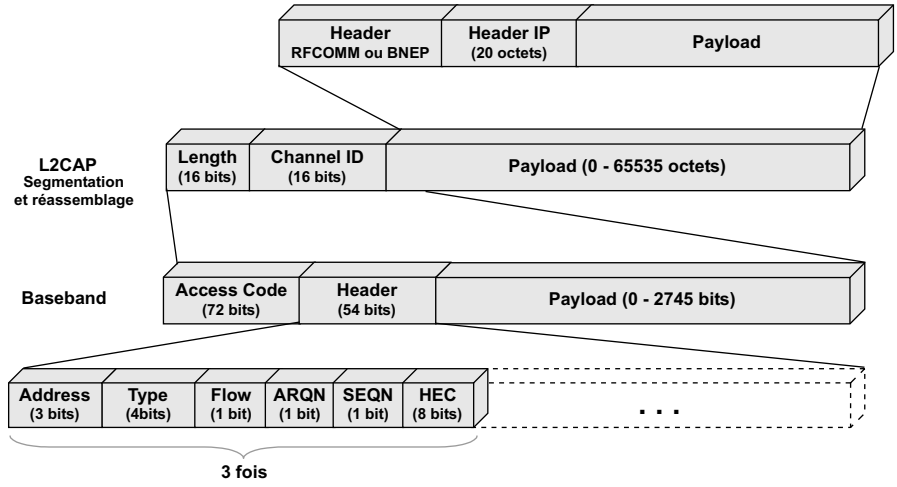


Figure 17.63 Le format des données.

Les données issues de l'application, par exemple IP dans la figure 17.63 sont adaptées à l'interface radio par la couche L2CAP (segmentation). L'en-tête L2CAP indique la longueur totale des données et le canal de communication utilisé. L'en-tête Baseband comporte deux champs. Le premier sur 72 bits comporte un fanion de 4 bits, puis sur 68 bits les informations de synchronisation de la station dont le contenu dépend du type de trame. Suit un champ de 54 bits qui contient la même information répétée trois fois (protection contre les erreurs). Ce champ identifie la station (*Address* attribuée par le maître), le type de message (contrôle ou données) et de communication (synchrone ou asynchrone). Le bit *Flow* permet de réaliser un contrôle de flux (XON-XOFF), Les champs **ARQN** (*Automatic Repeat reQuets Numbers*) servent à l'acquittement des trames alors que le champ **SEQN** (*SEQuence Number*) autorise une numérotation de celles-ci. Enfin le champ **HEC** (*Header Error Check*) permet un contrôle d'erreur de type CRC sur les informations d'en-tête.

L'évolution des normes 802.15

La norme 802.15-1 (Bluetooth) tente de couvrir tous les domaines des réseaux personnels (WPAN). Cependant, elle utilise la même bande de fréquence que le Wi-Fi, le sous-groupe de travail 802.15-2 a défini les mécanismes à mettre en œuvre pour faire cohabiter un réseau Wi-Fi et Bluetooth. Se spécialisant de plus en plus vers des services personnels, la norme 802.15-3 (**UWB**, *Ultra Wide Band*) définit un standard essentiellement orienté diffusion de morceaux musicaux et de séquences vidéos consultables en ligne (*streaming*). Ce nouveau standard accepte jusqu'à 254 connexions et offre un débit total de 55 Mbit/s. Enfin, le standard 802.15-4 (ZigBee) implémente un système bon marché à faible débit (200 kbit/s), portée (10 m) et à très faible consommation d'énergie destiné à des systèmes embarqués légers (badge...) et à des jouets.

17.5 CONCLUSION

L'évolution des réseaux LAN, WLAN et WPAN se déroule en parallèle voire en complémentarité et non en concurrence. C'est surtout dans le domaine de la domotique que les solutions sans fil devraient connaître la plus grande croissance. Bien qu'actuellement les réalisations ne soient pas satisfaisantes en terme de qualité de service, la téléphonie qui n'est qu'un aspect particulier de la mobilité, devrait se développer largement sur ce type de réseaux.

EXERCICES

Exercice 17.1 Distinction CSMA/CD IEEE 802.3 et Ethernet

Comment peut-on distinguer un réseau Ethernet d'un réseau IEEE 802.3 ?

Exercice 17.2 Séquence de synchronisation bit en 802.3 et 802.5

Une séquence de synchronisation bit de 7 octets en 802.3 précède le délimiteur de début de trame, ce n'est pas le cas en 802.5. Justifiez ce choix.

Exercice 17.3 Transmission synchrone et protocole 802.3

Dans les transmissions en mode synchrone, en l'absence d'émission de données, la synchronisation des horloges émission et réception est maintenue par l'émission de fanions. Les réseaux 802.3 10 base 5 (Ethernet sur coaxial épais) émettent les données en mode synchrone et cependant aucun fanion n'est émis entre deux émissions. Pour maintenir la synchronisation des horloges et éviter l'émission d'un préambule de synchronisation important, serait-il possible, en l'absence d'émission de données, de maintenir une activité par l'émission de fanions sur le bus ? Justifier votre réponse.

Exercice 17.4 Rapidité de modulation

Quelle est la rapidité de modulation en bauds d'un réseau local 802.3 (Ethernet) lorsqu'il émet une suite continue de 1 ou de 0 ?

Exercice 17.5 Conception d'un réseau Ethernet à 100 Mbit/s

On veut concevoir un réseau local sur fibre optique, le cahier des charges spécifie :

- distance entre les deux stations les plus éloignées 200 km ;
- nombre maximum de stations connectées 1 000 ;
- vitesse de propagation sur le support 200 000 km/s ;
- débit binaire nominal 100 Mbit/s ;
- longueur maximum d'une trame : 4 500 octets ;
- implémentation du protocole CSMA/CD.

Qu'en pensez-vous ?

Exercice 17.6 Plan d'adressage d'une entreprise

Votre entreprise comporte quatre établissements : Paris, Strasbourg, Brest et Marseille reliés en étoile par des LL (liaisons louées). Compte tenu des informations suivantes, établissez le plan d'adressage de votre entreprise :

– les LL seront adressées en point à point ;
– chaque établissement devra pouvoir distinguer 10 sous-réseaux ;
– chaque sous-réseau pourra éventuellement comprendre plus de 500 machines mais moins de 1 000.

La représentation choisie devra permettre de distinguer très simplement les établissements concernés dans un échange. N'ayant aucun besoin de connexion vers l'extérieur, l'entreprise utilisera des adresses privées de classe A.

Exercice 17.7 Comptabilité des systèmes 802.11b, g et a

Les différentes technologies 802.11 ont été développées dans le respect d'une comptabilité entre les différents systèmes. Qu'en est-il de la compatibilité entre les versions 802.11b, 802.11g, 802.11a ?

Exercice 17.8 Performance des réseaux 802.11

La version 802.11b offre un débit physique maximal de 11 Mbit/s. En admettant que le protocole d'accès utilisé soit le mode DCF, quel est le débit maximal et minimal entre deux stations en mode point à point (réseau ad-hoc de deux stations) ? La figure 17.64 rappelle les différentes valeurs des silences inter-trames.

	FHSS (en μs)	DSSS (en μs)
Time Slot	50	20
SIFS	28	10
PIFS	78	30
DIFS	128	50
EIFS		310
CW_{min}	16	32
CW_{max}	1 024	1 024

Figure 17.64 Les valeurs de silences inter-trames.

On admettra que les données délivrées par l'application sont limitées à 1 500 octets (MTU Ethernet).

Chapitre **18**

Pontage, commutation et VLAN

18.1 PONT OU COMMUTATEUR ?

L'accroissement du trafic dans les réseaux à diffusion conduit à l'effondrement de ceux-ci (collisions). L'augmentation du débit dans les réseaux de type Ethernet ne résout pas le problème, elle en repousse simplement l'apparition. Un concentrateur spécifique qui, contrairement aux hubs, ne diffuserait pas les trames MAC mais assurerait une mise en relation directe du port d'origine de la trame et du port où est raccordée la machine destination résoudrait le problème des collisions. Ce mode de transfert correspond au fonctionnement des commutateurs. Cependant, un commutateur n'achemine ni les messages de *broadcasts* ni ceux de *multicasts* utilisés dans les réseaux locaux. Les ponts (*Bridge*) sont des éléments réseaux capables, à l'instar des commutateurs, d'assurer la mise en relation d'un port d'entrée avec un port de sortie tout en autorisant la diffusion des messages de *broadcast* et de *multicast*. Les commutateurs utilisés dans les réseaux locaux ne sont donc pas des commutateurs au sens strict mais constituent une évolution des techniques de pontage. En fait un commutateur, dans un réseau local (*LAN switch*), n'est qu'un pont utilisant en interne des techniques de commutation pour assurer l'acheminement des trames *unicasts*.

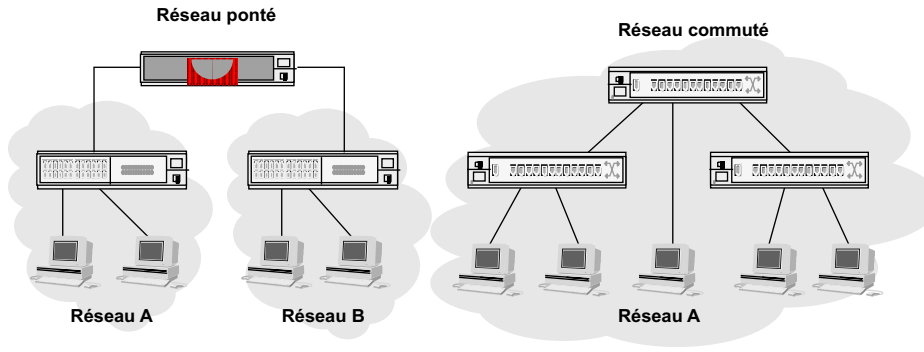


Figure 18.1 Distinction ponts et commutateurs.

Dans les réseaux locaux, la différence essentielle entre un pont et un commutateur réside dans leur utilisation et non dans leur fonctionnalité. Un pont est généralement utilisé pour interconnecter deux ou plusieurs segments d'un réseau local, alors qu'un commutateur ou *LAN switch* peut être utilisé comme un pont mais aussi en lieu et place d'un hub. Dans la représentation de la figure 18.1, le réseau ponté est constitué de deux sous-réseaux *A* et *B*, chacun constituant un domaine de collision spécifique. La diffusion des messages *unicast* n'intéresse que le segment dans lequel la station est insérée, seuls les messages de *broadcast,* d'*unicast* et *multicast* à destination explicite de l'autre segment transitent par le pont, ainsi une collision dans le segment *A* n'est pas vue du segment *B*.

18.2 LES PONTS

18.2.1 Généralités

Les ponts ou *bridges* sont des éléments d'interconnexion de niveau 2. Ils permettent d'interconnecter deux ou plusieurs réseaux (ponts multiports) dont les couches physiques sont dissemblables (figure 18.2). Les ponts sont transparents aux protocoles de niveau supérieur.

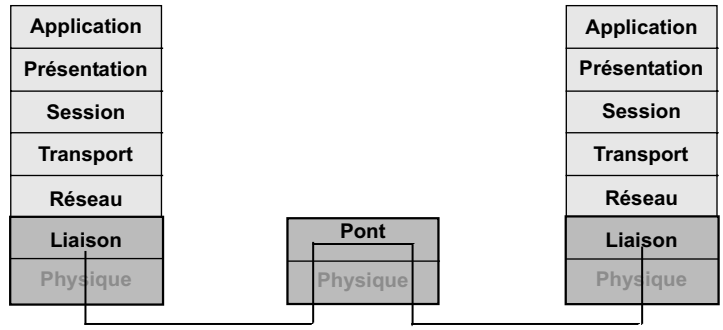


Figure 18.2 Situation des ponts dans le modèle OSI.

Les ponts assurent des fonctions d'adaptation de débit ou de support entre réseaux semblables (Ethernet/Ethernet ou Token Ring/Token Ring) ou dissemblables (Ethernet/Token Ring). Agissant au niveau 2 du modèle de référence, les ponts ont accès à l'adresse MAC. De ce fait, ils peuvent acheminer les trames, en fonction de l'adresse MAC, réalisant ainsi un « routage de niveau 2 » (figure 18.3). Les réseaux ainsi interconnectés constituent un seul réseau logique.

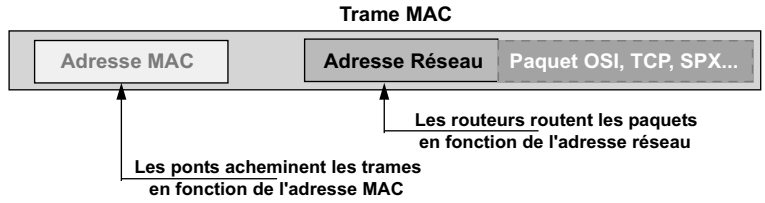


Figure 18.3 Les fonctions de filtrage et d'acheminement des ponts.

18.2.2 Les différents types de ponts

Les ponts sont caractérisés par le mode d'établissement des tables d'acheminement et par la distance qui sépare les réseaux interconnectés. On distingue :

- les ponts simples, sans fonction d'acheminement, qui diffusent toutes les trames reçues sur tous les ports (sauf le port d'arrivée), ces ponts ne sont plus utilisés, ce sont de simples répéteurs multiport qui permettent de prolonger un réseau ;
- les ponts simples, avec fonction d'acheminement, ces derniers dirigent les trames selon une table d'acheminement (correspondance adresse MAC/port) introduite par l'administrateur à la configuration du pont (pontage statique) ;
- les ponts transparents (**TB**, *Transparent Bridge*) ou ponts à apprentissage (*Learning bridge*), ces ponts construisent dynamiquement une table d'acheminement et la maintiennent à jour ;
- les ponts à routage par la source, ou routage contrôlé par l'émetteur (*Source routing*), dans ces ponts, la route suivie par la trame est inscrite dans la trame elle-même. Préalablement à l'envoi de données, la source émet une trame de découverte de route vers le destinataire, cette route est mémorisée puis indiquée dans tout message vers cette même destination. D'origine IBM, le routage par la source est utilisé dans l'interconnexion des réseaux Token Ring et FDDI ;
- enfin, on distingue les ponts locaux des ponts distants (*Remote bridge*). Les ponts distants interconnectent des réseaux locaux *via* une liaison spécialisée ou un réseau de transport (figure 18.4). Ils doivent assurer des fonctions d'adaptation de protocole entre le protocole local et le protocole du lien d'interconnexion (X.25, Frame Relay, ATM, PPP...). Ces ponts sont généralement désignés sous le terme de pont à encapsulation et utilisés pour interconnecter des réseaux dont le protocole réseau n'est pas routable (Netbios, SNA...).

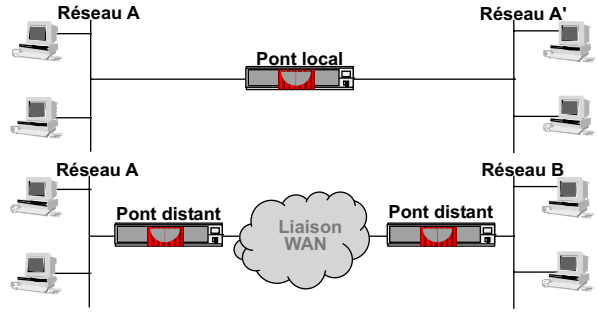


Figure 18.4 Pont local et pont distant

18.2.3 Les ponts transparents

Les ponts et les commutateurs établissent dynamiquement, par écoute du trafic sur chacun de leurs ports, une table d'acheminement (**FDB**, *Forwarding Data Base*). La FDB mémorise le couple port de réception/adresse MAC source (figure 18.5).

Pour construire cette table, les ponts examinent le trafic reçu par chacun de ses ports. La table d'acheminement (**FDB**, *Forwarding Data Base*) est construite par examen des adresses MAC sources. En associant l'adresse MAC source de la trame au port par lequel elle y est entrée, le

© Dunod – La photocopie non autorisée est un délit

commutateur apprend la localisation géographique des stations. À réception d'une trame, le pont (commutateur) consulte la table d'acheminement (table de commutation) et achemine la trame reçue sur le seul port où est localisé le destinataire. Les trames à destination d'une adresse non inscrite dans la table et celles de diffusion (*Broadcast*) sont répétées sur tous les ports, sauf le port de réception.

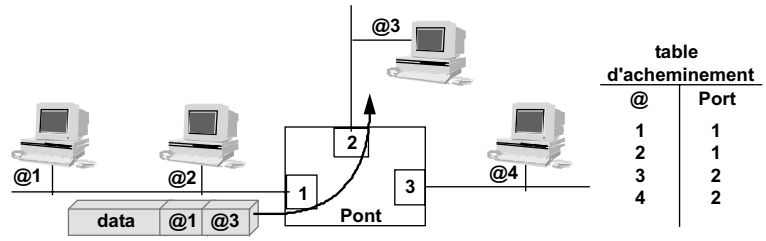


Figure 18.5 Principe d'acheminement des ponts.

Les tables ne peuvent posséder autant d'entrées que de stations connectées. Aussi, périodiquement, les adresses les plus anciennes sont effacées. À cet effet, on associe, à chaque entrée de la table, un temporisateur. Ce temporisateur est réinitialisé à chaque réception d'une trame de même origine. À échéance du *timer*, l'entrée est effacée. Ce procédé autorise la mobilité et évite l'engorgement des tables. Par défaut, la valeur de la temporisation est fixée à 5 min, elle est paramétrable de 10 s à 11 jours. En principe une table peut contenir jusqu'à 1 024 entrées, ce nombre correspond au nombre maximal de stations actives sur un réseau Ethernet.

La table peut être modifiée par l'administrateur, il est alors possible de réaliser des filtres (filtrage statique). En associant des adresses sans limite d'âge à un port, on interdit la mobilité des stations. On peut de même, en fonction d'une adresse source ou destination, interdire l'acheminement vers tel ou tel port. La figure 18.6 illustre le traitement réalisé par un pont (commutateur) lors de la réception d'une trame.

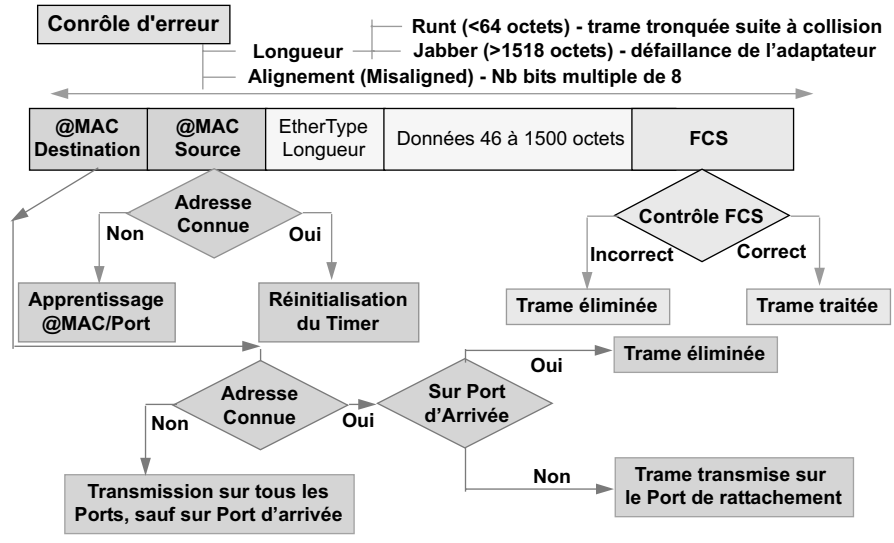


Figure 18.6 Le traitement des trames 802.3 dans un pont.

La fonction d'acheminement des ponts (commutateurs) permet d'isoler chaque brin du trafic existant sur un autre brin. Cette faculté, associée à la non-retransmission des trames erronées (erreurs de FCS[1], trame incomplète...), permet, dans les réseaux de type Ethernet, de découper un réseau physique en plusieurs sous-réseaux logiques, dits domaines de collision. Une collision sur un brin est invisible sur un autre. L'architecture adoptée est généralement du type *backbone* (réseau fédérateur). Dans le modèle d'architecture d'interconnexion représentée en figure 18.7, seul le trafic interdépartemental transite sur le réseau *backbone*.

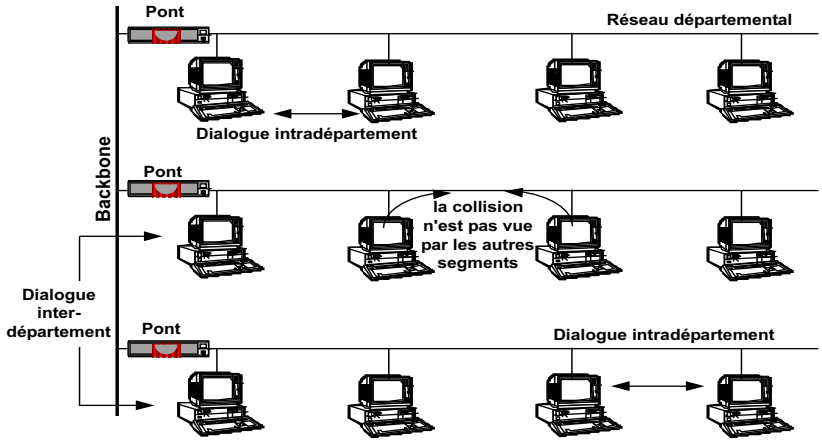


Figure 18.7 L'architecture d'un réseau backbone.

Le pont est dit transparent car il ne fait que recopier la trame sur le port destination sans en modifier l'adresse source. Il n'a donc, en principe, nul besoin d'une adresse MAC. Cependant, pour des raisons d'administration, à chaque interface MAC du pont est associée une adresse MAC.

18.2.4 Le *Spanning Tree Protocol* (STP) ou arbre recouvrant

Généralités

Les facultés d'auto-configuration des ponts transparents en ont fait l'un des éléments majeurs de l'interconnexion locale des grands réseaux. La sécurisation de ces réseaux a fait apparaître la nécessité de duplexer les organes d'interconnexion (figure 18.8).

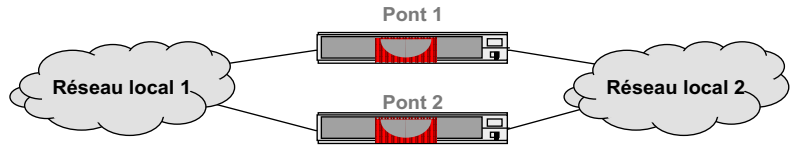


Figure 18.8 L'interconnexion redondante.

1. C'est uniquement la fonction de contrôle d'erreur réalisée par les ponts et en principe non réalisée par les commutateurs qui distingue ces deux éléments.

© Dunod – La photocopie non autorisée est un délit

Cependant, la mise en parallèle de ponts transparents volontaire, par mesure de sécurité, ou par erreur, dans un réseau complexe, engendre un phénomène de bouclage qui conduit à l'effondrement du réseau. Ce phénomène est illustré par la figure 18.9.

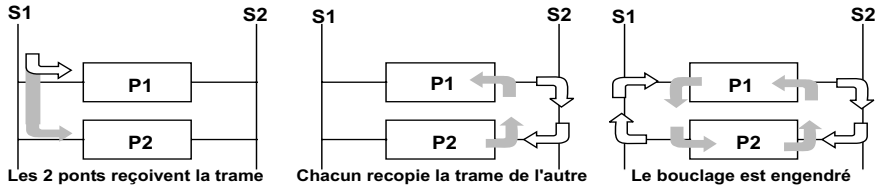


Figure 18.9 Bouclage des trames sur des ponts en parallèle.

La trame émise sur le segment S1 à destination d'une station non encore enregistrée dans les ponts est reçue par les deux ponts (P1 et P2), elle est retransmise sur le segment S2, la trame émise par le pont 1 sur le segment 2 est reçue par le pont 2, tandis que celle émise par le pont 2 est recopiée par le pont 1. Chacun recopie alors la trame sur le segment 1... Une situation de boucle est engendrée. Développé à l'origine par DEC et normalisé par l'IEEE (IEEE 802.1D), l'algorithme du *spanning tree* (**STP**, *Spanning Tree Protocol*) ou « arbre recouvrant » est un protocole d'apprentissage de la topologie du réseau dont le but est :

– d'éliminer les boucles en désactivant les ports des ponts qui engendrent ces boucles ;
– de contrôler en permanence la disponibilité des ponts actifs ;
– et, en cas de défaillance d'un pont actif, de basculer le trafic sur le pont mis en sommeil.

Le principe en est relativement simple, il s'agit de construire un graphe en arbre. À partir d'un pont élu, désigné pont racine (*Bridge root*), l'algorithme du *spanning tree* détermine le chemin le plus court en éliminant les risques de bouclage. Les ponts en boucle sont déclarés ponts *backup* et, tant que le pont actif est en fonction, ils sont mis en sommeil (figure 18.10).

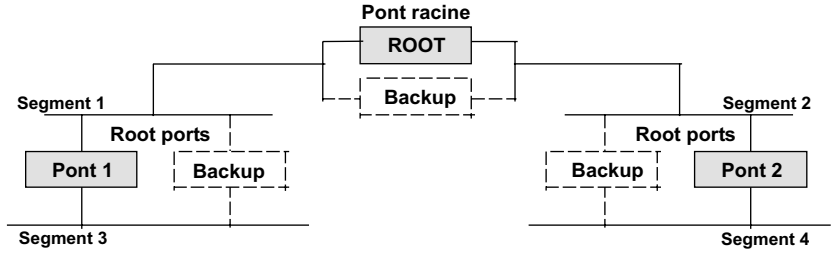


Figure 18.10 Exemple de configuration du Spanning Tree Protocol.

L'algorithme du spanning tree

Pour construire l'arbre recouvrant (*Spanning tree*), les ponts s'échangent des messages de diffusion (**BPDU**, *Bridge Protocol Data Unit*). Le *spanning tree* utilise deux types de message, les messages de configuration (figure 18.11) et les messages d'indication de changement de topologie.

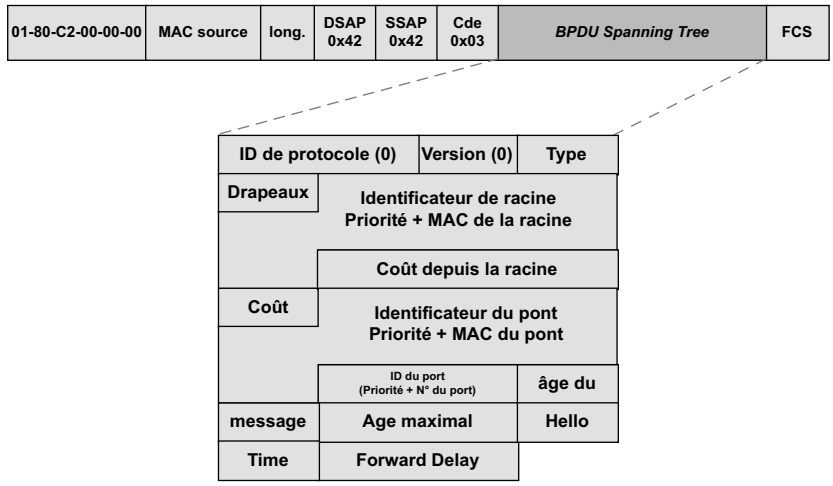


Figure 18.11 La BPDU de configuration.

Le message de configuration (BPDU de configuration) utilise l'encapsulation IEEE 802.2 LLC1 (*Logical Link Control* mode datagramme) avec un SAP de 0x42 et une adresse MAC destination de diffusion 01-80-C2-00-00-00. Les champs identification du protocole, *Type* sur 2 octets, et *Version* (1 octet), non utilisés, doivent toujours être mis à 0. Le champ suivant sur 1 octet distingue un message de configuration (0), d'un message d'information de topologie (128).

Chaque pont possède un identificateur (**ID**, *bridge IDentifier*) construit à partir d'un indicateur de priorité (2 octets de poids fort du champ) et de l'adresse MAC du pont. L'adresse MAC du pont est celle de son port de plus faible adresse. Le champ priorité est fixé à 0x8000 par défaut. Sa valeur peut être modifiée par l'administrateur (0 à 0xFFFF). Plus ce nombre est faible, plus la priorité est élevée. Le pont racine élu est le pont de plus petit ID, à priorité égale, c'est celui de plus petite adresse MAC. Au démarrage, chaque pont émet une BPDU le signalant comme pont racine. Tout pont qui reçoit une BPDU avec un ID inférieur au sien, cesse ses émissions et rediffuse les trames reçues. À la fin du processus, seul le pont racine continue à émettre son identifiant. Il est élu pont racine.

Le port par lequel un pont reçoit en premier la trame d'identification du pont racine est appelé « *root port* ». Pour déterminer l'arbre minimal, chaque pont se voit affecter, par l'administrateur, un coût. Le pont racine émet une trame de diffusion avec un coût nul, chaque pont répète cette trame en incrémentant le coût du sien (*Root path cost*). Un pont qui reçoit, sur un port « non racine », une trame dont le coût, depuis la racine, est inférieur au coût des trames qu'il émet, en déduit qu'il existe, depuis la racine, une route de moindre coût. Il se met alors en sommeil (pont *backup*). En cas d'égalité entre deux ponts, c'est le pont de plus petit ID qui est élu. L'éventuel pont en boucle sur la racine détermine qu'il est pont *backup* simplement parce qu'il reçoit des trames identiques sur ses deux ports et que son ID est supérieur à celui de la trame reçue. En principe, le coût de traversée des ponts est le même pour tous, la valeur recommandée était « 1 000/Débit en Mbit/s ». L'accroissement des débits a rendu cette valeur obsolète, la recommandation IEEE 802.1p fixe de nouvelles valeurs (figure 18.12). Il est, aussi, possible, en jouant sur les valeurs du niveau de priorité et de coût, de privilégier un chemin par rapport à un autre.

© Dunod – La photocopie non autorisée est un délit

Débit du réseau	Valeurs recommandées	Plages admises
Réseaux IEEE 802.3		
10 Mbit/s	100	50-600
100 Mbit/s	19	10-60
1 Gigabit/s	4	3-10
10 Gigabit/s	2	1-5
Réseaux IEEE 802.5		
4 Mbit/s	250	100-1000
16 Mbit/s	62	40-400
100 Mbit/s	19	10-60

Figure 18.12 Valeurs des coûts recommandées par l'IEEE.

Périodiquement une trame de diffusion est émise (paramètre *Hello Time* valeur par défaut de 2 s, valeur recommandée 20 s). Si un pont *backup* reste plus de cet intervalle de temps sans rien recevoir, il en déduit que le pont, dont il est le *backup*, est défaillant. Il émet alors une trame de configuration. Cette diffusion de BPDU, sur un lien WAN, peut consommer une partie importante de la bande passante. Aussi, lorsque les réseaux sont interconnectés *via* des liens WAN à faible bande passante, il est recommandé de ne pas mettre en service le *spanning tree*.

Les ponts transparents peuvent être dans cinq états :

– l'état *Disabled*, dans cet état le pont ne participe à aucune activité, il est inerte ;
– l'état *Listening* qui correspond à la phase de configuration et de construction de l'arbre recouvrant. Dans cet état, le pont n'accepte, ni ne retransmet les trames utilisateurs ;
– l'état *Learning*, c'est la phase d'apprentissage, le pont met à jour sa base de données d'acheminement. Dans cet état, le pont ne participe toujours pas à la retransmission des trames ;
– l'état *Forwarning*, c'est l'état de fonctionnement normal d'un pont, il participe alors à l'acheminement des trames sur le réseau ;
– enfin, l'état *Blocking*, dans cet état le pont est en sommeil, il n'achemine aucune trame mais participe aux opérations du *spanning tree* et d'administration des ponts.

Conclusion

L'algorithme du *Spanning Tree Protocol* utilise une adresse de diffusion. En cas de système multiconstructeur, il est important de vérifier que les adresses de diffusion sont identiques (figure 18.13).

	Ethernet	Token Ring, FDDI
IEEE	01-80-C2-00-00-00	80-01-43-00-00-00
IBM	03-00-00-00-80-00	C0-00-00-00-01-00
DEC	09-00-2B-01-00-00	90-00-D4-80-00-00
Retix	09-00-77-00-00-01	90-00-EE-00-00-80
Spider Systems	09-00-39-00-70-00	90-00-9C-00-0E-00
Ungerman-Bass	01-DD-01-00-00-00	80-BB-80-00-00-00

Figure 18.13 Les adresses de diffusion du spanning tree.

Les informations de coût et d'ID peuvent être initialisées par le constructeur. Dans ce cas, l'administrateur ne maîtrise ni le pont racine ni la topologie. Un pont racine mal déterminé peut constituer

un véritable goulet d'étranglement. En effet, chaque pont retransmet le trafic vers le port racine ainsi de suite jusqu'à ce qu'il atteigne sa destination. Si le destinataire n'est pas localisé dans la branche montante, le pont racine reçoit tout le trafic.

Le *spanning tree* définit des routes statiques qui ne prennent pas en compte le trafic réel sur les branches du réseau. Considérons le réseau représenté figure 18.14. Compte tenu des coûts indiqués (C), le pont P3 est en sommeil. Si le trafic entre le segment R1 et R2 est important, le délai de retransmission des trames du segment R1 vers le segment R3 peut être prohibitif. Il eut été plus intéressant de configurer le réseau pour que le pont *backup* soit le pont P2, sauf si le trafic P1, P2 est important ! Le routage par la source (**SR**, *Source Routing*), étudié ci-après, autre mode d'acheminement dans les réseaux pontés, remédie à cet inconvénient, il détermine la route optimale dans le réseau en fonction de critères prédéfinis (charge, délai...).

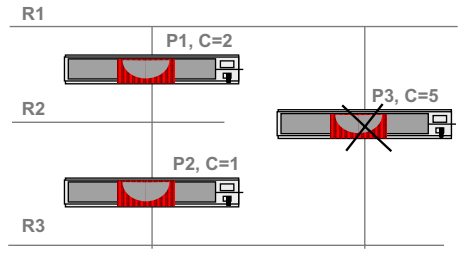


Figure 18.14 La topologie du réseau et spanning tree.

18.2.5 Les ponts à routage par la source

Généralités

D'origine IBM, le routage par la source (**SR**) est un mode de fonctionnement spécifique des ponts dans l'environnement Token Ring. Dans le SR, les ponts n'entretiennent aucune table d'acheminement. Ils se contentent de router les trames selon les indications contenues dans le champ d'information de routage (**RI**, *Routing Information*) de la trame Token Ring. Le *spanning tree* et le *source routing* ne sont pas incompatibles, la plupart des ponts dans l'environnement Token Ring utilisent les deux algorithmes.

La présence d'un champ RI est indiquée par le bit *multicast* du champ Adresse source de la trame MAC (à 0, pas de champ RI à 1, présence du champ RI). Il contient la liste des ponts à traverser pour joindre le destinataire. La trame MAC 802.5, modifiée, est représentée figure 18.15. Dans le *source routing*, ce sont les stations et non les ponts qui entretiennent les tables d'acheminement. Ces tables peuvent être statiques (initialisées par l'administrateur) ou dynamiques (construites par la station).

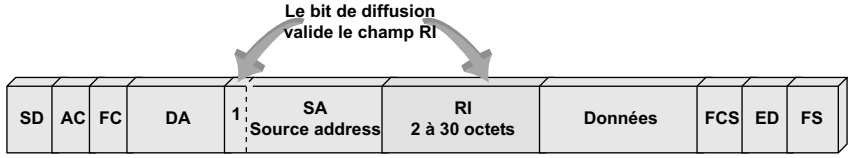


Figure 18.15 La trame MAC 802.5 validant le champ RI.

© Dunod – La photocopie non autorisée est un délit

Principe

Lorsqu'une station désire envoyer un message, elle consulte sa table d'acheminement (association d'une adresse MAC et d'une route à suivre). Si l'adresse MAC destination n'y est pas enregistrée, elle diffuse sur le réseau une trame de découverte.

Lorsqu'un pont reçoit une trame de découverte, il y enregistre son identifiant (*Route designator*) et, si sa MTU est plus petite que la MTU enregistrée, met à jour ce champ, enfin, il diffuse la trame sur tous ses ports, sauf le port d'arrivée. Le destinataire reçoit ainsi de nombreuses trames de découverte (fonctionnement dit **ARE**, *All Route Explorer*). Il ne renvoie à la source que la première arrivée (meilleur chemin) en inversant le bit sens. Le fonctionnement du *source routing* est illustré figure 18.16.

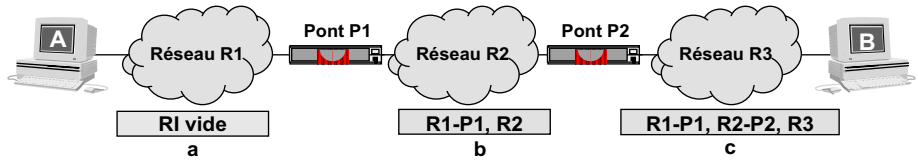


Figure 18.16 L'enregistrement de route.

La station *A*, ignorant le chemin pour joindre *B*, diffuse une trame de découverte avec le champ RI vide (trame « a » de la figure 18.16). Le pont P1, à réception de cette trame, la renseigne de l'identifiant du réseau dont est issue la trame (R1), de sa propre identification (P1) et de celle du réseau sur lequel il retransmet la trame (R2), la trame contient alors les informations représentées par la trame « b ». Notons qu'il spécifie la MTU du réseau 2 et recalcule le FCS. Le pont P2 reçoit cette trame, le champ RI étant renseigné, il examine si son identifiant figure dans le champ de routage, auquel cas il détruit la trame (il l'a déjà vue). Dans le cas contraire, il renseigne la trame de son identifiant (P2) et de celui du réseau de réémission (R3). Si la valeur du champ MTU est supérieure à celle qu'il admet, il met à jour le champ MTU. La nouvelle trame est représentée en « c ». La station *B* reçoit la trame, elle apprend ainsi le chemin pour joindre *A* (*bit sens*) et accuse réception de celle-ci. À la réception de l'accusé, *A* connaît le chemin pour joindre *B*.

Le champ RI (figure 18.17), d'un maximum de 30 octets, contient les informations de :

- *type de trame*, sur 3 bits ce champ identifie, selon sa valeur, la nature de la trame :
  - 001, trame d'information à router selon les informations contenues dans le champ RI,
  - 010, trame d'apprentissage **ARE** (*All Route Explorer*), cette trame est diffusée par une station qui désire connaître le chemin pour joindre une autre station et par tout pont qui la reçoit (multiples trames sur le réseau),
  - 100, trame d'apprentissage **STE** (*Spanning Tree Explorer*), mode de découverte qui réduit le trafic engendré par le fonctionnement ARE. La trame de découverte n'emprunte que les branches établies précédemment par le *Spanning Tree Protocol*.
- *longueur*, ce champ, de 5 bits, spécifie, en octets, la longueur du champ RI (de 2 à 30 octets maximum),
- *sens*, ce bit (S) indique si la route à suivre doit être lue de gauche à droite (S=0, la route à suivre suit l'ordre des indications du champ RI) ou de droite à gauche (S=1, la route à suivre suit l'ordre inverse des LAN du champ RI),

– **MTU** (*Maximum Transfert Unit*), ce champ de 6 bits indique la taille maximale des unités de données qui peuvent être transférées sur le réseau traversé, les valeurs sont codifiées (516, 1500, 2052, 4472, 8144, 11407, 17820, 65535),
– le champ **NCFI** (*Non Canonical Format Indentifier*), ce bit introduit par la recommandation IEEE 802.1Q indique le format d'écriture des adresses MAC dans la trame (0 format non canonique, 1 format canonique),
– enfin, le champ Route qui contient *n* sous-champs *Route designator*. Ce champ identifie, sur 12 bits, le réseau (LAN ID) et sur 4 bits le pont traversé, à la fois en réception et en émission. Les identificateurs sont initialisés par l'administrateur de réseau.

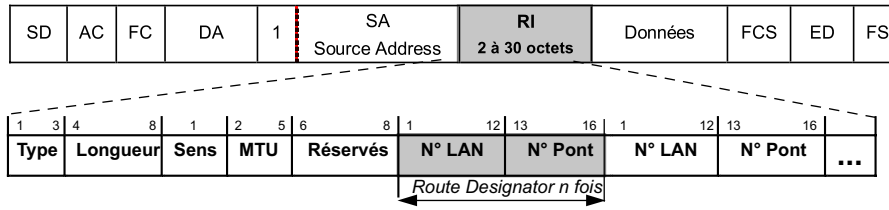


Figure 18.17 La structure du champ RI.

*Les ponts SRT (*Source Routing Transparent*)*

Pour les environnements hétérogènes, l'IEEE a spécifié (IEEE 802.1) un pont pouvant fonctionner à la fois comme pont transparent et comme pont à routage par la source.

Lorsqu'une trame est reçue par un pont, celui-ci examine le bit de *multicast* du champ Adresse MAC source. Si ce bit est positionné, la trame est diffusée selon les informations d'acheminement du champ RI, sinon elle est émise selon l'arbre défini par le *Spanning Tree Protocol.*

Ces ponts permettent de réaliser des interconnexions dans des environnements imparfaitement connus sans se soucier d'éventuels bouclages.

18.2.6 Le pontage par translation

Le pontage par translation permet de réaliser des opérations de pontage entre réseaux différents. En principe, l'architecture d'un pont IEEE 802.3/Token Ring ou 802.3/FDDI ou encore FDDI/Token Ring (figure 18.18) ne devrait pas poser de problème, le niveau d'hétérogénéité étant le niveau MAC, le pont remonte jusqu'au niveau « trame LLC » (pont LLC).

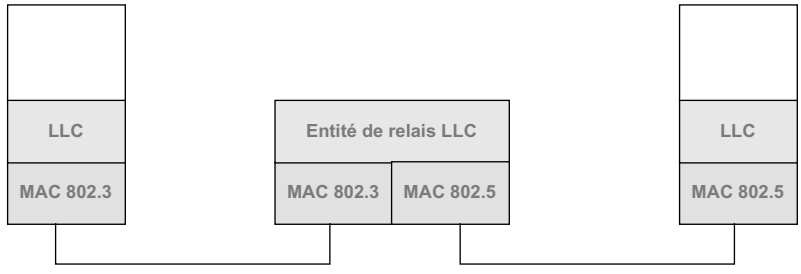


Figure 18.18 Principe de l'architecture d'un pont à translation.

© Dunod – La photocopie non autorisée est un délit

Cette approche est toute théorique, en effet, les réseaux du type Ethernet n'utilisent pas l'encapsulation LLC, le pont devra alors générer le format LLC et éventuellement l'encapsulation SNAP. Mais, la véritable difficulté réside dans la différence de taille des trames de chacun des deux réseaux. Ethernet a une taille de trame limitée à 1 500 octets, lorsqu'une trame Token Ring ou FDDI de taille supérieure doit lui être envoyée, celle-ci est soit abandonnée, soit fragmentée. Dans le premier cas le pont n'est pas fiable, dans le second il ne peut plus être considéré comme un pont, puisque la fragmentation n'est introduite qu'au niveau 3 du modèle de référence (modèle OSI). En pratique, les deux solutions existent. Il est aussi possible de limiter la taille des trames Token Ring et FDDI en ajustant le temps de possession du jeton.

Compte tenu de la complexité de tels ponts, il est préférable, pour réaliser l'interconnexion de réseaux différents, d'utiliser un routeur.

18.3 LA COMMUTATION DANS LES LAN

18.3.1 Principe de base

Issue de la téléphonie et des réseaux grande distance (**WAN**), puis mis en œuvre dans le monde Ethernet (*Switched Ethernet*) pour résoudre les problèmes d'effondrement des réseaux (collisions) et garantir une certaine bande passante, la technique de commutation est aujourd'hui largement utilisée pour réaliser tout type de réseaux. Traditionnellement, la commutation consiste, en fonction d'un identifiant (label), à mettre en relation directe un port d'entrée avec un port de sortie, la relation étant établie préalablement à toute communication par un protocole de signalisation (table de commutation).

La commutation dans les réseaux locaux n'ouvre pas explicitement un circuit virtuel. À l'instar des ponts dont ils ne sont, rappelons-le, qu'une adaptation (ponts multiport), les commutateurs établissent dynamiquement (commutation dynamique) une table de localisation ou d'acheminement (figure 18.19).

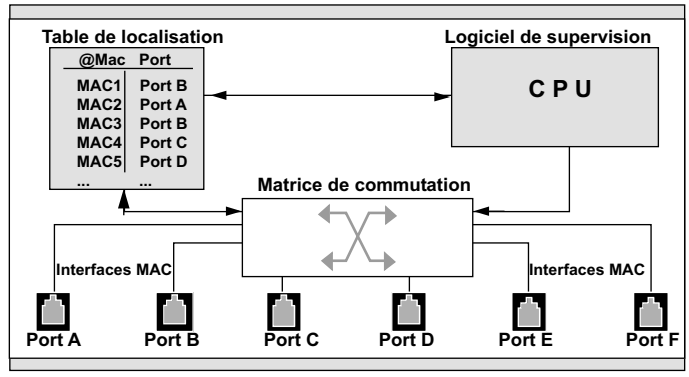
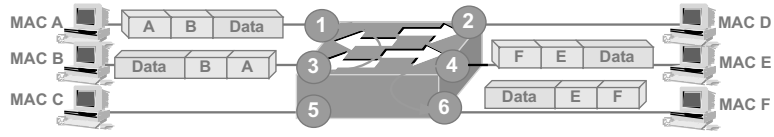


Figure 18.19 Principe d'un commutateur.

Pour construire sa table d'acheminement (**FDB**, *Forwarding Data Base*), le commutateur examine le trafic reçu par chacun de ses ports et associe au port l'adresse MAC source de la trame reçue. Le commutateur apprend ainsi la localisation géographique des stations. À réception d'une

trame, le commutateur consulte la table d'acheminement (table de commutation) et achemine la trame reçue sur le seul port où est localisé le destinataire autorisant ainsi un acheminement en simultané de plusieurs trames (figure 18.20).



@MAC	PORT	AGE
A	1	
B	3	
C	5	
D	2	
E	4	
F	6	

Figure 18.20 La commutation autorise le parallélisme des communications.

Les trames à destination d'une adresse non inscrite dans la table et celles de diffusion sont répétées sur tous les ports, sauf le port de réception. Les tables ne pouvant posséder autant d'entrées que de stations connectées, périodiquement, les adresses les plus anciennes sont effacées. À cet effet, à chaque entrée de la table, est associé un temporisateur réinitialisé à chaque réception d'une trame de même origine.

18.3.2 Notion d'architecture des commutateurs

Historiquement, dans les premiers commutateurs spatiaux, des relais électromagnétiques mettaient en relation un circuit d'entrée avec un circuit de sortie (commutateur *crossbar*), par la suite, les relais furent remplacés par des semi-conducteurs (transistors). Le principe des commutateurs *crossbar* est représenté figure 18.21, à chaque croisement, un transistor établit ou rompt la liaison entre les deux conducteurs. Les points « noirs » de la figure schématisent l'état passant des transistors et donc la relation entre les conducteurs, les points « clairs » représentent l'état bloqué du transistor et donc la coupure entre les deux circuits.

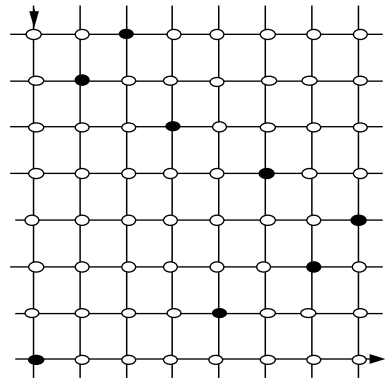


Figure 18.21 Principe d'une matrice de type crossbar.

© Dunod – La photocopie non autorisée est un délit

Autorisant le parallélisme dans le traitement des trames, les commutateurs de type *crossbar* sont très efficaces mais aussi très complexes ; le nombre de points de connexion évolue en N^2 où N représente le nombre de ports. Une solution à cette complexité est fournie par les commutateurs multi-étage dont la réalisation la plus courante est le commutateur Banyan. Les commutateurs du type Banyan ne comportent que $N \cdot LogN$ composants. La figure 18.22 illustre le principe de mise en relation d'un port d'entrée avec n'importe quel port de sortie. Chaque port d'entrée de ce système peut être mis en relation avec tout port de sortie.

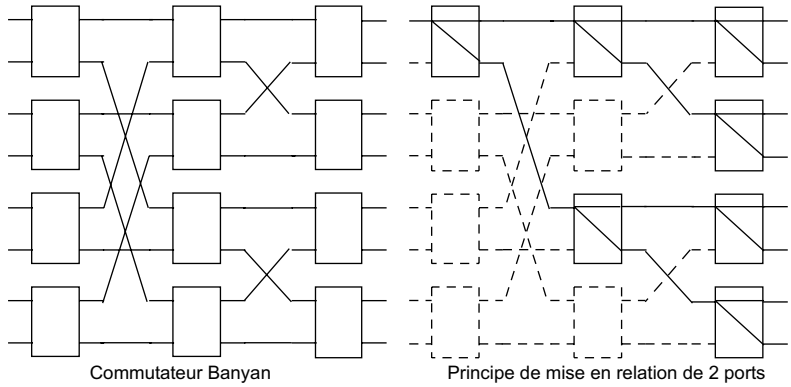


Figure 18.22 Principe d'un commutateur de type Banyan.

Ces architectures répondent mal au problème de la diffusion. Aussi, des architectures, certes peut-être moins efficaces que celles du type Banyan mais beaucoup simples, ont la faveur des constructeurs. Ce sont les architectures à bus et à mémoire partagée. La première correspond à la réalisation d'un réseau très haut débit (*Collapsed backbone*), le débit du bus devant être au moins égal à la demi-somme des débits incidents. La seconde solution, la plus courante, est celle de la mémoire partagée à accès multiples simultanés. Toutes les trames sont recopiées en mémoire centrale avant d'être commutées. Ce dernier type d'architecture permet de résoudre simplement les mécanismes de blocage.

Un commutateur peut mettre en relation n'importe quel port d'entrée avec n'importe quel port de sortie. Si simultanément, plusieurs flux d'entrée doivent converger vers un même port de sortie, il peut y avoir dépassement des capacités d'émission du port de sortie et pertes de données. Afin d'éviter ces pertes, le système est doté de *buffers* d'attente. Les commutateurs peuvent disposer exclusivement de *buffers* d'entrée ou de sortie. En cas de conflit d'accès à un port de sortie, si le système ne possède que des *buffers* en entrée, il peut se produire un blocage en sortie (perte de données). Si le système n'est doté que de *buffers* de sortie, on ne peut exclure un blocage en entrée que si les *buffers* de sortie sont suffisamment dimensionnés pour admettre une convergence de tous les flux d'entrée vers un unique port de sortie. Cette solution conduit à la réalisation de *buffers* de grande taille. Dans ces conditions, les constructeurs adoptent généralement une solution mixte : *buffers* en entrée et *buffers* en sortie (figure 18.23).

Enfin, quelle que soit la taille des *buffers*, la perte de trames par débordement n'est pas à exclure. Aussi, les commutateurs mettent-ils en œuvre un contrôle de flux de type *Xon*/*Xoff* par l'intermédiaire de la trame « Pause » décrite au chapitre précédent (§ 17.3.6, figure 17.22).

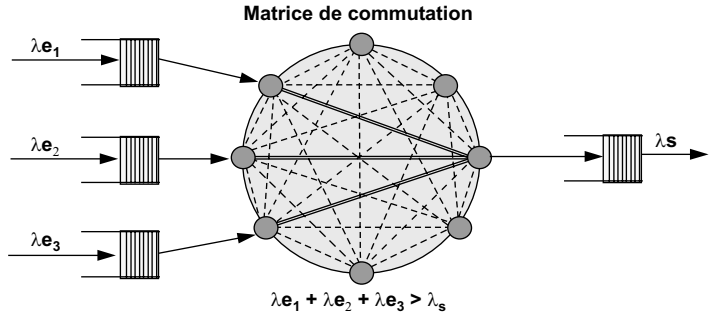


Figure 18.23 Congestion dans les commutateurs.

18.3.3 Les différentes techniques de commutation

La commutation améliore la gestion de la bande passante en ne mettant en relation que les ports intéressés par la communication. L'acheminement s'effectue au niveau MAC, ce qui autorise des performances élevées. Deux techniques de base sont mises en œuvre. Les premiers commutateurs (commutateurs Kalpana) relayaient la trame vers le port destination dès la lecture de l'adresse. Cette technique : lecture de l'adresse au vol et commutation rapide (*Fast forward* ou C*ut through*) est très performante mais propage les trames sans en avoir vérifié la validité et en particulier les trames corrompues par une collision. Ce mode de fonctionnement distingue les commutateurs des ponts, les ponts ne propageant les trames qu'après en avoir vérifié l'intégrité, d'où l'appellation de commutateur et non de pont. Cependant, les trames de collision sont identifiables, leur longueur est inférieure à la fenêtre de collision. Aussi, pour éviter la propagation des collisions, certains commutateurs ne retransmettent les trames qu'après avoir reçu 64 octets. Réémettant les trames avant d'en avoir reçu l'intégralité, ce mode de fonctionnement interdit l'adaptation des débits.

L'accroissement des performances des mécanismes de commutation a autorisé un retour au mode initial de fonctionnement des ponts. Les trames reçues sont intégralement lues avant retransmissison (*Store and forward*), ce qui autorise un contrôle d'erreur, ne sont alors retransmises que les trames non erronées et la conversion éventuelle de débit (port *auto sense*).

La première technique est plus performante en terme de nombre de trames commutées par seconde (faible temps de latence). Cependant, elle propage les trames erronées et en particulier les trames ayant subi une collision. L'*adaptative error free* combine les deux techniques. Initialement le commutateur démarre en mode *Cut through*, et si le taux d'erreur atteint un seuil prédéterminé, le commutateur bascule en mode *store and forward.*Rappelons, qu'en mode *cut through* il n'y a pas de mémorisation des données, il ne peut donc y avoir adaptation de débit entre le débit du port d'entrée et celui de sortie.

18.3.4 Les différents modes de commutation

La configuration du système peut être statique (les tables de commutation sont introduites par l'administrateur) ou dynamique (les tables de commutation sont construites par analyse de trafic et apprentissage des adresses MAC). Le commutateur peut mettre en relation des stations (commutation par port) ou des segments de réseaux (commutation de segment). La figure 18.24 illustre ces différents types.

© Dunod – La photocopie non autorisée est un délit

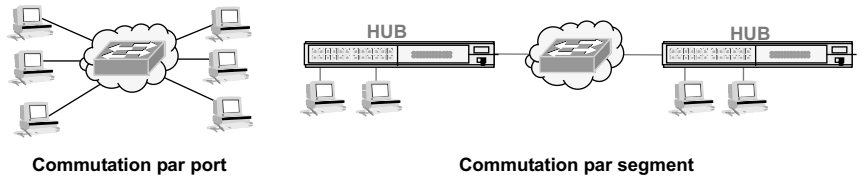


Figure 18.24 Les différents modes de commutation.

La combinaison des différentes techniques conduit à considérer quatre modes de commutation :

– la commutation statique par port permet de résoudre essentiellement les problèmes liés aux modifications fréquentes de réseau (brassage électronique depuis une console d'administration) ;
– la commutation statique par segment autorise la réalisation de différents réseaux interconnectés (segments), cette technique préserve la bande passante lors de l'accroissement des réseaux ;
– la commutation dynamique par port garantit à chaque station un débit maximal, son utilisation est préconisée pour les applications gourmandes en bande passante, elle permet les transferts isochrones entre stations Ethernet. La commutation dynamique par port assimile le commutateur à un hub ;
– la commutation dynamique par segment permet, dans une infrastructure existante (réseaux d'étage), de garantir à chaque sous-réseau (segment) un accès sécurisé, au débit nominal du raccordement, à un ou plusieurs serveurs collectifs (applications clients/serveurs, messagerie...). La commutation dynamique par segment prend en compte les sous-réseaux existants et assure une relation interdomaine sans intervention de l'administrateur. Le fonctionnement du commutateur est similaire à celui d'un pont.

18.3.5 Ethernet *full duplex*

Dans la commutation par port, une station est reliée directement à un port, c'est une liaison en point à point et par conséquent, les risques de collision sont inexistants. L'adaptateur peut alors émettre et recevoir en même temps des messages différents, l'échange est *full duplex*. La technologie *full duplex* (**FDSE**, *Full Duplex Switched Ethernet*) permet de doubler la bande passante d'un réseau local. Initialement réservée aux liens inter-commutateurs, la technologie *full duplex* est aujourd'hui supportée par la plupart des adaptateurs. Il suffit pour cela d'invalider la détection de collision.

18.3.6 Pontage, commutation et trafic *multicast*

Le protocole GARP

La norme IEEE 802.1p définit deux modes de fonctionnement des ponts et commutateurs. Dans le mode de type 1, les ponts ne mettent en œuvre aucune règle de filtrage spécifique, ils ne réalisent que l'acheminement du trafic vers le port où l'*host destination* est raccordé (fonctionnement traditionnel des ponts). Dans le mode de type 2, les ponts mettent en œuvre des règles de filtrage étendues :

– le mode A correspond au mode de fonctionnement traditionnel des ponts (type 1). Les trames *unicast* dont l'adresse destination est connue sont acheminées, les trames *unicast* d'adresse inconnue et les trames de *multicast* et *broadcast* sont diffusées ;

– le mode B est similaire au type 1, cependant les trames *unicast* ne sont acheminées que si leur adresse destination ne figure pas dans une liste de filtrage d'interdiction (acheminement de toutes les trames sauf interdiction) ;
– enfin dans le mode C, la trame *unicast* n'est transmise que si l'adresse destination figure explicitement dans la base de filtrage (acheminement des seules trames autorisées).

Le protocole GARP (*Generic Attribue Registration Protocol*) assure la diffusion des informations de filtrage (inscription ou suppression d'attributs) à travers le réseau ponté ou commuté. En particulier, il sert à la diffusion des informations d'acheminement des trames de *multicast* (**GMRP**, *Generic Multicast Registration Protocol*) et de constitution des VLAN (**GVRP**, *Generic VLAN Registration Protocol*). Le format générique des messages GARP, illustré en figure 18.25, utilise l'encapsulation LLC de l'IEEE.

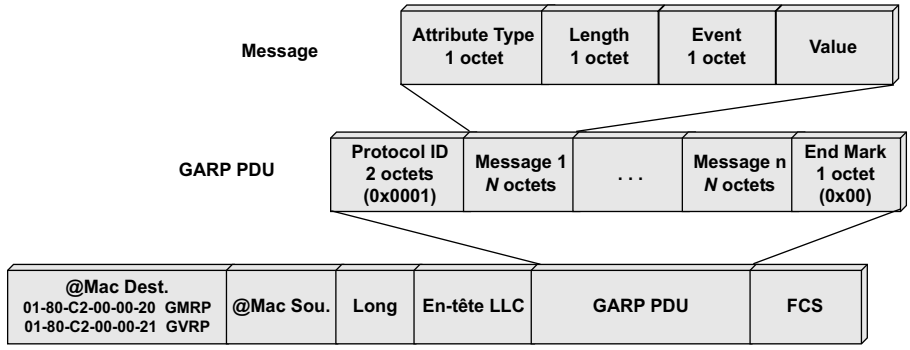


Figure 18.25 Format des messages GARP.

Les protocoles utilisateurs de GARP sont distingués par leur adresse *multicast* MAC destination. La GARP PDU contient une liste de messages. Chaque message est identifié par le champ *Attribue Type* dont les valeurs dépendent du protocole (GMRP ou GVRP). Le champ longueur indique, en octets, la longueur totale de chaque message (type, longueur, événement, valeur). L'action associée à l'attribut (enregistrement ou désenregistrement d'attribut) est définie par le champ Événement (*Event*). Le champ Valeur contient l'adresse de *multicast* (GMRP) ou l'indentification du VLAN concerné (GVRP).

Le protocole GMRP

Le protocole GMRP (**GMRP**, *Generic Multicast Registration Protocol*) permet de limiter la diffusion du trafic *multicast* aux seuls ports d'un pont sur lequel l'adresse du groupe *multicast* a été enregistrée.

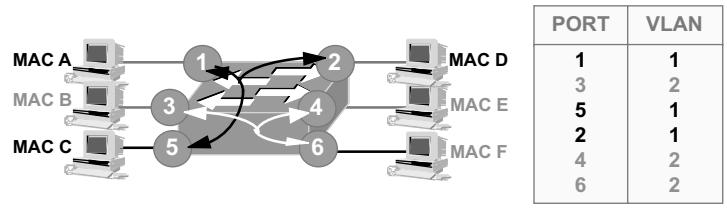
Le principe est simple, une station mettant en œuvre le protocole GMRP demande explicitement au pont auquel elle est raccordée d'être destinataire des messages *multicast* des groupes dont elle communique l'adresse (enregistrement). Cette information se propagera dans le réseau global limitant ainsi le trafic *multicast* aux seuls éléments ayant fait une annonce d'inscription. En conjugaison avec le *Spanning Tree*, GMRP construit un arbre de diffusion *multicast*. Ce protocole est peu utilisé.

© Dunod – La photocopie non autorisée est un délit

18.4 LES RÉSEAUX VIRTUELS OU VLAN (*VIRTUAL LOCAL AREA NETWORK*)

18.4.1 Principes généraux des VLAN

Avec l'accroissement des réseaux, les messages de diffusion (ARP, annonces de service...) occupent une part de plus en plus importante de la bande passante. En définissant, indépendamment de la situation géographique des systèmes, des domaines de diffusion (domaine de *broadcast*), les VLAN autorisent une répartition et un partage optimal des ressources de l'entreprise. Application directe de la commutation statique, les VLAN associent un port à un identifiant. Ne peuvent communiquer que les machines raccordées à des ports de même identifiant. Ainsi, sur le commutateur de la figure 18.26 deux VLAN sont déclarés. La communication entre stations n'est possible qu'entre les stations A, C et D d'une part et les stations B, E et F d'autre part. Il en est de même pour les *brodcasts* qui ne sont diffusés qu'au sein de leur VLAN respectif (domaine de diffusion).



PORT	VLAN
1	1
3	2
5	1
2	1
4	2
6	2

Figure 18.26 Principe des VLAN.

La communication n'est autorisée qu'entre machines d'un même VLAN. Les communications inter-VLAN doivent transiter par un routeur (figure 18.27). Ainsi, les réseaux virtuels permettent de réaliser des réseaux axés sur l'organisation de l'entreprise tout en s'affranchissant de certaines contraintes techniques, notamment celles liées à la localisation géographique des équipements.

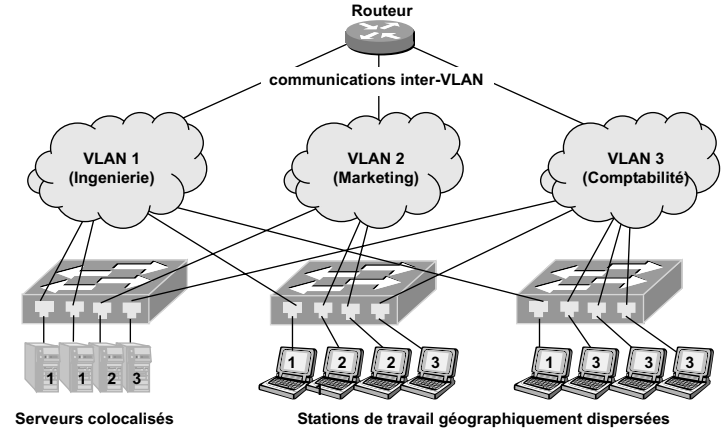


Figure 18.27 La communication inter-VLAN.

En fait, les VLAN introduisent la notion de segmentation virtuelle, qui permet de constituer des sous-réseaux logiques selon des critères prédéfinis (ports, adresses MAC, adresses réseau...).

Un logiciel d'administration permet d'affecter chaque système raccordé à un commutateur à un réseau logique d'appartenance. L'affectation peut être introduite manuellement par l'administrateur station par station (VLAN statique) ou automatiquement par rapport à un identifiant propre à la station comme l'adresse MAC, IP...).

18.4.2 Les différents niveaux de VLAN

Les échanges à l'intérieur d'un domaine sont sécurisés et les communications inter-domaines sont autorisées et peuvent être contrôlées par les filtres configurés dans le routeur. L'appartenance à un VLAN étant définie logiquement et non géographiquement, les VLAN permettent d'assurer la mobilité (déplacement) des postes de travail. Selon le regroupement effectué, on distingue :

– les VLAN de niveau 1 ou VLAN par port (*Port-based VLAN*) : ces VLAN associent chaque port d'un commutateur à un VLAN. Une station raccordée à 1 port est automatiquement affectée au VLAN du port. Si le port est raccordé à un hub, toutes les stations de ce hub appartiennent au même VLAN (VLAN par segment). La configuration est statique (VLAN statique), le déplacement d'une station implique son changement de VLAN. C'est le mode le plus sécurisé, un utilisateur ne peut changer sa machine de VLAN. Un port, donc les stations qui lui sont raccordées, ne peut appartenir qu'à un seul VLAN.

– les VLAN de niveau 2 ou VLAN MAC (*MAC Address-based VLAN*) : ces VLAN associent les stations par leur adresse MAC. De ce fait, deux stations raccordées à un même port (segment) peuvent appartenir à deux VLAN différents. Les relations adresses MAC/VLAN sont introduites par l'administrateur. En fonction du critère d'appartenance à un VLAN, ici l'adresse MAC, les ports déterminent automatiquement leur VLAN d'appartenance (VLAN dynamique). Il existe des mécanismes d'apprentissage automatique d'adresses (lecture des adresses MAC des stations raccordées), l'administrateur n'ayant plus qu'à effectuer les regroupements par simple déplacement et regroupement de stations dans le logiciel d'administration (*Drag&Drop*). Une station peut appartenir à plusieurs VLAN. Les VLAN de niveau 2 sont indépendants des protocoles supérieurs. La commutation, s'effectuant au niveau MAC, autorise un faible temps de latence ;

– les VLAN de niveau 3 ou VLAN d'adresses réseaux (*Network Address-based VLAN*) : ces VLAN sont constitués de stations définies par leur adresse réseau (plage d'adresses) ou par masque de sous-réseau (*Subnet* d'IP). Les utilisateurs d'un VLAN de niveau 3 sont affectés dynamiquement à un VLAN. Une station peut appartenir à plusieurs VLAN par affectation statique. Ce mode de fonctionnement est le moins performant, le commutateur devant accéder à l'adresse de niveau 3 pour définir le VLAN d'appartenance. L'adresse de niveau 3 est utilisée comme étiquette, il s'agit bien de commutation et non de routage. L'en-tête n'est pas modifié.

Il est aussi envisageable de réaliser des VLAN par :

– protocole (IP, IPX...), la communication ne pouvant s'établir qu'entre stations utilisant le même protocole ;

– par application (N° de port TCP), la constitution des VLAN est alors dynamique, un utilisateur pouvant successivement appartenir à des VLAN différents selon l'application qu'il utilise ;

– par mot de passe (constitution dynamique des VLAN au login de l'utilisateur).

© Dunod – La photocopie non autorisée est un délit

La figure 18.28 illustre ces différentes approches. Les VLAN peuvent être définis sur un ou plusieurs commutateurs, que ceux-ci soient locaux ou distants. Cependant, il devra y avoir, entre chaque commutateur, autant de liens (physiques ou virtuels) que de VLAN interconnectés.

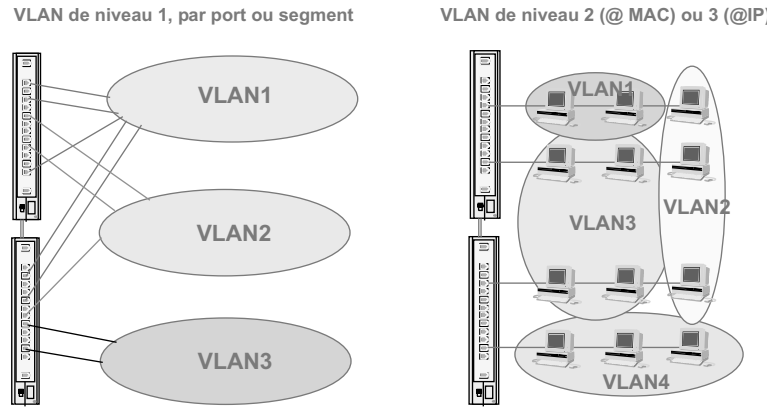


Figure 18.28 Les différents niveaux de VLAN.

18.4.3 L'identification des VLAN (802.1Q)

Principe

Lorsqu'un réseau comporte plusieurs commutateurs, chaque commutateur doit pouvoir localiser toutes les machines (table d'acheminement) et connaître le VLAN d'appartenance de la source et du destinataire (filtrage de trafic). Lorsque le réseau est important, les tables peuvent devenir très grandes et pénaliser les performances. Il est plus efficace d'étiqueter les trames. L'étiquette identifie le VLAN de la station source, le commutateur n'a plus alors qu'à connaître les VLAN d'appartenance des stations qui lui sont raccordées. Ainsi, on distingue deux types d'équipement, ceux qui savent gérer l'étiquetage et qui ont donc connaissance des VLAN (les VLAN *aware*) et ceux qui ignorent cette appartenance (VLAN *unaware*).

Dans le réseau de la figure 18.29 cohabitent des équipements *awares* et *unawares*. Les trames émises par les équipements *awares* sont marquées (*tagged*), celles émises par les équipements *unawares* ne sont pas marquées (*untagged*). La mixité des équipements nécessite que soit défini un VLAN par défaut : le VLAN auquel sont rattachés les équipements *unawares* (VLAN C de la figure 18.29). Lorsqu'un équipement *aware* reçoit une trame marquée à destination d'un équipement *unaware*, il en extrait le *tag*.

La norme IEEE 802.1p/Q

➤ Marquage des trames

Un VLAN correspond à un domaine de *broadcast*. Cependant, lorsque plusieurs VLAN sont définis sur un même segment, cette définition est mise en défaut. Il est évidemment possible d'imaginer que le commutateur transforme le *broadcast* en une rafale d'*unicasts*. La solution adoptée par

l'IEEE est toute différente : un seul VLAN peut être déclaré par port[2], sauf pour les liaisons inter-commutateur supportant le trafic de VLAN différents (liens dits : *trunk link*, figure 18.29).

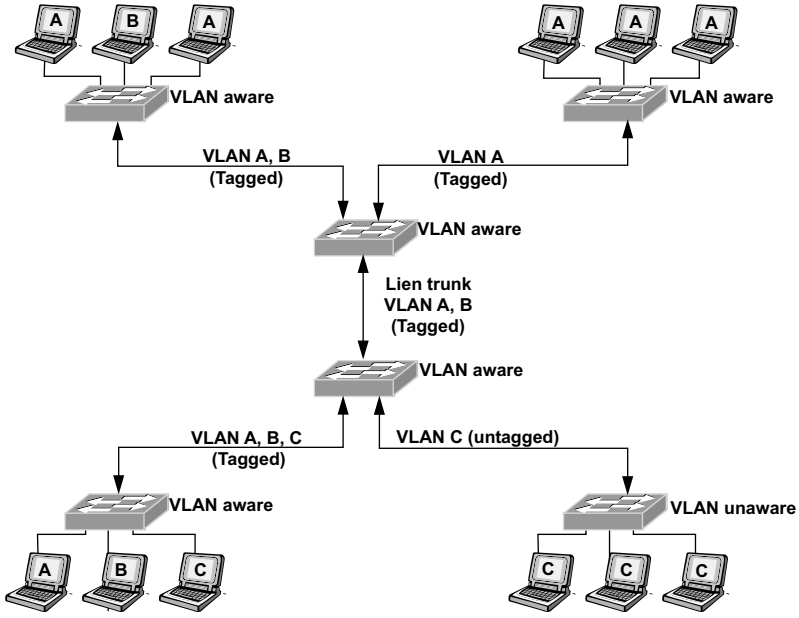


Figure 18.29 Principe de l'étiquetage des trames dans les VLAN.

Les VLAN sont définis dans les normes 802.1Q et 802.1p (802.1p/Q[3]) qui introduisent quatre octets supplémentaires dans la trame MAC. Ces quatre octets permettent d'identifier les VLAN (*VLAN tagging*) et de gérer huit niveaux de priorité (*Qualité of Service, QoS*). La figure 18.30 illustre l'étiquetage d'une trame MAC des réseaux de type 802.3.

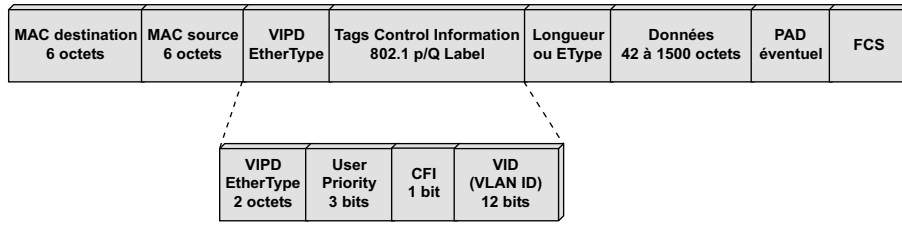


Figure 18.30 Le format de la trame 802.1p/Q.

La trame 802.1p/Q augmente la taille de la trame 802.3, la taille maximale passe ainsi de 1 518 à 1 522 octets. Cet accroissement de la taille des trames limite l'usage des trames marquées aux équipements *awares*. En particulier, la plupart des équipements terminaux (station, périphérique)

2. Certaines implémentations autorisent le raccordement de périphériques partagés par plusieurs VLAN (superposition de ports).

3. 802.1Q concerne les VLAN, 802.1p la qualité de service.

© Dunod – La photocopie non autorisée est un délit

sont encore de type *unaware*, en conséquence, sur les liens d'accès aux commutateurs (*Access link*) ne circulent que des trames non marquées. Les trames sont identifiées par le port d'entrée et le *tag* est extrait par le port de sortie (figure 18.31). Lorsqu'un port d'un équipement *aware* reçoit une trame non marquée, le commutateur affecte le numéro du VLAN du port d'arrivée ou le numéro du VLAN par défaut si ce port n'a pas été configuré.

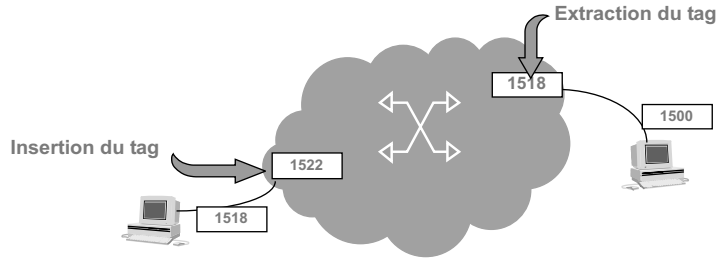


Figure 18.31 L'identification des VLAN internes au réseau.

Pour garantir la compatibilité avec l'existant, le marquage des trames est vu comme une encapsulation supplémentaire. Ainsi, le champ **VPID** (*VLAN Protocol ID*) est similaire au champ Ethertype de la trame 802.3, il identifie le format 802.1 p/Q, sa valeur est fixée à 0x8100 (figure 18.30). Les 2 octets suivants permettent de définir 8 niveaux de priorité (*User Priority*). Les commutateurs de dernière génération disposent de plusieurs files d'attente. Les trames sont affectées à telle ou telle file suivant leur niveau de priorité.

Le bit **CFI** (*Canonical Format Identifier*) est, en principe, inutilisé dans les réseaux 802.3, il doit être mis à 0. Dans les réseaux Token Ring, à 1, il indique que les données du champ Routage par la source sont au format non canonique. Le champ **VID** (*VLAN IDentifier*) identifie, sur 12 bits, le VLAN destination. L'introduction de 4 octets supplémentaires implique que les commutateurs d'entrée et de sortie recalculent le FCS.

➤ Communication intra et inter-VLAN

Lorsque une trame doit être diffusée sur un port appartenant au même commutateur que le port d'origine, la communication est réduite au commutateur concerné. Mais lorsque le destinataire n'est pas situé sur le même commutateur, la trame doit être diffusée sur le réseau. Pour limiter la diffusion aux seuls équipements appartenant au VLAN concerné, les équipements *awares* annoncent périodiquement les VLAN qu'ils gèrent (figure 18.32). Le protocole **GVRP** (*GARD VLAN Registration Protocol*) permet de faire connaître aux autres éléments du réseau les VLAN gérés.

Les communications entre VLAN doivent, en principe, transiter par un routeur. Ce dernier doit posséder un attachement sur chaque VLAN routé. La notion d'interfaces virtuelles évite la multiplication des interfaces physiques sur le routeur. Celui-ci possède une seule interface physique reliée à 1 seul port du commutateur (lien et port *trunk*), sur le routeur plusieurs interfaces virtuelles peuvent être définies (figure 18.33). Lorsque le routeur reçoit une trame marquée, il retire le *tag*, consulte la table de routage et les filtres de trafic associés, il détermine alors l'interface virtuelle de sortie. Chaque interface virtuelle est associée à un VLAN, et marque la trame sortante. L'acheminement peut aussi être réalisé directement par un commutateur enrichi de fonctions de routage (commutation de niveau 3).

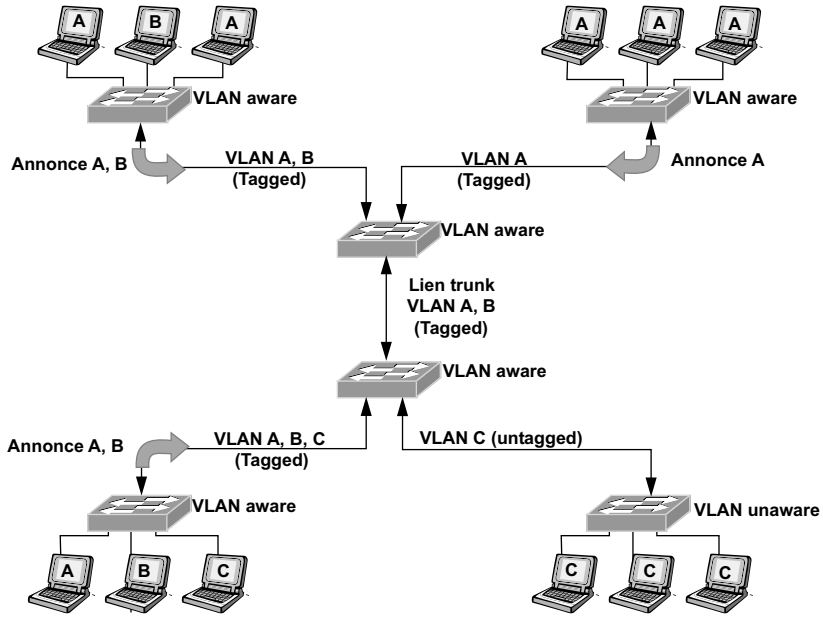


Figure 18.32 Les annonces des VLAN (GVRP).

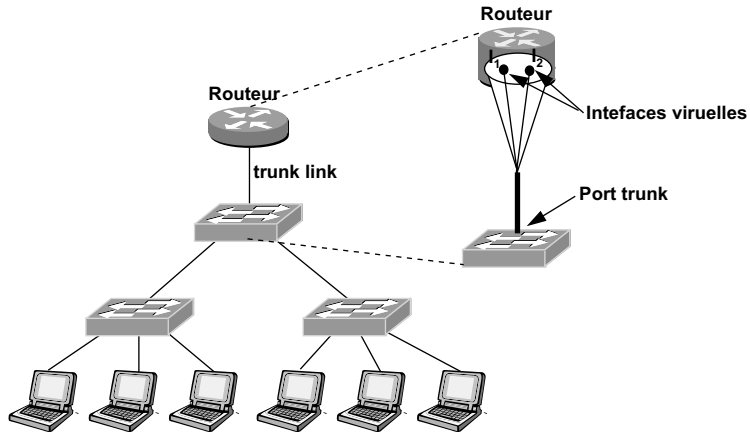


Figure 18.33 Notion d'interfaces virtuelles.

18.5 CONCLUSION

À l'origine imaginés pour des raisons essentiellement de performance, les ponts puis les commutateurs permettent aujourd'hui, non seulement d'améliorer les performances par segmentation des réseaux mais surtout apportent un niveau de sécurité supérieur en isolant les trafics des différents utilisateurs (VLAN).

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 18.1 Interconnexion d'un réseau 802.3 et 802.5

Vous envisagez de réaliser un **pont** susceptible d'interconnecter un réseau 802.3 avec un réseau 802.5. Quels sont les problèmes à résoudre ?

Exercice 18.2 *Spanning Tree Protocol* (STR)

Construisez l'arbre recouvrant (*Spanning tree*) du réseau de la figure 18.34 en prenant en compte les identifiants (**ID**) et les coûts (**C**) indiqués. Commentez la solution obtenue, en existe-t-il une meilleure ?

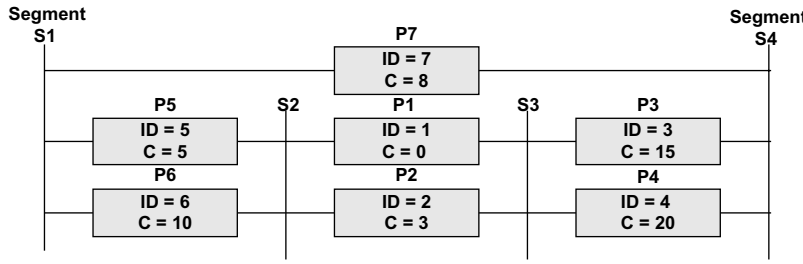


Figure 18.34 Le réseau ponté avec chemins redondants.

Exercice 18.3 Performances hub/commutateur

Comparez les performances d'un réseau de type Ethernet, pour une architecture à base de hubs, de commutateurs *cut through* (retransmission à la volée, dès lecture de l'adresse destination), et de commutateurs *store and forward* (stockage et retransmission). On formulera les hypothèses suivantes :

- l'échange ne concerne que deux stations qui accèdent donc immédiatement au support (pas de collision) ;
- le temps de transit sur le réseau et le temps CPU des machines d'extrémité sont considérés comme nul ;
- les cartes réseaux fonctionnent en mode *half duplex* ;
- le temps de latence des hubs et commutateurs sera admis égal au temps d'acquisition en réception des informations nécessaires aux commutateurs avant retransmission ;
- les trames de données seront remplies au maximum de la capacité d'emport d'une trame Ethernet (MTU) ;
- chaque trame de données sera explicitement acquittée, un acquittement correspond à une trame TCP/IP dont le champ de données est vide ;
- la pile protocolaire est TCP/IP, aucune option n'est invoquée.

1. Quelle est la MTU des réseaux de type Ethernet (version 10 et 100 Mbit/s) ?
2. Complétez la figure 18.35 en exprimant la longueur de chaque champ en bits. La figure représente un message de données suivi de son acquittement.

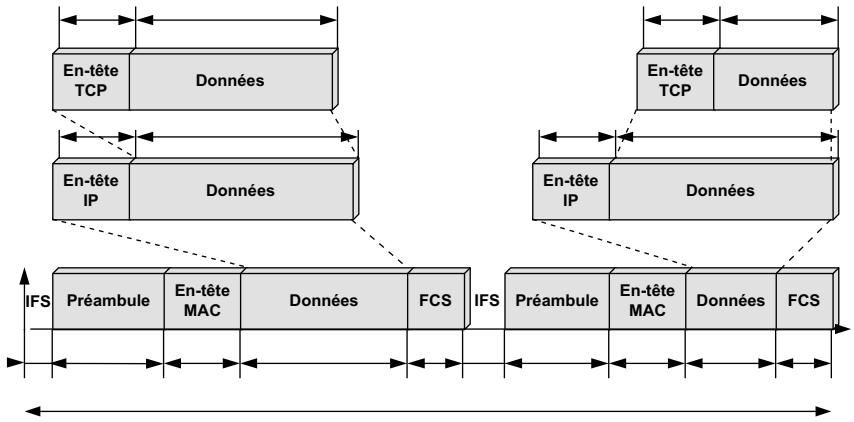


Figure 18.35 Taille des différents champs en bits.

3. Exprimez en bits les temps de latence totale pour un cycle pour chacun des équipements : hub, commutateur *cut through* et commutateur *store and forward*.
4. Établissez le rapport entre le nombre de bits utiles et le nombre de bits transmis ou qui auraient pu l'être durant un cycle d'échange et déduisez l'efficacité des équipements : hub, commutateur *cut through* et commutateur *store and forward*.

   Résumez les résultats dans la figure 18.36.

Équipement	Volume des données utiles en bits	Durée de l'échange en bits (hors temps de latence)	Temps de latence dans l'équipement en bits	Durée totale de l'échange exprimé en bit	Efficacité du système
Hub					
Commutateur *cut through*					
Commutateur *store and forward*					

Figure 18.36 Échange à compléter.

5. En réalité les stations sont connectées *via* un commutateur 10/100, l'une des stations a une interface réseau à 10 Mbit/s, l'autre à 100. Le commutateur peut-il, sur cette liaison, fonctionner en mode *cut through* ? Justifiez votre réponse.
6. La commutation *cut through* est plus efficace que la commutation *store and forward*. Cependant dans un système de commutation par segment les trames erronées, à cause d'une collision, sont retransmises. Imaginez une solution pour que les commutateurs *cut through* ne propagent pas les collisions. Quelle serait alors l'efficacité du système ?

© Dunod – La photocopie non autorisée est un délit

Exercice 18.4 Choix d'un équipement

En fonction des critères de choix imposés, indiquez l'équipement répondant le mieux (hub ou commutateur) et éventuellement complétez la réponse en indiquant la technologie interne de l'équipement et/ou le mode de configuration du réseau.

Caractéristiques du réseau	Critères de choix	Équipement/technologie complémentaire
Peu chargé, et peu de *broadcasts*	Performance	
Relativement chargé, peu de *broadcasts* et d'erreurs	Performance et simplicité de l'administration	
Relativement chargé, peu de *broadcasts*, de nombreuses erreurs (câblage défectueux)	Performance et simplicité de l'administration	
Relativement chargé et de nombreux *broadcasts*	Performance	
Trafic voix/données	Qualité des liaisons voix	

Figure 18.37 Tableau à compléter.

Chapitre **19**

Interconnexion des réseaux et qualité de service

19.1 L'INTERCONNEXION DES RÉSEAUX, GÉNÉRALITÉS

19.1.1 Définition

Le déploiement des réseaux d'établissement a permis le traitement local des informations. Cependant, pour assurer la cohérence du système d'information de l'entreprise, il est nécessaire d'organiser l'échange d'information entre ses différentes composantes. Tel est l'objet de l'interconnexion des réseaux. Indépendamment de la distance qui les sépare et des protocoles utilisés, l'interconnexion consiste à mettre en relation des machines appartenant à des réseaux physiquement distincts par l'intermédiaire d'éléments d'interconnexion, appelés relais dans la terminologie OSI. Le relais peut n'être qu'un simple élément matériel (pont, routeur...) mais aussi un réseau (figure 19.1).

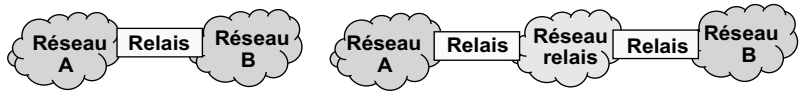


Figure 19.1 Principe de l'interconnexion des réseaux.

19.1.2 Les problèmes liés à l'interconnexion

La mise en relation d'un système A avec un système B peut se réaliser très simplement si A, B et le relais utilisent les mêmes protocoles, comme, par exemple, l'interconnexion de deux réseaux locaux utilisant TCP/IP *via* un réseau IP. Cependant, dans la plupart des cas, le protocole du réseau relais est différent du protocole local, par exemple l'interconnexion de deux réseaux locaux TCP/IP *via* un réseau de transport X.25, Frame Relay (relais de trame) ou ATM. Quand les deux éléments à raccorder mettent en œuvre des technologies différentes, l'hétérogénéité est de bout en bout. Dans ce cas, pour assurer l'interfonctionnement des systèmes, une unité d'interfonctionnement (**UIF**) réalise les adaptations nécessaires. Trois techniques peuvent alors être utilisées : la conversion de service, la conversion de protocole et l'encapsulation.

19.1.3 Les notions de conversion de service et de protocole

Dans la conversion de service (figure 19.2), le relais reçoit les messages selon le format B, il assure la transposition de l'unité de service SDU(B) (*Service Data Unit*) en une unité de service SDU(C). Cette technique est utilisable lorsque les protocoles à mettre en relation sont différents mais compatibles. C'est le cas, par exemple, du passage d'un réseau Ethernet 802.3 10Base5 à un réseau Ethernet 802.3 10BaseT. L'UIF intervient alors au niveau physique (sous-couche **PMD**, *Physical Medium Dependant*).

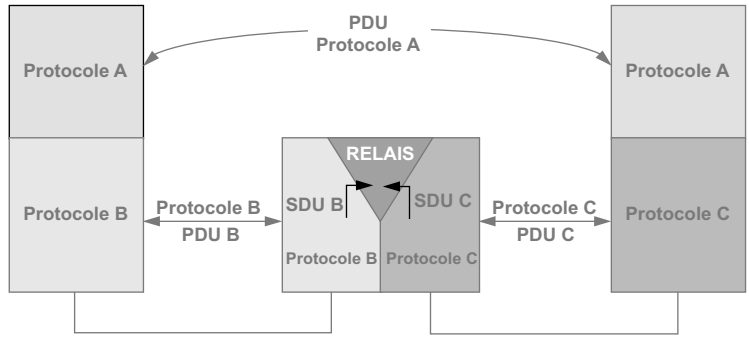


Figure 19.2 La conversion de service.

La conversion de protocole (figure 19.3) intervient lorsque les protocoles d'extrémité sont différents et incompatibles. C'est, par exemple, le cas lors de l'interconnexion d'un réseau de type Ethernet et d'un réseau de type Token Ring, l'UIF intervient ici au niveau MAC.

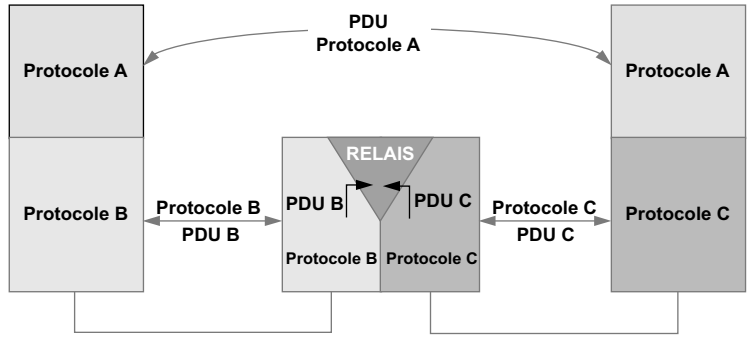


Figure 19.3 La conversion de protocole.

La différence entre ces deux méthodes est toute théorique et transparente à l'utilisateur.

19.1.4 L'encapsulation ou *tunneling*

Généralités

La conversion de protocole est irréversible. En effet, si on interconnecte deux réseaux IP *via* par exemple un réseau X.25, il est aisé, à partir des informations d'en-tête du datagramme IP de confectionner un en-tête X.25, mais il est totalement impossible à partir des données d'en-tête X.25 de

reconstituer le datagramme d'origine. Pour disposer des informations nécessaires à la reconstruction du datagramme d'origine, il suffirait d'insérer un sous-champ entre l'en-tête du nouveau protocole et les données à transporter. Cette méthode serait lourde, il est préférable de transporter, dans le champ de données d'X.25, le datagramme IP complet. Le travail des UIF s'en trouve alors facilité. Ce mécanisme se nomme encapsulation de données. On parle aussi de *tunneling*, car on a réalisé un « tunnel » X.25 qui transporte des données IP. L'encapsulation de données est illustrée par la figure 19.4.

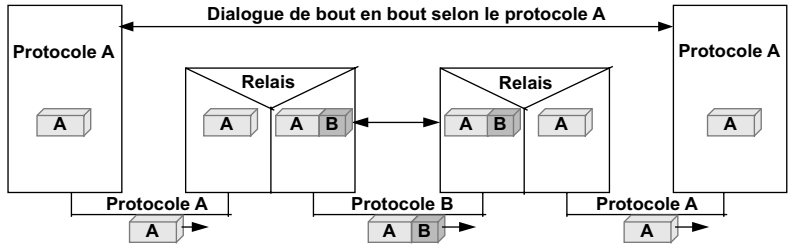


Figure 19.4 L'encapsulation de données.

Dans le schéma de la figure 19.4, les PDU du protocole A, issues de l'un des systèmes, sont encapsulées dans des PDU (*Protocol Data Units*) du protocole B par le premier relais. Les données sont transférées en mode transparent par le réseau qui considère l'intégralité de la PDU (A) comme des données. Le relais final exécute l'opération inverse, la PDU du protocole A est restituée.

L'encapsulation est utilisée chaque fois que le protocole du réseau intermédiaire (relais) est incompatible avec celui des réseaux d'extrémité.

Exemples d'encapsulation

➤ Transport des données dans un réseau Frame Relay

Généralités

Parfaitement adapté à l'interconnexion des réseaux locaux, le Frame Relay ou relais de trames assure le transport de protocoles divers (X.25, TCP/IP, SNA...) en mode transparent (encapsulation ou *tunneling*). Le réseau Frame Relay est vu, vis-à-vis de ces protocoles, comme un support physique.

Les mécanismes d'encapsulation dans le relais de trames sont définis dans la norme ANSI/TI.617 annexe G pour X.25 (couramment appelé annexe G) et annexe F pour l'encapsulation multiprotocole. L'IETF précise l'encapsulation multiprotocole de la RFC 1490 (similaire à l'annexe F). Généralement, l'annexe G est préférée pour l'encapsulation X.25 et la RFC 1490 pour le transport des autres protocoles.

Encapsulation X.25 (Annexe G)

Le transport d'X.25 dans le Frame Relay est des plus simples, la trame HDLC (LAP-B) est directement encapsulée dans une trame relais de trames. Il n'y a aucune donnée protocolaire spécifique d'ajoutée. Cette simplification améliore les performances, mais exclut tout multiplexage protocolaire sur la même connexion. Le DLCI est dédié à un transport X.25, cette technique n'interdit nullement plusieurs circuits virtuels X.25 sur le même DLCI (1 par protocole à transporter).

© Dunod – La photocopie non autorisée est un délit

Cependant, la liaison reste une liaison point à point, le réseau relais de trames n'a aucun moyen d'acheminer les paquets X.25 (pas de mécanisme de résolution d'adresse entre une adresse X.121 et un numéro de DLCI). L'interconnexion de réseaux X.25 *via* un réseau Frame Relay est illustré en figure 19.5.

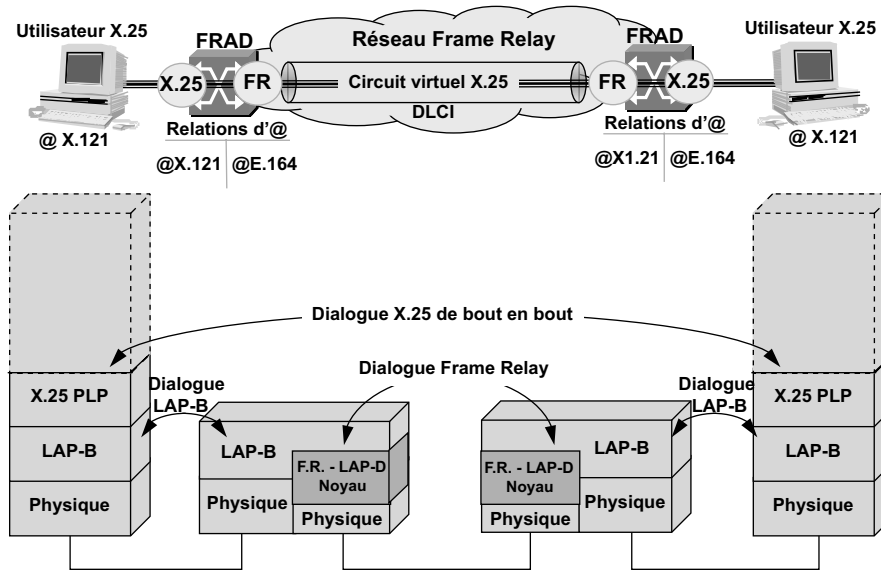


Figure 19.5 Le transport d'X.25 dans le Frame Relay.

À réception du paquet d'appel, le FRAD (*Frame Relay Access Device*) d'entrée consulte la table de correspondance d'adresse, examine si une liaison virtuelle est déjà établie vers la destination E.164 correspondante. Si ce n'est pas le cas, il ouvre une liaison virtuelle, celle-ci établie, le paquet d'appel X.25 est transmis ouvrant ainsi un circuit virtuel X.25 de bout en bout. Le réseau Frame Relay est alors vu comme un simple support physique pour les réseaux X.25 interconnectés (*tunneling*). La figure 19.6 représente l'encapsulation telle qu'elle est définie dans l'annexe G.

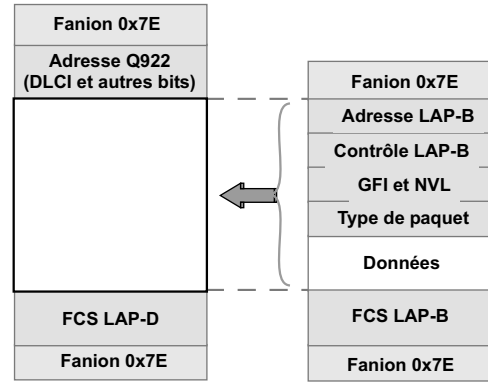


Figure 19.6 L'encapsulation de l'annexe G.

Notons que le FCS de la trame LAP-B n'est pas recopié dans la trame, c'est le FCS de la trame Frame Relay qui est utilisé dans le réseau. Le FCS de la trame LAP-B est recalculé par la passerelle de sortie du réseau.

Encapsulation multiprotocole (RFC 1490)

La RFC 1490 pallie l'un des défauts de l'annexe G, elle identifie le protocole transporté et permet ainsi le multiplexage de protocoles différents sur un même DLCI. L'encapsulation multiprotocole définie dans la RFC 1490 a un format similaire à celui de la trame d'information non numérotée de LAP-D (champ Contrôle UI = 0x03) et introduit un champ d'identification : le **NLPID** (*Network Level Protocol Identifier*) qui identifie le protocole encapsulé (figure 19.7). Le champ PAD, facultatif, n'apparaît que pour restaurer l'alignement de la trame sur des mots de 16 bits, ce champ, lorsqu'il est présent, est mis à zéro.

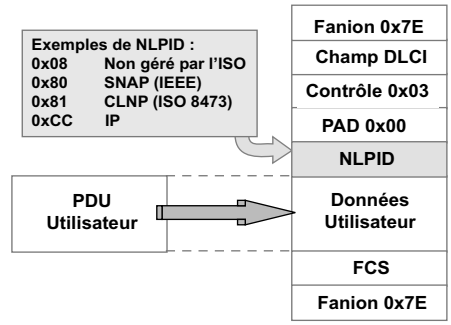


Figure 19.7 Le format général de l'encapsulation multiprotocole.

Les différentes valeurs du NLPID sont attribuées par ISO, cependant tous les protocoles ne disposent pas NLPID, on utilise alors le format **SNAP** (*SubNetwork Access Protocol*) défini par l'IEEE (OUI et Ethertype). Dans ce mode d'encapsulation (NLPID non défini), le champ de la trame Frame Relay vaut alors 0x80. La figure 19.8 décrit les trois formats type d'encapsulation sur le Frame Relay. La valeur 0x00-00-00 du champ OUI indique que le champ PID est codé comme le champ Ethertype de l'Ethernet DIX.

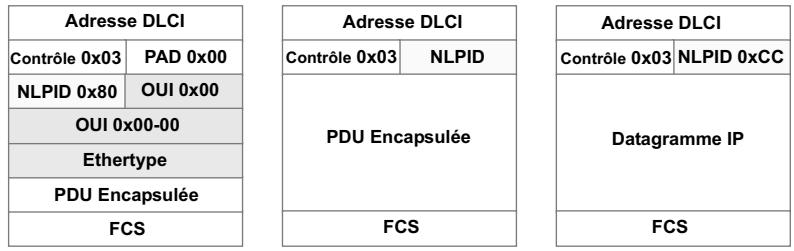


Figure 19.8 L'encapsulation Frame Relay (RFC 1490)

Le protocole IP du DoD disposant d'un NLPID (*Network Level Protocol ID*) assigné (0xCC) et d'un Ethertype géré par l'IEEE (0x0800), l'encapsulation du protocole IP peut utiliser l'un ou l'autre des deux formats. Seul, en principe, le format NLPID est autorisé. En allégeant l'en-tête de 48 bits, le format NLPID est plus performant.

© Dunod – La photocopie non autorisée est un délit

➤ Transport des données dans un réseau ATM

À l'instar du Frame Relay, ATM utilise deux modes d'encapsulation (RFC 1483, *Multiprotocol Encapsulation over ATM*). Le *VC multiplexing*, comme l'annexe G, crée autant de circuits virtuels ATM indépendants que de protocoles à transporter. Cette méthode est dite *Null Encapsulation*. Le second mode utilise l'AAL5 (figure 19.9), les données utilisateur sont encapsulées dans une trame LLC (*Logical Link Control*) de type SNAP (*SubNetwork Access Protocol*) déjà décrite précédemment.

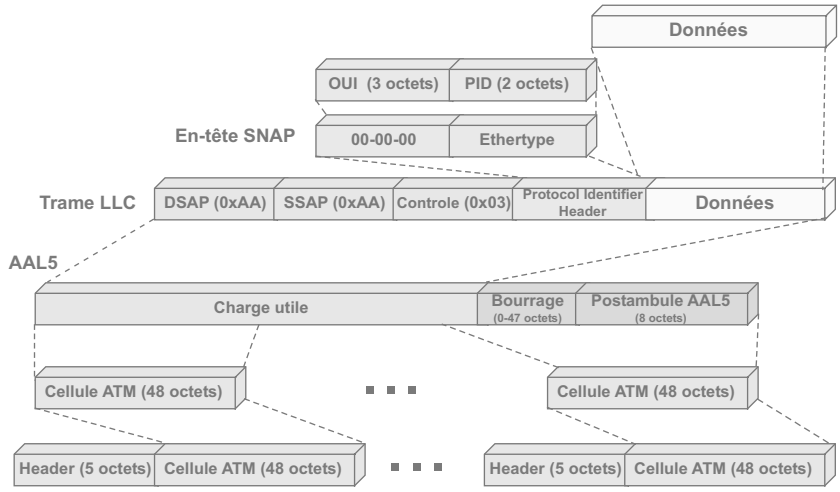


Figure 19.9 L'encapsulation Frame Relay (RFC 1490)

19.2 LES ÉLÉMENTS D'INTERCONNEXION (RELAIS)

19.2.1 Définitions

Selon le niveau du modèle de référence où se réalise l'interconnexion de deux ou plusieurs réseaux, l'ISO distingue quatre types de relais (figure 19.10) :

- les répéteurs, organes d'interconnexion locaux, ils agissent au niveau 1 du modèle de référence ;
- les ponts (*bridges*) interviennent au niveau 2 ;
- les routeurs[1] sont des éléments d'interconnexion de niveau 3 ;
- au-dessus, on parle de passerelles. Cependant, l'usage désigne une interconnexion de niveau 4 comme un adossement de transport. L'adossement de transport n'est pas conforme au modèle de référence, la couche 4 n'étant plus alors de bout en bout.

1. En principe, il conviendrait de réserver le terme de routeur à l'interconnexion de réseaux dont les espaces d'adressage sont homogènes et d'utiliser le terme de passerelle inter-réseau lorsque les espaces d'adressage des réseaux à interconnecter sont différents. Cependant, le langage courant utilise le terme de routeur dans les deux cas. Nous nous conformerons à cet usage.

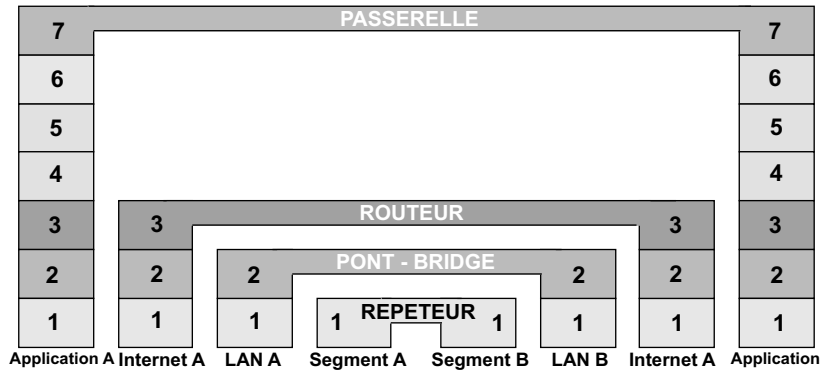


Figure 19.10 Les organes d'interconnexion selon l'ISO.

Généralement les passerelles agissent au niveau applicatif, elles mettent en relation des applications de même nature mais d'architecture différente ; c'est, par exemple, le cas d'une interconnexion d'une messagerie **SMTP** (*Simple Mail Transfer Protocol*) du monde TCP/IP avec une messagerie X.400 du monde ISO.

19.2.2 Les répéteurs

Les répéteurs réalisent une connexion physique entre deux segments d'un même réseau logique (figure 19.11). Agissant au niveau physique, les réseaux interconnectés doivent être homogènes. Un répéteur ne fait que retransmettre d'un côté les bits reçus sur l'autre, il agit par diffusion.

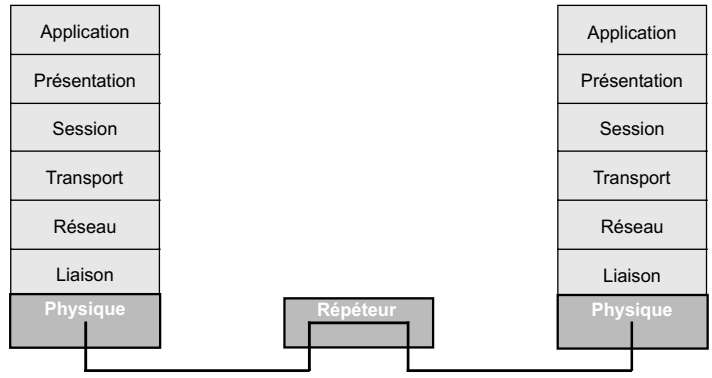


Figure 19.11 Situation des répéteurs dans le modèle OSI.

De ce fait, il ne peut que réaliser la prolongation ou le changement de support et non une interconnexion, au sens fonctionnel, de deux réseaux. Il est utilisé pour réaliser l'adaptation des supports (passage coaxial à la fibre optique, par exemple) ou pour accroître la portée géographique d'un réseau (régénération du signal et récupération d'horloge, figure 19.12). L'utilisation de répéteurs est sans incidence sur les protocoles transportés. Cependant, en augmentant la portée du réseau, il peut être nécessaire de modifier les temporisations.

Les répéteurs peuvent aussi être utilisés pour réaliser l'isolation galvanique de deux segments de réseau alimentés par des réseaux électriques différents ou reliés à des terres dont l'équipotentialité

© Dunod – La photocopie non autorisée est un délit

n'a pas été réalisée (interconnexion de réseaux situés dans des bâtiments différents ou alimentés par des réseaux courant fort[2] différents).

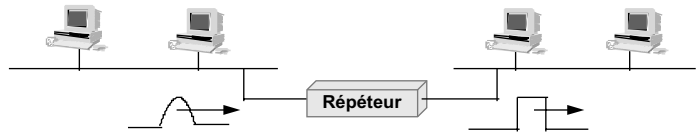


Figure 19.12 Fonction de régénération de signaux des répéteurs.

La figure 19.13 illustre le changement de support et la prolongation de la portée géographique par l'utilisation de répéteurs dans les réseaux de type Ethernet et Token Ring.

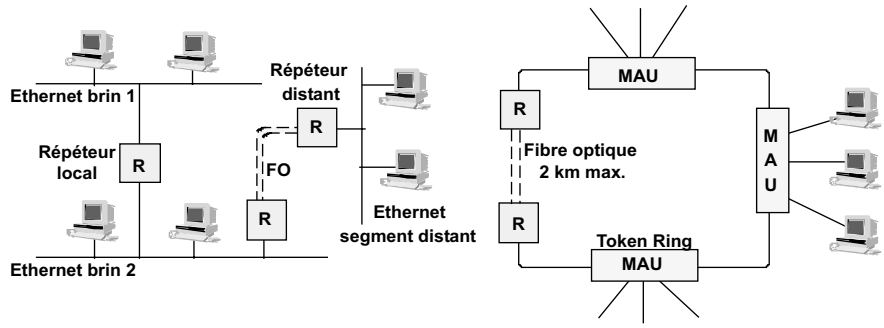


Figure 19.13 L'interconnexion par des répéteurs.

19.2.3 Les ponts

Les ponts ou *bridges* sont des éléments d'interconnexion de niveau 2. Ils permettent d'interconnecter deux ou plusieurs réseaux (ponts multiports) dont les couches physiques sont dissemblables (figure 19.14). Les ponts sont transparents aux protocoles de niveau supérieur.

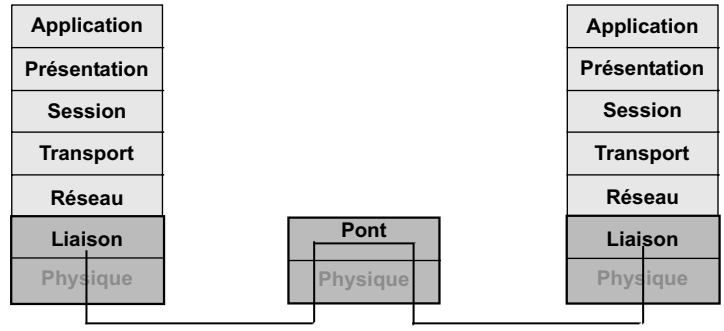


Figure 19.14 Situation des ponts dans le modèle OSI.

2. On appelle courant fort, la distribution de l'énergie électrique et par opposition courant faible les réseaux filaires téléphoniques et informatiques.

Les ponts assurent des fonctions d'adaptation de débit ou de support entre réseaux locaux. Agissant au niveau 2 du modèle de référence, ils ont accès à l'adresse MAC. De ce fait, ils peuvent acheminer les trames, en fonction de l'adresse MAC, réalisant ainsi un acheminement de niveau 2 » (figure 19.15). Les ponts ne peuvent interconnecter que des réseaux dont l'espace d'adressage est homogène. Les réseaux interconnectés constituent un seul et unique réseau logique.

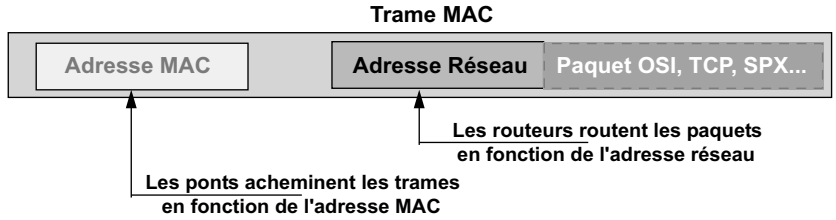


Figure 19.15 Les fonctions de filtrage et d'acheminement des ponts.

19.2.4 Les routeurs

Généralités

Un routeur est un élément d'interconnexion de niveau 3 qui achemine (route) les données vers un destinataire identifié par son adresse de niveau 3 (X.121, IP du DoD ou autre). Agissant au niveau 3 (figure 19.16), les routeurs offrent plus de possibilités que les ponts puisqu'ils peuvent mettre en œuvre les mécanismes du niveau 3 (segmentation, réassemblage, contrôle de congestion...).

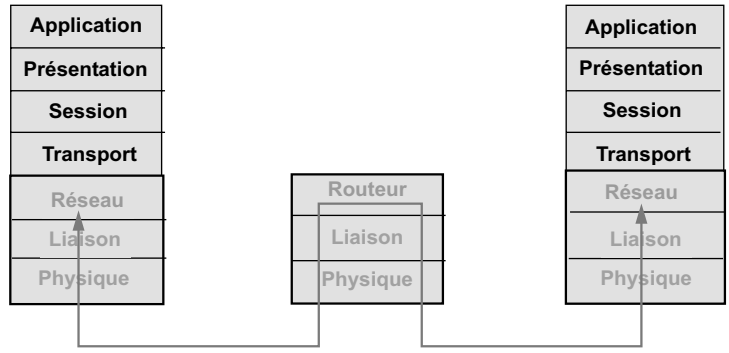


Figure 19.16 Situation des routeurs dans le modèle de l'ISO.

Les routeurs et les passerelles inter-réseau

Un routeur permet le relayage de paquets entre deux réseaux d'espace d'adressage homogène (IP/IP, ISO/ISO...). Lorsque l'espace d'adressage n'est pas homogène, par exemple interconnexion de réseaux IP *via* un réseau X.25, il est nécessaire de mettre en œuvre un mécanisme de conversion d'adresses (IP/ISO) non défini au niveau 3 de l'ISO. Ce mécanisme n'est pas normalisé et chaque constructeur apporte sa solution. L'organe d'interconnexion n'est plus strictement un routeur, c'est une passerelle[3] inter-réseau, que le langage courant continue d'appeler routeur.

3. Pendant longtemps, les RFC ont ignoré le terme de routeur et n'ont utilisé que celui de passerelle (*Gateway*).

© Dunod – La photocopie non autorisée est un délit

La figure 19.17 illustre l'interconnexion de deux réseaux homogènes, ceux-ci mettent en œuvre le protocole TCP/IP et le réseau d'interconnexion utilise le protocole IP, l'espace d'adressage est identique. Les données issues d'un réseau sont transportées par un protocole appartenant à la pile TCP/IP : **PPP** (*Point-to-Point Protocol*).

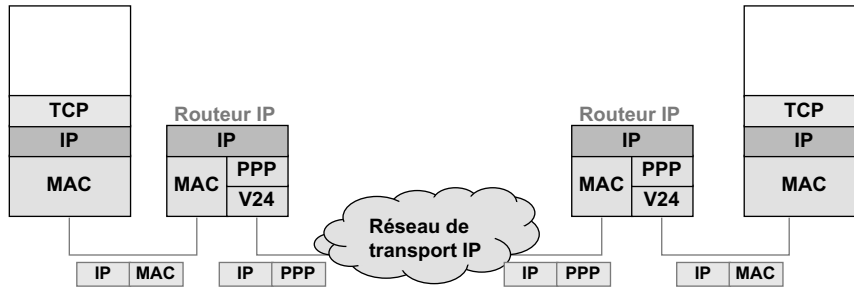


Figure 19.17 L'interconnexion de réseaux homogènes.

L'acheminement de datagrammes IP entre deux réseaux locaux directement reliés par un routeur est illustré par la figure 19.18. En 1, la machine source de la figure 19.18 doit envoyer un datagramme à la machine d'adresse IP *@IPD* n'appartenant pas au même réseau, ou sous-réseau, qu'elle ; pour cela, elle doit faire appel au service du routeur. Les données acquises lors de sa configuration lui indiquent l'adresse IP de la « passerelle » par défaut. Elle émet alors une requête ARP pour découvrir l'adresse MAC de cette « passerelle ». Puis lui transmet le message. En 2, le routeur recevant un datagramme dont l'adresse IP n'est pas la sienne, sait qu'il doit en réaliser l'acheminement. Il consulte alors sa table de routage qui lui indique l'interface de sortie. Cette interface est une interface de réseau local, pour acheminer le paquet il doit donc connaître l'adresse MAC du destinataire. Pour cela en 3, il émet une requête ARP sur ce segment local, puis achemine le datagramme vers son destinataire.

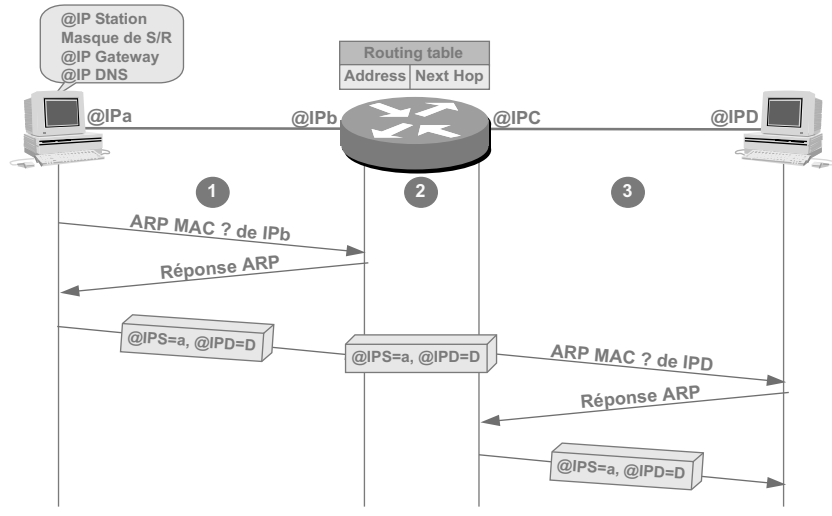


Figure 19.18 Le mécanisme global d'acheminement entre deux réseaux locaux.

Le mécanisme est évidemment plus complexe lorsque les protocoles d'extrémité et de cœur de réseau sont différents (figure 19.19).

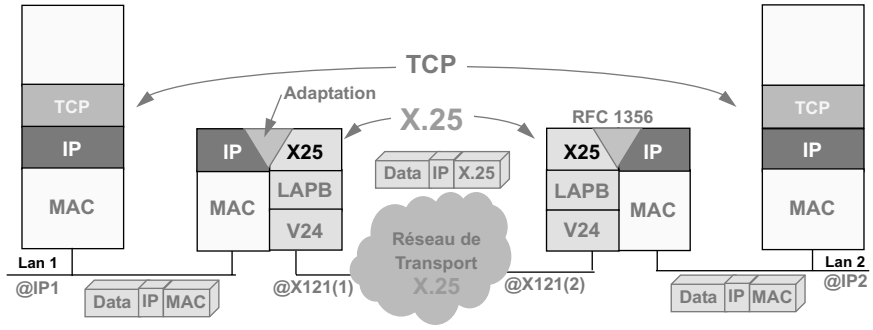


Figure 19.19 L'interconnexion de réseaux hétérogènes.

Les deux réseaux locaux IP LAN 1 et LAN 2 sont reliés *via* un réseau X.25 (RFC 1356). Le protocole inter-réseau utilisé (X.25) est totalement incompatible avec le protocole des réseaux d'extrémité (TCP/IP). Non seulement les adresses sont incompatibles (X.121 pour X.25 et IP pour TCP/IP), mais les réseaux utilisent des techniques différentes (mode datagramme pour TCP/IP et mode orienté connexion pour X.25). La passerelle devra assurer la conversion d'adresse, l'ouverture et la fermeture des circuits virtuels et ceci pour chaque adresse IP distante.

L'architecture d'un routeur

Un routeur met en relation un couple de ports d'accès (LAN ou WAN) identifiés par une adresse réseau. Le schéma de la figure 19.20 représente l'architecture simplifiée d'un routeur.

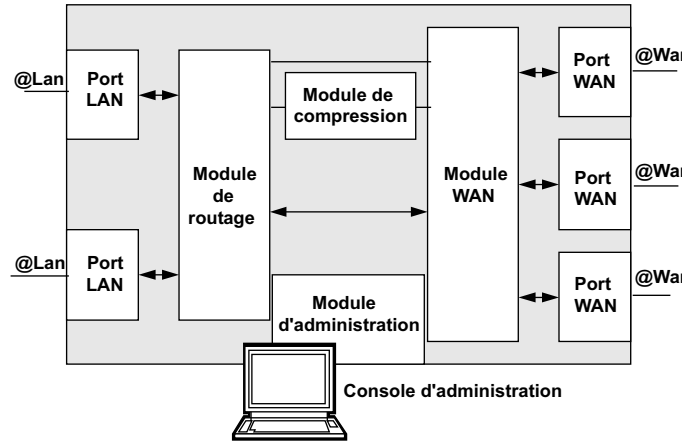


Figure 19.20 L'architecture simplifiée d'un routeur.

La configuration générale d'un routeur consiste en une succession de déclarations pour effectuer la mise en relation des différents modules, et en un ensemble de paramètres décrivant leurs caractéristiques (protocole utilisé, MTU, taille fenêtre...). Un routeur n'est pas obligatoirement une

© Dunod – La photocopie non autorisée est un délit

machine spécifique, une station d'un réseau local peut participer à l'acheminement des données (Unix, Linux, Windows NT...).

L'opération de routage est consommatrice de temps CPU, elle constitue une limite à l'évolution des réseaux IP vers les hauts débits. En effet, l'augmentation du débit en ligne suppose que les équipements intermédiaires aient des capacités de traitement en adéquation. Une nouvelle génération de routeurs destinée au cœur de réseau, les giga-routeurs, autorise le routage de plusieurs millions de paquets par seconde permettant ainsi d'interfacer directement les routeurs avec des liens à plusieurs Gbit/s. Le gain de performance peut être obtenu en distribuant les traitements sur chaque interface d'entrée[4] et en acheminant les paquets vers l'interface de sortie par une technique de commutation (figure 19.21).

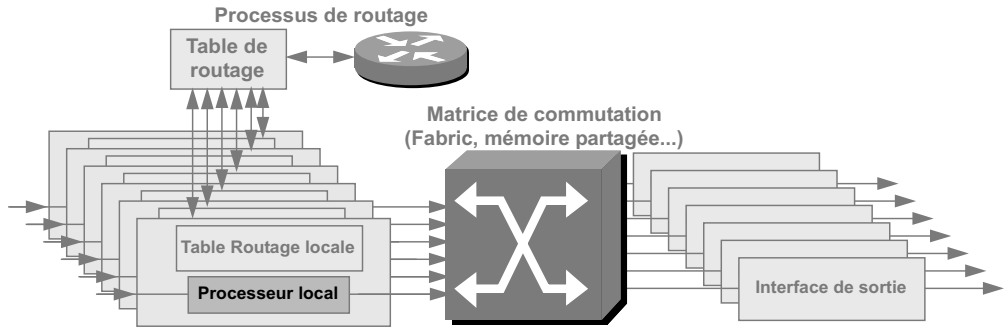


Figure 19.21 La structure d'un giga-routeur.

19.3 LES TECHNIQUES DE ROUTAGE

19.3.1 Généralités

L'étude de ces techniques a été initialisée au chapitre 6. Rappelons-en le principe, les routeurs acheminent les paquets selon des informations contenues dans des tables dites tables de routage. Ils utilisent essentiellement deux modes de routage :

– le routage statique ou fixe, dans ce type de routage, les tables de routage sont introduites par l'administrateur de réseau à la configuration du réseau ;
– le routage au moindre coût, dans ce type de routage, les tables de routages indiquent pour chaque destination le chemin de coût le moins élevé. Périodiquement, des échanges d'information entre les routeurs permettent de maintenir ces tables à jour. Les algorithmes de vecteur distance (*Distance vector routing*) et à état des liaisons (*Link state routing*) sont de cette nature.

La station qui a des données à transmettre connaît le routeur auquel elle est rattachée (routeur ou passerelle par défaut). Ce routeur doit ensuite déterminer le prochain noeud à atteindre pour trouver le destinataire. Ce choix est effectué par consultation de la table de routage en fonction d'une politique de routage. Rappelons qu'un protocole de routage n'indique pas comment est prise la décision de routage (politique de routage), il détermine seulement comment sont échangées les

4. En fait, un giga-routeur est constitué d'un routeur logique par interface et d'un mécanisme de distribution de tables de routages sur ces interfaces.

informations de routage. Dans la pratique, ces notions sont confondues. Un protocole de routage résout essentiellement trois problèmes :

– il découvre les autres routeurs du réseau,
– il construit les tables de routage,
– il maintient les tables de routage à jour.

Si on veut réaliser l'interconnexion de réseaux d'opérateurs différents, il est nécessaire, à l'interface entre les réseaux, de définir un protocole commun d'échange des informations de routage. Chaque opérateur peut alors, en interne dans son réseau, utiliser le mode de routage qui lui convient. Aussi, outre l'aspect de limitation du trafic de gestion, le domaine global de routage (**Internet**) a été subdivisé en domaines de routage autonomes (**AS**, *Autonomous System*). Cette division conduit à distinguer deux familles de protocoles de routage (figure 19.22) :

– les protocoles de routage intra-domaine, pour le routage à l'intérieur d'un même domaine (**IGP**, *Interior Gateway Protocol*). Les paquets de service du protocole de routage identifient le domaine d'appartenance, tout paquet qui n'appartient pas au même domaine est ignoré. Cette technique limite la diffusion à l'intra-réseau ;
– les protocoles de routage inter-domaine (**EGP**, *Exterior Gateway Protocol*). Ces protocoles routent les paquets d'information dans l'inter-réseau. Ces protocoles doivent prendre en compte les accords commerciaux ou politiques entre les différents opérateurs des systèmes autonomes. Notons que les machines d'accès à l'inter-réseau mettent en œuvre les deux types de protocole, un protocole intra-domaine sur leurs liens intra-domaines, et un protocole inter-domaine sur le ou les lien(s) inter-réseaux.

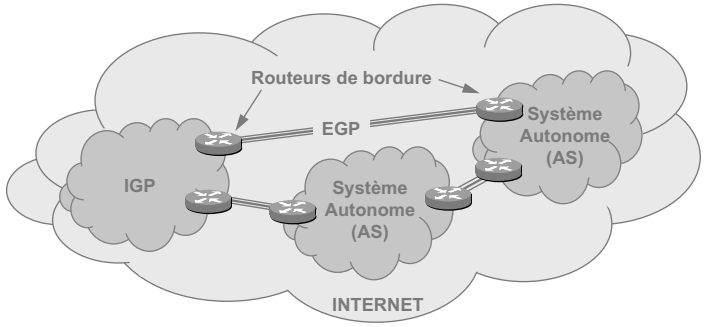


Figure 19.22 Le découpage d'Internet en domaines de routage.

19.3.2 Le routage vecteur-distance, RIP

RIP v1

Issu des travaux de Bellman-Ford, le protocole **RIP** (*Routing Information Protocol*, RFC 1058), développé par l'Université de Californie (UCB, *University of California at Berkeley*) pour Unix BSD 4.2 (*Berkeley Software Distribution*) et utilisé initialement dans Arpanet, est en raison de sa simplicité, de sa solidité, de sa facilité de mise en œuvre et, ceci malgré ses lacunes, le protocole de routage vecteur distance le plus diffusé.

© Dunod – La photocopie non autorisée est un délit

RIP distingue deux types d'équipement : les actifs et les passifs. Les premiers diffusent périodiquement leurs routes vers les autres nœuds tandis que les seconds écoutent et mettent simplement leur table à jour en fonction des informations reçues. Un routeur fonctionnant en mode actif envoie toutes les 30 secondes un message de diffusion pour signaler qu'il connaît une route pour accéder à un réseau et en signale le coût en nombre de sauts.

RIP v1 présente plusieurs inconvénients. Il ne contient aucune information sur le masque de sous-réseau, par conséquent le routeur doit, d'une part, disposer localement de cette information et, d'autre part, le masque de sous-réseau doit être identique sur tout le réseau. Il ne supporte pas le trafic *multicast*.

Dans les grands réseaux, la diffusion des tables toutes les 30 s induit un trafic important et un temps de convergence (stabilisation des tables) conséquent qui peut être de plusieurs minutes. Pour limiter ce temps, la visibilité d'un routeur est limitée à 15 sauts, une métrique de 16 représente une route non joignable. Il n'y a pas d'accusé de réception des messages. Si un routeur ne reçoit aucun message durant 180 s, la route silencieuse est déclarée inaccessible (coût = 16). Lorsqu'un routeur est arrêté par la procédure normale d'extinction, il envoie, à ses voisins, sa table avec tous ses liens à 16. Cette procédure permet une convergence plus rapide vers la nouvelle situation. D'autres solutions sont mises en œuvre pour améliorer la convergence et éviter les boucles :

– *Split horizon* ou horizon coupé, les données de routage ne sont pas renvoyées vers le nœud d'où on les a apprises ;
– *Poison reverse*, qui complète le *split horizon*. Si, après avoir détecté une route coupée, un routeur reçoit une information d'accessibilité avec un coût important par rapport au coût initial, il ignore cette information. Il estime alors que le message lui est revenu par une boucle.

Lorsqu'une nouvelle route est annoncée, si le routeur contient déjà une entrée de même coût dans sa table, il ignore cette information. De ce fait, non seulement RIP ne peut faire d'équilibrage de charge mais, dans un réseau maillé, le chemin est dépendant de l'ordre de mise en marche des routeurs.

Les messages ne sont pas authentifiés. Il est alors possible à un individu malveillant de générer des messages RIP avec des coûts tels que toutes les routes passent par un même routeur. Le nœud ainsi attaqué devient alors un véritable goulet d'étranglement, le réseau peut ainsi être complètement paralysé (congestion).

La taille maximale d'un message RIP (figure 19.23) est de 512 octets de charge utile, auxquels il convient d'ajouter 28 octets pour l'en-tête UDP (port 520) et IP.

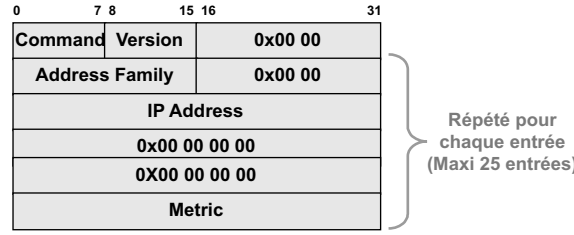


Figure 19.23 Le message RIP v1.

Cette taille limite le nombre d'entrées dans un message à 25. Le message comporte les informations suivantes :

– le champ *Command* permet de distinguer les différents types de message :

1) *Request*, qui permet de demander à un système distant d'envoyer tout ou partie de sa table de routage. Ce message permet, à un routeur, lors de son démarrage d'acquérir rapidement les informations de routage sans attendre une diffusion ;
2) *Response*, message contenant tout ou partie d'une table de routage. Ce message peut être envoyé en réponse au message précédent (*Request*), ou lors d'une simple mise à jour périodique ;
3) et 4) *Traceon* et *Traceoff*, ces messages aujourd'hui obsolètes, doivent être ignorés ;
5) réservé à Sun Microsystems ;
6) réservé à d'éventuelles nouvelles commandes ;

– le champ *Version* identifie la version du protocole, il doit être mis à 1 ;
– l'ensemble des champs suivants contient les informations en relation avec les routes :
  – *Address Family* identifie la famille d'adresse, cette valeur est à 2 pour IP. Toute autre valeur doit être ignorée. Les deux octets suivants doivent être mis à zéro ;
  – *IP Address* contient l'adresse IP d'un réseau, d'un sous-réseau ou d'une station ou un routeur par défaut (0.0.0.0) ;
  – les deux champs suivants doivent être mis à zéro ;
  – *Metric* indique, en nombre de sauts, la distance du réseau IP identifié précédemment. La valeur maximale est de 15.

Le protocole **IGRP** (*Interior Gateway Routing Protocol*) de Cisco remédie à de nombreux inconvénients de RIP. Dans RIP, le coût est représenté par le nombre de sauts, une voie plus rapide (débit) est ignorée si le nombre de sauts est plus important. IGRP utilise une métrique, configurable par l'administrateur, qui permet de privilégier un lien :

$$M = F \times \left(\frac{k_1}{D \times (1 - C)} + \frac{k_2}{T} \right)$$

Avec M : valeur de la métrique,
F : coefficient indiquant la fiabilité de ligne, la valeur 255 indique un taux de perte de 100 %,
D : débit du lien,
C : charge du lien,
T : somme des temps de traitement, d'émission et de propagation d'un datagramme,
Les coefficients k_1 et k_2 sont des facteurs de pondération fixés par l'administrateur, ils peuvent être modifiés dynamiquement en fonction de la valeur du champ TOS (*Type Of Service*).

IGRP permet en outre, la prise en compte des masques de sous-réseaux, le partage de charge et la limitation des domaines de diffusion en introduisant la notion de systèmes autonomes.

RIP v2 (RFC 1721 à 1724)

Mettant à profit les champs non utilisés de RIP v1, RIP v2 remédie à certains inconvénients de RIP v1 tout en restant compatible avec lui. RIP v2 permet de diffuser le masque de sous-réseau (*Subnet Mask Field*). Un champ d'authentification peut être inséré entre l'en-tête RIP et la première entrée.

© Dunod – La photocopie non autorisée est un délit

Ce champ est repéré par la valeur « *Address Family ID* » à 0xFFFF. La figure 19.24 compare le format du message RIP v1 et RIP v2 avec authentification simple.

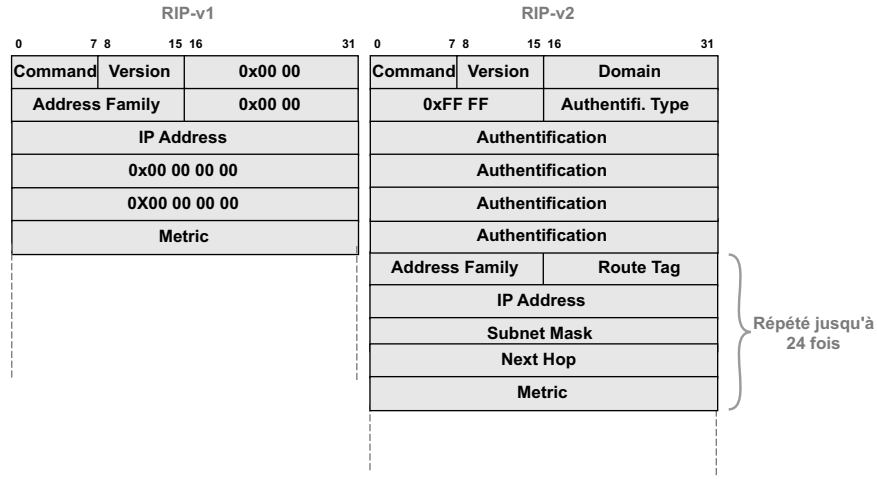


Figure 19.24 Le format des messages RIP v2.

Le champ *Type authentification* à 0x0000 indique qu'il s'agit d'une authentification simple, suit alors le mot de passe en clair sur 16 octets. Un autre format, plus complexe, permettant de crypter le mot de passe est aussi défini.

Le champ *Domain* permet de subdiviser le réseau en différents réseaux logiques. Les routeurs ignorent les messages émanant d'un domaine autre que le leur. Le champ *Address Family* a la même signification. Cependant, le nouveau champ *Route Tag* pourra être utilisé en conjonction avec un protocole de routage externe (EGP). Le champ *Next Hop* identifie le routeur d'origine, mais il permet aussi de forcer une route vers un autre routeur.

RIP-v2 peut fonctionner en mode *broadcast* et en mode *multicast*. L'utilisation du mode *multicast* permet, dans un environnement mixte, aux routeurs RIP-v1 d'ignorer les messages adressés à l'adresse *multicast* 224.0.0.9.

Si RIP-v2 pallie de nombreuses insuffisances de RIP-v1, sa portée, toujours limitée à 15 sauts, le destine aux petits et moyens réseaux.

19.3.3 Le routage à état des liens (OSPF)

Généralités

Contrairement au protocole à vecteur distance, le protocole à état des liens ne diffuse, sur le réseau, que les modifications qu'il a détectées dans la topologie du réseau : lien inaccessible, coût modifié... Chaque nœud entretien une base de données qui est le reflet total de la cartographie du réseau. Cette vision globale, par chaque routeur, du réseau permet d'éviter la formation de boucles. Le coût de la liaison (métrique) est configurable interface par interface, plusieurs métriques peuvent être utilisées simultanément (longueur de la file d'attente, débit, distance...). À partir de ces éléments, chaque routeur calcule la route de moindre coût selon l'algorithme de Dijkstra.

OSPF (*Open Shortest Path First*) est capable d'assurer un routage par type de service (champ TOS du datagramme IP), il peut aussi assurer l'équilibrage de charge entre plusieurs routes de même coût. Lorsque le réseau est important, la diffusion des messages et la détermination de la nouvelle table de routage pénalisent les performances globales du réseau. Aussi, OSPF a introduit la notion d'aire limitant ainsi l'espace de diffusion et le volume de calcul à effectuer.

La notion d'aire de routage

Une aire ou zone (*Area*) correspond à une subdivision logique d'un réseau OSPF (figure 19.25). Il est important de ne pas confondre la notion d'aire d'OSPF avec celle de système autonome (**AS**, *Autonomus System*). Un AS est constitué d'un ou plusieurs réseaux sous la responsabilité administrative d'une même autorité administrative. Les protocoles de routage utilisés dans chacun des AS peuvent être différents, un protocole spécifique (**EGP**, *External Gateway Protocol*) gère l'échange d'information entre les différents AS alors que les différentes aires OSPF utilisent toutes le protocole OSPF.

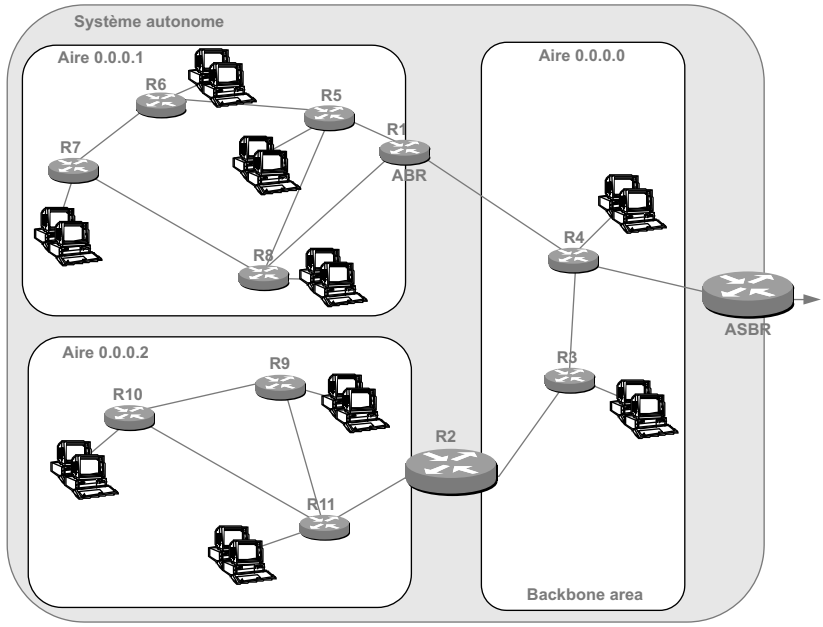


Figure 19.25 Les aires OSPF.

La hiérarchie introduite par OSPF est limitée à deux niveaux. L'environnement OSPF comprend les éléments suivants :

– une zone dite fédératrice (*Area backbone*) assure l'interconnexion de toutes les autres zones. Chaque zone est identifiée par un numéro de zone unique sur 32 bits, ce numéro est un identifiant et non une adresse IP, même si parfois on se sert de l'adresse IP comme identifiant. Le numéro 0.0.0.0 identifie la zone fédératrice. Le *backbone* assure l'acheminement inter-zone. Lorsqu'un réseau OSPF ne comporte qu'une seule zone, cette zone est obligatoirement la zone 0.0.0.0 ;

© Dunod – La photocopie non autorisée est un délit

– des routeurs de zone ou *Internal Router* (**IR**), ces routeurs n'annoncent que les routes internes à leur zone. En principe, on limite une zone à 50 routeurs maximum ;
– des routeurs qui assurent la connexion au *backbone*, et qui annoncent les routes extérieures à la zone. Ainsi, sur la figure 19.25, il s'agit du routeur R1 (**ABR**, *Area Boundary Router*), le routeur R2 qui correspond à une interface locale entre la zone 2 et la zone 0 est considéré comme appartenant au *backbone* ;
– des routeurs frontières de système autonome (**ASBR**, *Autonomous System Boundary Router*). Ces routeurs assurent l'échange d'information avec les autres systèmes autonomes. Les routes extérieures au système autonome sont apprises par des protocoles autres qu'OSPF (routage statique, EGP, BGP...)

La réduction du nombre de routeurs par zone de diffusion limite le trafic de gestion mais les échanges entre routeurs sont encore nombreux. Pour limiter ce trafic, OSPF introduit la notion de routeur désigné (**DR**, *Designated Router*). C'est ce dernier qui assure la diffusion des messages vers les routeurs de la zone ce qui ne nécessite que *N* messages (1 message vers le DR et *N*–1 messages du DR vers les hôtes). L'élection du routeur désigné est similaire à celle du moniteur du réseau Token Ring. Dans les réseaux **NBMA** (*Non Broadcast Multiple Access*), il faut configurer chaque routeur avec la liste des adresses des routeurs de l'aire et leur priorité.

L'administrateur réseau affecte une priorité (0 à 255) à chaque routeur. Pour une zone donnée, c'est le routeur de plus haute priorité qui est désigné. Un routeur de priorité 0 ne pourra jamais être élu routeur désigné. En cas d'égalité, c'est le routeur de plus grand identificateur qui est élu. L'identificateur est en principe l'adresse IP qui désigne le routeur. Un routeur désigné de *backup* est aussi élu. Lorsqu'un routeur est mis sous tension, il écoute le trafic et apprend ainsi quel est le routeur désigné et son *backup*. Il accepte, même si sa priorité est plus grande, ces informations. C'est l'absence de trafic en provenance du routeur désigné qui permet de détecter sa panne et de déclencher le mécanisme d'élection.

L'agrégation de routes

L'utilisation de zones offre un mécanisme puissant d'affectation des adresses IP. Si tous les réseaux ou sous-réseaux d'une zone ont des adresses IP contiguës, le routeur ne signale qu'une seule route aux autres routeurs. Cette propriété permet d'une part de minimiser le trafic d'annonce et, d'autre part, d'alléger les tables de routage La figure 19.26 illustre ce principe.

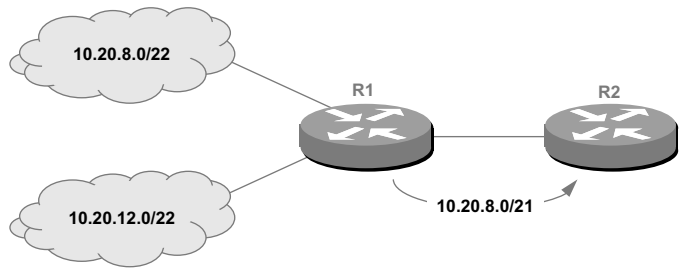


Figure 19.26 L'agrégation de routes dans OSPF.

En routage vecteur distance, les deux sous-réseaux de la figure 19.26 seraient annoncés individuellement et constitueraient 2 entrées dans les tables de routage de R1 et de R2. En OSPF, le routeur R1 considère que les réseaux ont en commun les 21 premiers bits, il n'annonce que cette seule information. Pour éviter d'éventuels conflits, les tables de routage classent en premier les plus grands préfixes.

Le fonctionnement succinct d'OSPF

➤ Généralités

Directement au-dessus d'IP (protocole 87) OSPF utilise des adresses *multicast*, 224.0.0.5 pour adresser tous les routeurs de l'aire et 224.0.0.6 pour communiquer avec le routeur désigné. Tous les messages d'OSPF utilisent le même en-tête de 24 octets (figure 19.27).

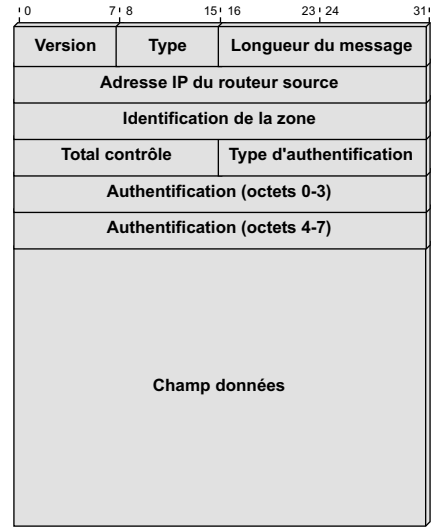


Figure 19.27 L'en-tête des messages OSPF.

Les différents champs sont :

- Version, sur 1 octet, indique la version courante du protocole. La version actuelle est la 2 ;
- Type, sur un octet précise le contenu du champ Données :
  - Type 1, message *Hello* pour déterminer le délai ;
  - Type 2, message de description de la base de données (topologie) ;
  - Type 3, requête d'état de la liaison (*Link state request*) ;
  - Type 4, message de mise à jour de l'état de la liaison (*Link state update*) ;
  - Type 5, acquittement d'un message d'état de la liaison ;
- Le champ Longueur du message indique en octets la longueur du message en-tête compris ;
- Adresse IP de l'expéditeur du message ;
- Identification de zone, numéro d'identification sur 32 bits de la zone (*Area*). Un routeur peut être multidomicilié (*Multi-homed*), c'est-à-dire qu'il peut avoir une interface sur plusieurs aires. Cette information est donc complémentaire de celle de l'hôte ;

© Dunod – La photocopie non autorisée est un délit

– Total de contrôle, calculé de manière similaire au total de contrôle de TCP ;
– Type d'authentification, 0 aucune, 1 mot de passe simple ;
– Authentification, contient un mot de passe en clair sur 8 caractères.

Le fonctionnement d'OSPF peut se décomposer en quatre étapes :
– élection du routeur désigné et de son *backup* ;
– synchronisation des données topologiques ;
– mise à jour des bases de données ;
– calcul du chemin le plus court.

Pour son fonctionnement OSPF met en œuvre trois sous-protocoles :
– le protocole « *Hello* » est utilisé entre deux routeurs adjacents pour synchroniser leur base de connaissance ;
– le protocole d'échange permet, lors de l'initialisation d'un routeur, l'acquisition des entrées de sa base de données ;
– le protocole d'inondation est utilisé par un routeur pour signaler la modification de l'état d'un lien qui lui est rattaché.

➤ Le protocole *Hello*

Le protocole *Hello*[5] permet de vérifier la connectivité entre les nœuds, d'élire le routeur désigné et le routeur *backup*. Un message *Hello* (figure 19.28) est envoyé périodiquement (intervalle *Hello*) pour tester la présence du routeur voisin. En l'absence de réception de message durant une période supérieure à une durée prédéterminée dénommée **intervalle de mort**, la liaison silencieuse est déclarée inaccessible.

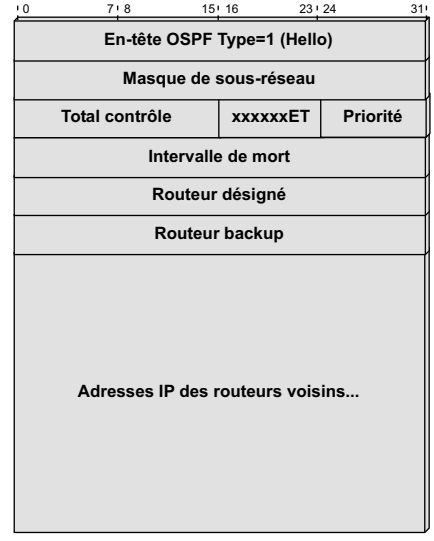


Figure 19.28 Le message Hello.

5. Attention, il ne faut pas confondre le sous-protocole *Hello* d'OSPF avec l'ancien protocole de routage *Hello*, aujourd'hui obsolète.

Dans les réseaux à diffusion, l'élection du routeur désigné se fait par écoute du trafic tandis que dans les réseaux NBMA, le message *Hello* est adressé à chaque routeur éligible (priorité non nulle). Lors de sa mise sous tension, le routeur ne connaît pas le routeur désigné, les champs Routeur désigné et *backup* sont mis à 0 (0.0.0.0). Si un routeur désigné et son ***backup*** existent, ceux-ci seront acceptés comme routeur désigné et *backup* par ce nouveau routeur même si il a une sa priorité est plus forte qu'eux.

Le message *Hello* contient la liste des routeurs identifiés par écoute ou réception des messages *Hello*. Lorsque dans la liste un routeur reconnaît sa propre adresse, il en déduit que la connectivité avec ce voisin est complète (connectivité bilatérale).

Le champ Options décrit les options supportées par le routeur. Seuls 2 bits sont utilisés. Le bit E à 1 indique que le routeur émet et reçoit des routes externes. Ce bit doit avoir la même valeur pour les deux routeurs d'extrémité d'une même liaison. Le bit T informe que le routeur a la possibilité de prendre en compte le champ TOS des datagrammes IP et de router en fonction de celui-ci.

➤ Le protocole d'échange

Après découverte de ses voisins, le routeur doit initialiser sa base de données topologiques. À l'aide des différentes informations fournies, il construit les entrées de la table (liste des liens et routeurs responsables de la mise à jour des valeurs d'état ou coût). Ces entrées lui permettront de construire une liste de demandes d'état de liens. Par la suite, les différents champs de la base seront maintenus à jour par le protocole d'inondation.

L'échange peut avoir lieu entre routeurs adjacents ou avec le routeur désigné. Durant cette phase le routeur ayant initialisé l'échange est déclaré maître (*Master*) et l'autre esclave (*Slave*). En cas de collision d'initialisation, c'est le routeur de plus grand identifiant qui est choisi. La figure 19.29 représente le format du message (message OSPF de type 2).

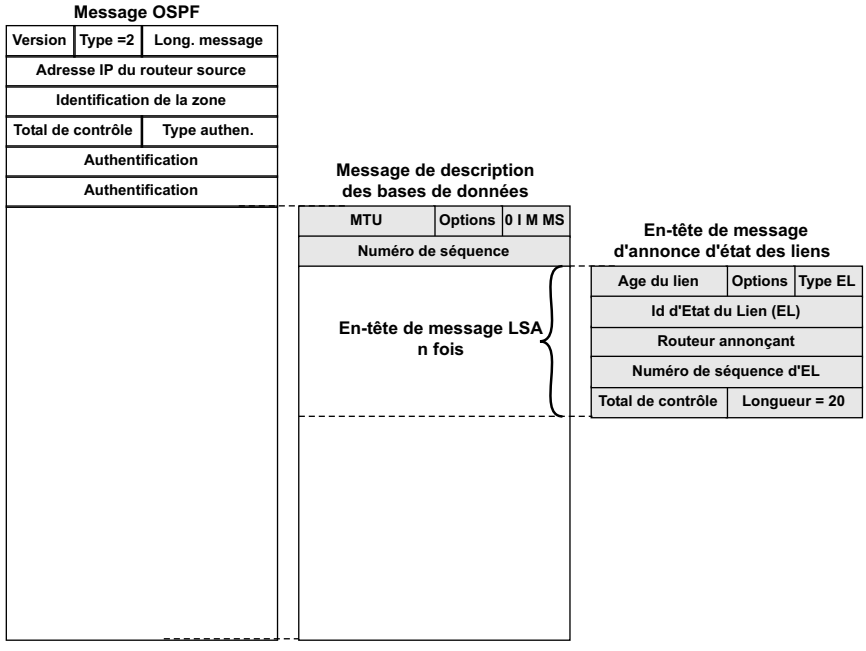


Figure 19.29 Le message de description de la base de données.

© Dunod – La photocopie non autorisée est un délit

Le champ MTU informe le routeur de la taille maximale des datagrammes supportée sur le lien. Le champ Option est identique à celui du message *Hello*. Dans le champ suivant, le bit *I* à 1 indique qu'il s'agit du premier message de description (*Initialize*), le bit *M* (*More*) informe que un ou des messages suivent ; tandis que le bit *MS* (*Master/Slave*) à 1 indique que l'émetteur est le maître. Le numéro de séquence permet de contrôler l'échange, seul le maître l'incrémente de 1 à chaque message envoyé. L'esclave recopie ce numéro dans son message d'acquittement (message de description de sa base de données avec le bit *MS* = 0, ce message pouvant éventuellement être vide).

Vient, ensuite, la description des entrées de la table des liaisons. Ce descriptif est en fait l'en-tête des messages d'annonce de l'état d'une liaison (**LSA**, *Link State Advertissement*). Chaque lien y est décrit très précisément. Le champ Age du lien indique en secondes le temps écoulé depuis la première annonce du lien. Le champ option est identique à celui du message *Hello*. L'information type d'état du lien (**EL**) peut prendre cinq valeurs selon la nature du routeur annonçant :

- Type 1 (*Router Link*), le routeur annonçant est un routeur interne à l'aire, le champ ID de l'état des liens indique son identifiant. Dans les messages d'état des liens, cet en-tête est suivi de la liste des liens et de leurs caractéristiques (voir figure 19.30) ;
- Type 2 *(Network Link*), le routeur est un routeur interne d'un réseau NBMA (sans diffusion), l'identifiant d'état des liens est alors l'adresse du routeur désigné. Dans les messages d'état des liens, cet en-tête est suivi de la liste des routeurs qui ont établi une relation de voisinage avec le routeur désigné ;
- Type 3 (**ABR**, *Area Boundary Router*), il s'agit alors d'un routeur de bordure d'aire, l'ID d'état des liens contient l'adresse IP du lien annoncé. Dans les messages d'état des liaisons, cet en-tête est suivi de la liste des routeurs de la zone accessibles par cette voie et le masque de sous-réseau associé ;
- Type 4, ce type de message est similaire au précédent mais s'adresse à un routeur d'aire terminale ;
- Type 5 (**ASBR**, *Autonomous System Boudary Router*), le routeur est en bordure de système autonome. L'ID d'état des liaisons correspond à l'adresse IP de la liaison. Dans les messages d'état des liaisons, cet en-tête est suivi de la liste des liens connus et de leurs caractéristiques.

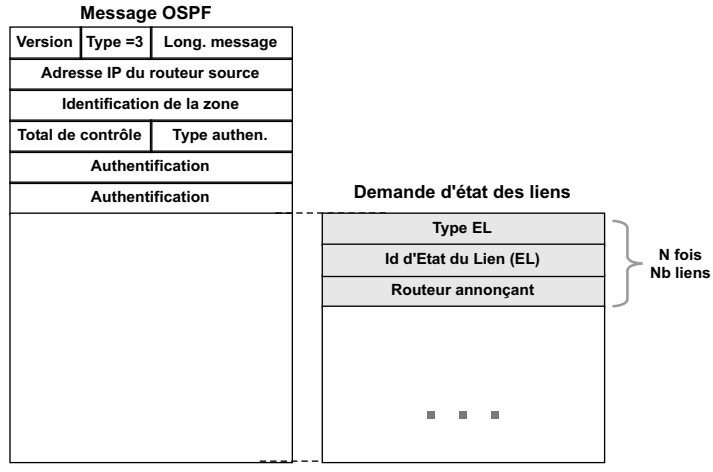


Figure 19.30 Le message de demande d'état des liens.

Dans les différents messages échangés, l'association de l'identifiant du routeur annonçant (celui à l'origine des informations concernant ce lien), de l'identifiant d'état des liens et du type d'état des liens distingue de manière unique un enregistrement. Le champ Numéro de séquence identifie une annonce. Le total de contrôle porte sur tout le message d'annonce d'état d'un lien. Dans le message de description de la base de données, le champ Données étant absent, le total de contrôle ne porte que sur les 20 octets d'en-tête LSA.

Chacun des routeurs participant à l'échange construit, pour les liens dont il n'a pas le descriptif ou pour lesquels l'information est trop vieille, une liste d'état des liens à demander. La structure de ce message (OSPF type 3) est représentée figure 19.30, la signification des champs est identique à celle du message de description de la base de données.

Le routeur cible renvoie un message de mise à jour des liens (*Link state update*) dont le contenu dépend du type d'état des liens. Les messages de mise à jour de l'état des liens des types EL = 1 décrivent les liens, les messages LSA des types EL = 2, 3, 4 donne une liste de réseaux et les masques associés, le type EL = 5 décrivent les liens externes. La figure 19.31 donne le format d'un message de mise à jour pour un EL de type 1.

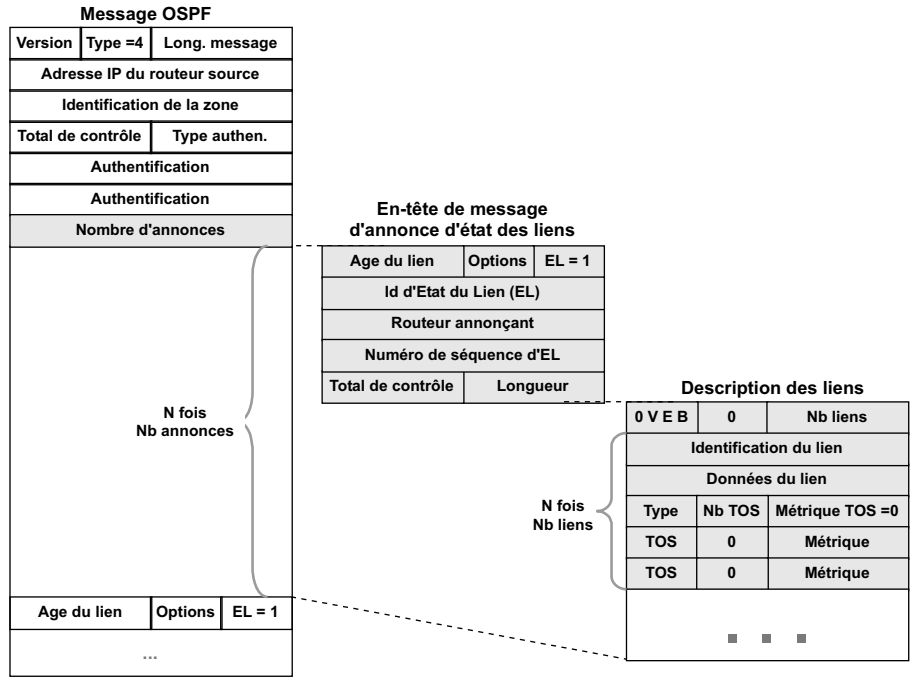


Figure 19.31 Le message d'annonce d'états des liens (EL = 1).

L'en-tête de description d'un lien précise la nature du routeur annonçant (bit **V** pour *Virtual*, routeur en extrémité d'un lien virtuel ; bit **E** pour *External*, routeur en frontière d'un système autonome ; **B** pour *Border*, routeur en bordure d'aire). Le champ significatif suivant indique le nombre de liens décrits pour ce routeur. La figure 19.32 indique, en fonction de la valeur du champ *Type*, la signification du champ d'identification du lien et du champ Données du lien. Enfin, la métrique est indiquée.

© Dunod – La photocopie non autorisée est un délit

Type	Type de lien décrit	ID du lien	Données du lien
1	Lien point à point vers un autre routeur	Identification du routeur distant (généralement son adresse IP)	Adresse IP de l'interface
2	Connexion à un réseau de transit	Adresse IP du routeur désigné	Adresse IP de l'interface
3	Connexion à un réseau terminal	Adresse du réseau IP	Masque de sous-réseau
4	Lien virtuel	Identification du routeur distant	Adresse IP d l'interface

Figure 19.32 La signification des champs Identification et Données du lien.

OSPF peut gérer plusieurs tables de routage et router en fonction du TOS. Les routeurs qui ont cette possibilité positionnent à 1 le bit T de l'en-tête du message d'état des liens (champ option). La partie descriptive du message d'état des liens fournit, pour chaque lien, une métrique par TOS géré. Le routage sera déterminé selon la valeur du champ TOS du datagramme IP (figure 19.33).

Codage OSPF	Valeur des bits du champ TOS				Description du service invoqué
	Délai	Débit	Fiabilité	Coût	
0	0	0	0	0	Service normal
2	0	0	0	1	Minimiser le coût financier
4	0	0	1	0	Maximiser la fiabilité
8	0	1	0	0	Maximiser le débit
16	1	0	0	0	Minimiser le délai

Figure 19.33 Le service et la valeur du TOS (Datagramme IP).

Si un routeur n'a pas la possibilité de router en fonction du TOS, il ne participera au routage des datagrammes qui invoquent un service en fonction du TOS. OSPF ne précise pas la manière dont sont calculées les métriques. L'administrateur du réseau peut ainsi privilégier tel ou tel lien, voire interdire un lien. Par exemple, si on ne veut pas que les données transitent *via* un réseau facturé au volume, il suffit de porter la métrique de ce lien à 65 535. En principe, la métrique d'un lien en fonction du débit correspond au temps mis pour transmettre un volume de 10^8 bits (Métrique = 10^8/Débit de l'interface).

Les messages *Link status update* sont acquittés par message OSPF de type 5. La figure 19.34 décrit ce message. La signification des champs est identique à celle déjà fournies.

À l'aide de ces informations, chaque routeur établit une arborescence du chemin le plus court (*Shortest Path Tree*) où il est la racine de l'arbre (algorithme de Dijkstra). Sur la base de cette arborescence, il génère sa ou ses tables de routage.

➤ Le protocole d'inondation

À chaque changement d'état d'un lien, le routeur qui en a la charge (routeur annonçant) émet un message d'avertissement d'état d'un lien (LSA, OSPF type 4, figure 19.31). Chaque routeur recevant ce message compare le numéro de séquence des liens qu'il a en mémoire et le numéro de séquence de l'annonce. Si l'annonce est plus récente, il la retransmet sur toutes ses interfaces, sauf celle par laquelle il l'a reçue et acquitte ce message (OSPF type 5, figure 19.34). Tout message reçu doit être acquitté. L'acquittement peut être implicite. Si l'annonce est faite vers le routeur désigné, celui-ci retransmet à tous les routeurs (adresse de diffusion) le message. La réception de ce message en provenance du routeur désigné vaut acquittement.

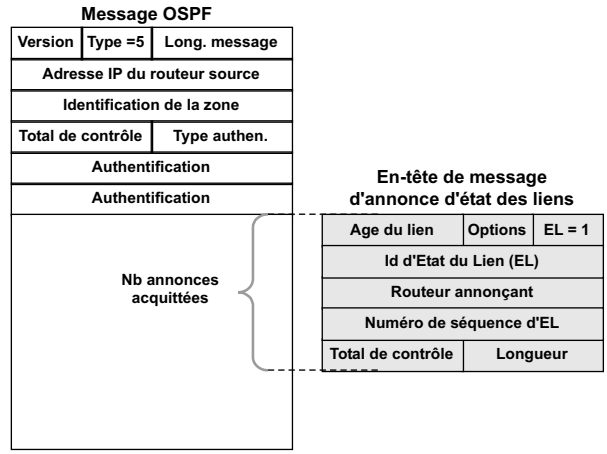


Figure 19.34 Le message d'acquittement d'annonce d'état des liens.

Conclusion

OSPF est un protocole de routage complexe. Complexe dans sa mise en œuvre (plan d'adressage, initialisation des métriques...), complexe dans son fonctionnement (temps de calcul...). Bien qu'OSPF remédie aux principaux inconvénients de RIP (temps de convergence, boucle...), le monde des réseaux d'entreprise est encore largement dominé par des protocoles du type vecteur distance, que ceux-ci soient normalisés (RIP) ou d'origine constructeur comme **IGRP** (*Interior Gateway Routing Protocol*) et **EIGRP** (*Enhanced Interior Gateway Protocol*) de chez Cisco.

Le choix, pour une entreprise de tel ou tel protocole de routage est un choix stratégique. Quelles que soient les qualités des protocoles propriétaires, ils sont et demeurent propriétaires ce qui constitue un handicap lors de l'évolution du réseau ou du renouvellement des équipements.

19.3.4 Le routage inter-domaine

Un système autonome (AS) correspond à un domaine de routage sous le contrôle d'une autorité d'administration unique. Les différents systèmes autonomes composant l'Internet doivent s'échanger leurs informations d'accessibilité. Ainsi, chacun des routeurs de bordure des deux systèmes autonomes de la figure 19.35 doit d'une part établir une connectivité et, d'autre part, informer son voisin des réseaux qu'ils savent atteindre.

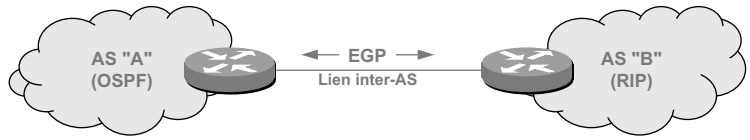


Figure 19.35 La connectivité de deux systèmes autonomes.

Ainsi, le routeur de bordure de l'AS « A » annonce au routeur de bordure de l'AS « B » par l'intermédiaire d'un protocole de routage inter-domaine (**EGP**, *External Gateway Protocol*) les informations (liste d'accessibilité) qu'il a acquises, par un protocole de routage intra-domaine (**IGP**,

© Dunod – La photocopie non autorisée est un délit

Interior Gateway Protocol), sur les réseaux accessibles par transit dans sa zone. Le routeur B va diffuser ces informations au format de l'IGP utilisé dans sa zone.

Le protocole de routage externe doit résoudre de nombreux problèmes spécifiques. Le premier concerne le routage politique. Supposons qu'une entreprise internationale dispose d'un réseau privé. Afin de minimiser le trafic sur son réseau, elle dispose d'un accès à Internet dans chacun des pays desservis par son réseau (figure 19.36). Cette entreprise s'oppose évidemment à ce que le trafic Internet transite par son réseau.

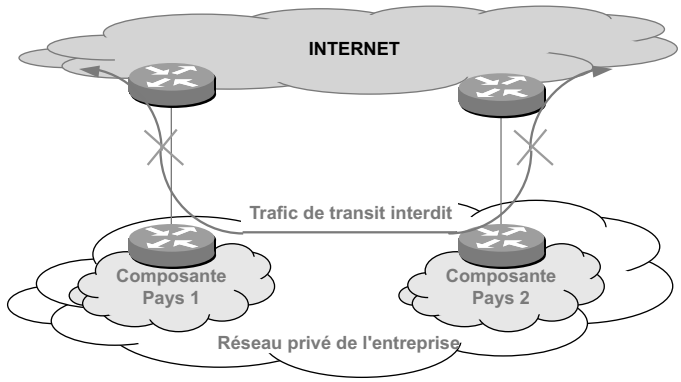


Figure 19.36 Problématique du routage politique.

Le second problème, mis en évidence par la figure 19.35, concerne les métriques. Quelle métrique utiliser dans les annonces puisque chacun des AS peut utiliser un protocole de routage interne différent et transparent à l'EGP ? Le coût annoncé est donc forfaitaire (distance arbitraire), ce qui permet aux administrateurs de favoriser le transit par tel ou tel réseau en fonction d'accords commerciaux ou autres, répondant ainsi à la préoccupation précédente.

De nombreux protocoles de routage externes ont été testés. Actuellement Internet met en œuvre **BGP 4** (*Border Gateway Protocol*). Les informations de routage échangées comprennent : le numéro de système autonome, la liste des réseaux de chaque système autonome, la distance relative vers chacun des sous-réseaux de l'AS et l'adresse IP du routeur d'accès à ces réseaux. BGP prend en compte des critères extérieurs aux domaines de routage (routage politique), il met en œuvre des mécanismes de détection et de suppression des boucles. BGP utilise quatre types de messages :

– les messages d'ouverture, utilisés lors de l'ouverture d'une session BGP entre deux routeurs, ils contiennent le numéro d'AS du système autonome émetteur et le délai au bout duquel, si le destinataire ne reçoit aucun message, il doit considérer le routeur source comme défaillant ;
– les messages de mise à jour, utilisés pour signaler, au routeur BGP voisin (*Peer router*) le changement d'état d'une ou plusieurs routes gérées par le routeur source (nouvelle route ou route devenue inaccessible) ;
– les messages de notification, utilisés pour clore une session BGP. Ils indiquent le motif de la fermeture de session ;
– les messages *Hello* (*Keep Alive*), ils ne contiennent aucune information, et sont utilisés par un routeur pour signaler, en l'absence de trafic, sa présence au routeur *peer*.

19.4 NOTIONS DE QUALITÉ DE SERVICE

19.4.1 Généralités

La notion de qualité de service (**QoS**, *Quality of Service*) recouvre un ensemble de techniques destinées à offrir de bout en bout aux applications le service dont elles ont besoin. Elle recouvre généralement deux aspects : l'aspect temporel (délai d'acheminement) et l'aspect sémantique (perte de données), qui s'expriment selon quatre paramètres : bande passante (débit), délai de transfert, variation de ce délai (gigue) et enfin fiabilité.

La qualité de service constitue un axe de recherche majeur dans les réseaux. Deux approches ont déjà été étudiées : la réservation de ressource (réseaux à état) et la prioritisation des flux (réseaux sans état). ATM et Frame Relay appartiennent à la première catégorie, ils mettent en œuvre des mécanismes de contrôle d'admission pour garantir ainsi à chaque nouvelle connexion qu'un service minimal lui sera rendu. En ce qui concerne les réseaux IP, aucun état n'est maintenu dans le réseau (réseau datagramme ou *best effort*), dans ce contexte seule l'approche de prioritisation semble possible.

Conçu à une époque où les seuls flux applicatifs à acheminer étaient tous de même nature (texte), IP n'implémentait qu'un mécanisme simple, aujourd'hui obsolète, de qualité de service défini selon les 3 bits, D (*Delay*), T (*Troughput*) et R (*Reliability*) du champ TOS. Le champ TOS a été redéfini par la RFC 1812 (*IP Precedence*[6]). Le traitement dans un réseau de flux sensibles au temps de transfert comme le trafic SNA et les applications multimédias a montré la nécessité de définir des mécanismes spécifiques pour garantir à chaque type de flux une certaine qualité de service. Deux approches de la QoS sont actuellement définies : *Integrated Services* (**IntServ**, RFC 1633) et *Differentiated Services* (**DiffServ**, RFC 2474).

19.4.2 *Integrated Services*

Le modèle *IntServ* (services intégrés) tend au respect de l'intégrité des flux, c'est une transposition des techniques de **CoS** (*Class of Services*) des réseaux à état dit dur (*hard-state*) tels que ATM et Frame Relay. IntServ ne définit qu'un état dit mou (*soft-state*) *via* un protocole de signalisation (**RSVP**, *Resource reSerVation Protocol*). Un réseau à état mou est un réseau qui maintient un contexte durant un certain temps. En l'absence de renouvellement périodique, cet état est détruit. IntServ définit 3 types de service invoqués par le protocole RSVP :

- un service garanti (*Guaranteed services*), similaire au service CBR (*Constant Bit Rate*) et VBR-rt (*Variable Bit Rate real-time*) d'ATM ;
- un service contrôlé (*Controlled load*) qui correspond au service ABR (*Available Bit Rate*) avec un minimum garanti d'ATM (*Guaranteed minimum cell rate*) ;
- un service *best effort*, assimilable à l'UBR (*Unspecified Bit Rate*) d'ATM.

RSVP reste dans la philosophie du protocole IP. En effet, si RSVP permet de décrire un état dans un routeur (*soft-state*), il ne crée pas pour cela une connexion (*Hard-state*). Si le réseau n'a pas la capacité de garantir la qualité de service invoquée, ATM ou Frame Relay refusent la connexion, ce n'est pas le cas de RSVP, le flux sera traité en *best effort*. La figure 19.37 illustre le principe de RSVP. La source (**A**) émet un message contenant les références du flux (adresse IP source

6. Voir chapitre 10, § 10.2.

© Dunod – La photocopie non autorisée est un délit

et destination, port source et destination, protocole), un contexte d'acheminement est mémorisé (message RSVP *Path*) mais aucune ressource n'est allouée. Elles le seront par le destinataire (**B**) dans un message de réponse RSVP *Resv*.

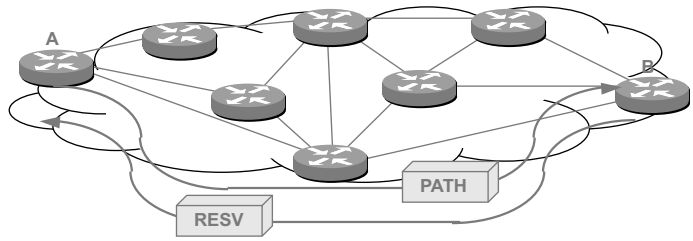


Figure 19.37 La réservation de ressources sous RSVP.

L'approche *Integrated Services* peut être considérée comme une adaptation dans le mode datagramme des techniques orientées connexion. Chaque application formule une demande de réservation de ressource de bout en bout. Le modèle IntServ et RSVP, compte tenu de sa complexité, n'est pas adapté aux grands réseaux des opérateurs, il n'a connu qu'un développement limité dans les réseaux privés.

19.4.3 *Differentiated Services*

Principe

L'approche *DiffServ* (services différenciés) est plus conforme à l'approche IP. *DiffServ* implémente un mécanisme de partage de bande passante en introduisant la notion de politique d'acheminement en fonction d'une classe de service (RFC 2474, *Differentiated Service* ou *Diffserv*). Les flux ne sont plus traités individuellement comme dans *IntServ*, mais sont affectés à une classe de service identifiée par un champ spécifique *Differentiated Services Field* (**DSF**). Tous les flux d'une même classe sont traités de la même manière dans le réseau dit traitement par saut (**PHB**, *Per Hop forwarding Behaviour*). Le champ *DiffServ* remplace le champ TOS d'IPv4 et le champ Classe de Service d'IPv6. La figure 19.38 rappelle la structure de chacun de ces champs.

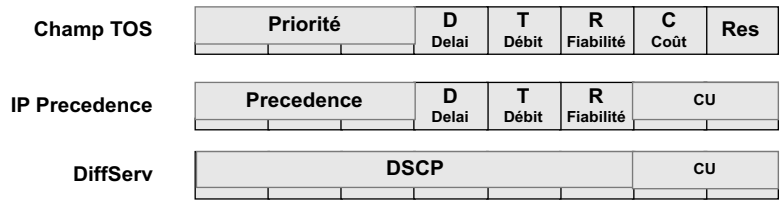


Figure 19.38 Les champs TOS, IP Precedence et DiffServ.

Diffserv répartit le trafic en trois classes de service (**CoS**, *Class of Service*) :

– *Assured Forwarding* ou *Olympic Service* (RFC 2597), équivalent des services ABR d'ATM, comporte 4 classes, elles-mêmes subdivisées en fonction d'une politique d'écartement (**RED**, *Random Early Drop*) en fonction de l'état du réseau (*Low drop*, *Medium drop* et *High drop*). À chaque classe sont affectées une priorité et une garantie de bande passante (figure 19.39).

– *Expedited Forwarding* ou *Premium Service* (RFC 2598), équivalent aux services CBR et VBR-rt d'ATM et défini spécifiquement pour les applications temps réel, minimise le temps de latence dans le réseau. Celui-ci prend en compte des contraintes fortes en matière de temps de traversée, de variation de celui-ci (gigue) et de pertes de données. L'utilisation de la classe *Premium* doit être limitée au sein du réseau, un abus d'utilisation peut fortement pénaliser les autres types de trafic (champ DSCP = 101DD0).
– *Best Effort*, équivalent du service UBR d'ATM, correspond au trafic traditionnel sur IP sans qualité de service (champ DSCP = 000000).

Classe	Codage DSCP	Valeur DD	Politique d'écartement
1 - Platinium	**001**DD0	01	*Low drop*
2 - Gold	**010**DD0	10	*Medium drop*
3 - Silver	**011**DD0	11	*High drop*
4 - Bronze	**100**DD0		

Figure 19.39 Les classes de services d'Assured Forwarding.

La classification des flux est réalisée à la périphérie du réseau (*Classifier*). Les propriétés du flux sont ensuite analysées (*Metering* ou dimensionnement) en fonction d'un contrat de service préétabli (**SLA**, *Service Level Agreement*). Les datagrammes sont alors marqués (*Marker*) par positionnement du champ **DS Field**. Le trafic différencié ou « colorisé » (*Multiflow Classifier*) est analysé, certains paquets peuvent être retardés (mise en forme du trafic ou *shaper*) voire éliminés pour prévenir un éventuel état de congestion (*Dropper*). Les paquets sont ensuite affectés à une file d'attente spécifique avant d'être transmis sur le réseau (*Forwarding*). La figure 19.40 illustre les mécanismes que nous venons de décrire.

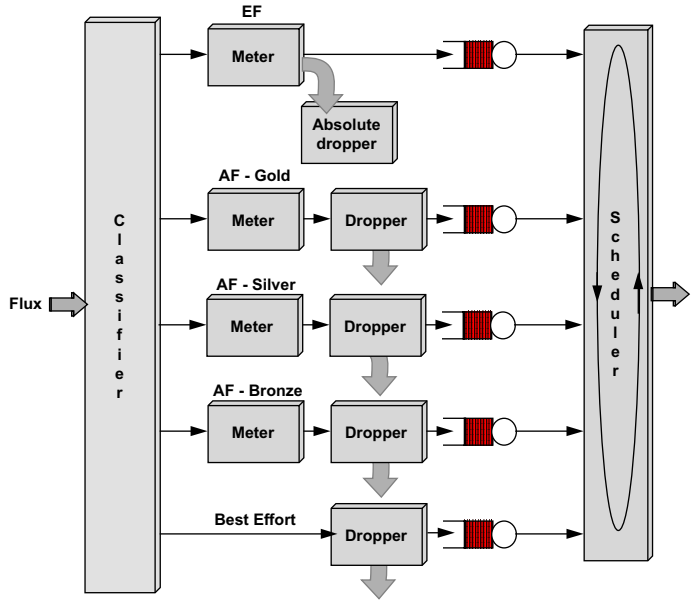


Figure 19.40 Traitement des flux sous DiffServ.

© Dunod – La photocopie non autorisée est un délit

L'architecture *DiffServ* est bien adaptée aux grands réseaux. En effet, les classes de services étant attribuées en périphérie du réseau *DiffServ*, elles ne génèrent ni trafic de gestion, ni surcharge CPU. Cependant, si *DiffServ* permet de hiérarchiser les flux, il ne dispose pas de mécanisme d'information d'état du réseau. De ce fait, les routeurs de bordure ne sont pas en mesure d'anticiper ni de réagir à un état de précongestion ou de congestion.

Notion de gestion des files d'attente dans les routeurs

La qualité de service offerte ne dépend pas seulement de l'attribut de priorité mais aussi des différents mécanismes mis en œuvre dans les routeurs pour gérer les données en attente de traitement. Deux mécanismes aux finalités différentes sont mis en œuvre dans les routeurs. Les mécanismes de gestion proprement dits, qui, en cas de congestion, déterminent comment, au sein d'une même file d'attente, seront éliminés les paquets, et les mécanismes d'ordonnancement qui ont pour objet de distribuer la ressource entre différentes files correspondant chacune à une classe de service différente.

➤ Les mécanismes de gestion des files d'attente

La gestion traditionnelle dite **FIFO** (*First-In, First-Out*) ou premier entré premier servi conduit, lorsque la file est pleine, à la perte de tous les nouveaux paquets entrants. Simple à mettre en œuvre, cette politique de gestion pénalise toutes les sources indifféremment de leur responsabilité dans la congestion. De plus, la régulation du trafic n'intervient que sur débordement, non seulement il n'y pas anticipation mais, la file d'attente étant pleine, le délai moyen de séjour peut être important (file saturée).

En mesurant la taille moyenne de la file d'attente et, dès qu'un certain seuil est atteint, en éliminant de manière aléatoire les paquets, le **RED** (*Random Early Discard*) pénalise d'autant plus un flux que la probabilité qu'un paquet appartenant à ce flux soit présent dans la file est importante. Le RED tente ainsi de réguler le trafic en écartant les paquets des flux les plus responsables d'un état naissant de congestion.

Cependant, le RED n'agit que sur des paramètres de volumétrie, il ne prend pas en compte la priorité des différents flux. À l'instar du RED dont il dérive, le **WRED** (*Weighted RED*), intervient à partir d'un certain seuil de remplissage des files, mais chaque type de flux se voit, en fonction de son niveau de priorité, attribuer un seuil différent.

De nombreuses autres méthodes ont été décrites. Cependant, rappelons que dans un réseau correctement dimensionné aucune élimination de paquets ne doit intervenir.

➤ Les mécanismes d'ordonnancement

Les mécanismes d'ordonnancement visent à garantir un partage équitable de la bande passante (*Fair Queueing*). Le mécanisme le plus simple le WFQ (*Weighted FQ*) réalise une insertion ordonnée en fonction d'un niveau de priorité dans la file d'attente (système à file d'attente unique), celle-ci étant ensuite traitée en mode FIFO.

Les autres méthodes s'appliquent aux systèmes à files multiples, dont le principe de base consiste à lire séquentiellement les différentes files, d'y prélever un paquet et, si une file est vide, de passer à la suivante (figure 19.41).

Ce mécanisme est inéquitable, il accorde d'autant plus de bande passante à une file que les paquets qui y séjournent sont de taille importante. Notamment ce principe est incompatible

avec les flux isochrones (voix...) qui se caractérisent généralement par de petits paquets et une priorité importante ! Le WRR (*Weighted Round Robin*) introduit la notion de priorité et peut offrir en fonction de celle-ci une bande passante différenciée (volume ou temps de lecture d'une file).

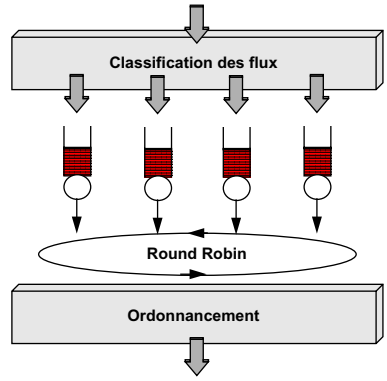


Figure 19.41 Principe du Round Robin.

➤ Mise en œuvre chez les constructeurs

Devant le besoin croissant de qualité de service, et notamment dans les réseaux privés, les constructeurs ont tous implémenté, dans leurs équipements, des mécanismes de QoS plus ou moins proches des solutions retenues par l'IETF et notamment de *DiffServ*.

Cependant, la gestion de la QoS ne crée pas de bande passante, elle la gère au mieux, par conséquent, la stratégie d'attribution d'un niveau de priorité ou d'une partie de la bande passante à tel ou tel flux doit être étudiée avec beaucoup d'attention. La figure 19.42 illustre un tel système de qualité de service.

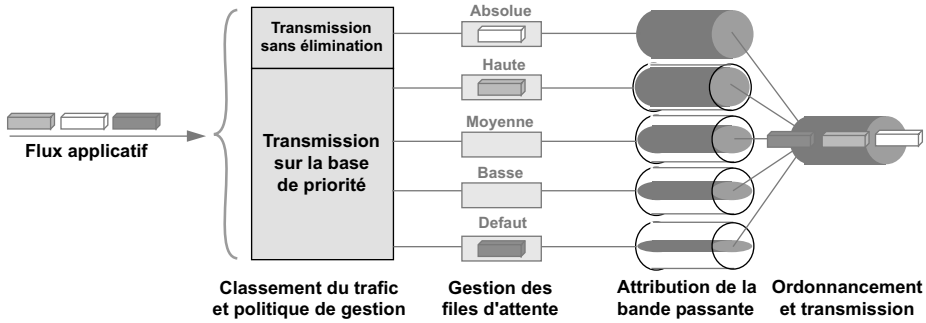


Figure 19.42 Routage fondé sur la notion de priorité.

Dans le système de la figure 19.42, les flux sont acheminés en fonction de deux politiques de gestion de la priorité. La première dite *Priority based forwarding* est attribuée aux flux qui ne doivent subir aucun retard, toute la bande passante du système leur est attribuée (administration du réseau, service voix). Dans la seconde, dite *Credit based wait and forwarding* si des flux plus

© Dunod – La photocopie non autorisée est un délit

prioritaires doivent être écoulés, les autres flux sont éventuellement mis en attente. C'est l'administrateur réseau qui définit, lors de la configuration du système, les critères d'affectation d'un flux à tel ou tel type de traitement et qui alloue toute ou partie de la bande passante à telle ou telle file d'attente.

19.4.4 Mise en œuvre dans les réseaux d'opérateur

La qualité de service est définie par un contrat conclu entre le client et l'opérateur (**SLA**, *Service Level Agreement*), les termes de ce contrat doivent être traduits en règles interprétables par les éléments actifs du réseau (**SLS**, *Service Level Specification*). Deux modèles de politique de gestion de la QoS peuvent être distingués :

– Le ***mode outsourcing*** ou gestion dynamique de la QoS. Lorsque le routeur d'entrée (*Edge router*) dit alors **PEP** (*Policy Enforcement Point*) reçoit un nouveau flux, il sollicite un serveur spécifique le **PDP** (*Policy Decision Point*) afin de déterminer qu'elles sont les règles à appliquer à ce flux. Ce mode de fonctionnement est associé aux réseaux mettant en œuvre un protocole de signalisation de bout en bout comme RSVP dans un réseau MPLS.

– Le ***mode provisionning*** ou gestion statique. Dans ce mode de fonctionnement, c'est le PDP (*Policy Decision Point*) qui, sans y avoir été sollicité, envoie aux PEP (*Policy Enforcement Point*) les règles de gestion permettant de classifier les flux. Ce mode de fonctionnement, propre aux réseaux sans signalisation, correspond à la mise en œuvre des réseaux *DiffServ* (figure 19.43).

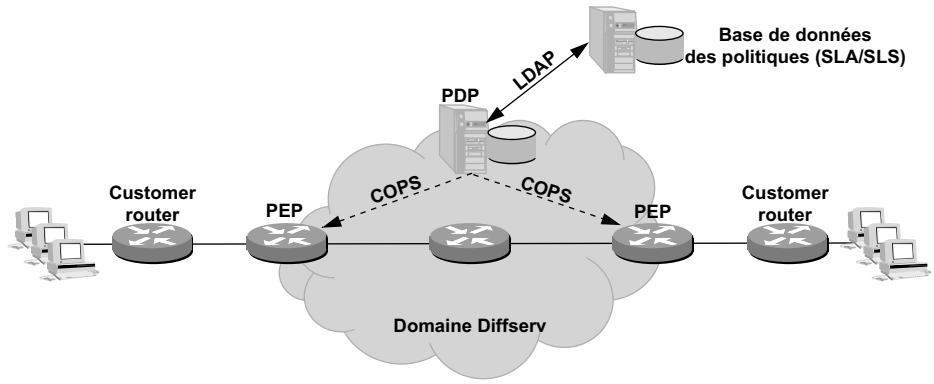


Figure 19.43 Mise en œuvre de la QoS dans un réseau DiffServ.

Le protocole **COPS** (*Common Open Policy Server*) organise les échanges entre les différents acteurs de la QoS (PEP et PDP). Les règles de gestions de la QoS sont stockées dans une base de données, le dialogue entre cette base de données et le PDP utilise le protocole **LDAP** (*Lightweight Directory Access Protocol*).

Dans un environnement multi-opérateur, le contrat, négocié avec son opérateur local (SLA, *Service Level Agreement*) n'est pas connu des opérateurs de réseaux de transit. En principe, chaque domaine *DiffServ* est indépendant et gère les classes de service selon sa propre politique.

Conclusion

Le véritable problème de la qualité de service réside dans la garantie de celle-ci de bout en bout. Or, compte tenu des différentes implémentations des constructeurs, des différentes approches des instances de normalisation et de la liberté de choix de chaque opérateur sur la politique de qualité de service qu'il intègre à son réseau, celle-ci ne peut valablement être garantie que pour des mises en relation qui restent dans le domaine privé ou d'un même opérateur. À titre indicatif, la figure 19.44 indique les correspondances généralement admises entre les différents modes de marquage de la QoS.

Domaine *IntServ*	Domaine 802.1p	Domaine *DiffServ* (DSCP)	
Garanti	5	101DD0	*Premium*
Charge contrôlée	3	011DD0	*Silver*
Best Effort	0	000000	*Best effort*

Figure 19.44 Correspondance entre les différents systèmes de QoS.

19.5 LE *MULTICAST* ET LE ROUTAGE *MULTICAST*

19.5.1 Introduction au *multicast*

L'IP *multicast* est un mécanisme qui permet de diffuser des datagrammes IP vers un ou plusieurs récepteurs sans que ces datagramme soient adressés individuellement à chaque hôte. Les nœuds de destination sont identifiés par une adresse de groupe (adresse *multicast*). Cette technique évite l'envoi de *N* datagrammes *unicasts* aux *N* clients d'une même source d'information.

Dans l'exemple de la figure 19.45, un serveur d'applications vidéo (serveur *multicast*) est raccordé à un réseau IP *multicast*.

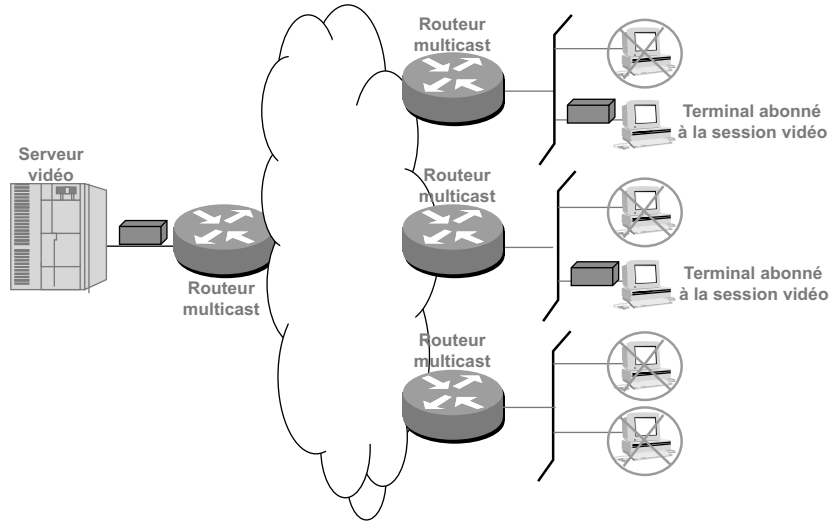


Figure 19.45 Principe d'un réseau multicast.

© Dunod – La photocopie non autorisée est un délit

Pour recevoir les émissions, les machines distantes doivent, au préalable, s'abonner au serveur vidéo. Le mécanisme d'abonnement est spécifique au logiciel serveur, il n'entre pas dans le cadre de notre étude. Les machines abonnées sont membres du groupe *multicast*. Une machine peut être membre de plusieurs groupes. Les informations ne sont diffusées sur les brins locaux que si au moins une machine locale s'est abonnée à un service *multicast*. Dans notre exemple, un seul exemplaire du datagramme est diffusé sur le réseau *multicast*, chaque routeur ayant un client abonné rediffuse le datagramme sur le brin local auquel il est raccordé. Sur le troisième réseau où aucune machine n'a rejoint un groupe de *multicast*, les informations vidéos ne sont pas diffusées.

La diffusion *multicast* nécessite deux protocoles. Le premier doit permettre au routeur local d'apprendre si des clients *multicast* sont actifs sur son brin local, le second doit assurer un routage optimal dans le réseau WAN.

19.5.2 Rappel sur l'adressage *multicast*

L'adressage multicast doit garantir qu'un seul message est diffusé sur le réseau, que le client *multicast* puisse être localisé (@IP *multicast*) et que la station puisse distinguer les messages qui lui sont destinés (@MAC *multicast*).

Des adresses IP *multicast* (classe D) ont été définies pour permettre de distinguer le groupe *multicast* de rattachement. Les applications *multicast* fournissent au coupleur (NIC) les adresses MAC *multicast* auxquelles il doit répondre. Ces adresses sont construites à partir des adresses IP *multicast*. Les adresses MAC *multicast* s'étendent de :

01-00-5E-00-00-00 à 01-00-5E-7F-FF-FF (RFC 1112).

La figure 19.46 rappelle comment, à partir de l'adresse IP *multicast* de la station, est construite l'adresse MAC *multicast*. Les 5 bits de l'adresse IP non utilisés pour former l'adresse MAC permettent, éventuellement, de distinguer 32 groupes *multicast* pour une même adresse MAC *multicast*.

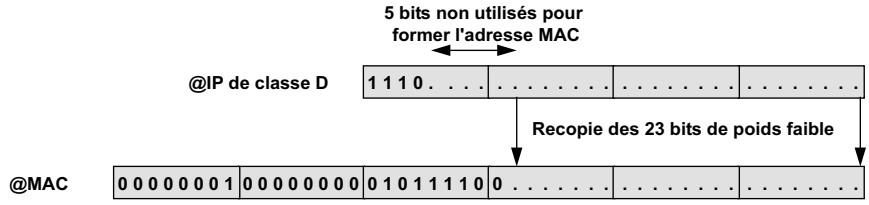


Figure 19.46 Mappage @IP et @IEEE multicast.

Les adresses de groupe les plus connues sont :

– 224.0.0.1, tous les hôtes *multicast* de ce sous-réseau ;
– 224.0.02, tous les routeurs *multicast* de ce sous-réseau ;
– 224.0.0.4, tous les routeurs exécutant le protocole de routage *multicast* DVMRP ;
– 224.0.1.11, applications audio (IETF) ;
– 224.0.1.12, application vidéo (IETF) ;
– 224.0.1.16, diffusion de musique (Music-Service) ;
– 224.0.1.17, *Audionew* (bulletins d'information radio) ;

19.5.3 Le protocole local IGMP (RFC 2236)

Le protocole **IGMP** (*Internet Group Management Protocol*) est le protocole d'apprentissage utilisé par les routeurs *multicast* pour découvrir l'existence, dans les sous-réseaux auxquels ils sont raccordés, de membres d'un groupe *multicast* (figure 19-47).

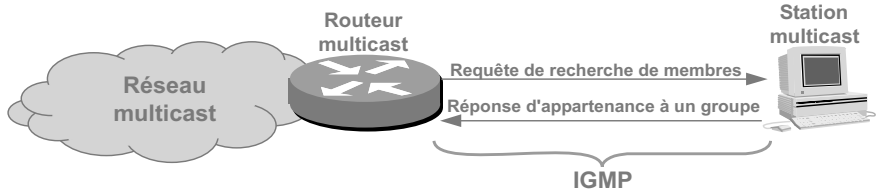


Figure 19.47 Principe du protocole IGMP.

Le protocole IGMP version 2 utilise quatre types de messages et un seul format (figure 19.48) :

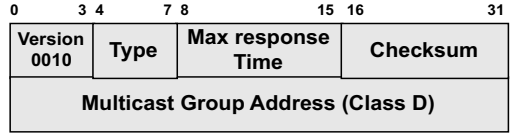


Figure 19.48 Le format des messages IGMP v2.

- Les messages de demande d'adhésion (*Host membership query*, type = 0x11) destinés à demander régulièrement aux stations à quel groupe *multicast* elles appartiennent. Un seul routeur *multicast* du réseau envoie régulièrement ces messages (routeur dominant), c'est celui de plus petite adresse IP. Le champ *Multicast group address* est à 0.
- Les messages de réponse (*Host membership report*, type = 0x16) sont envoyés par tout hôte appartenant à un groupe de diffusion *multicast*. Chaque hôte répond après un délai aléatoire avant le délai imposé (*Max response time*). Le champ *Multicast group address* est alors renseigné sur le groupe d'appartenance. Si un hôte a déjà répondu pour ce groupe, les autres hôtes du même groupe s'abstiennent alors de répondre.
- Lorsqu'un hôte quitte une session *multicast*, il envoie un message d'abandon de groupe (*Leave group message*, type 0x17) à l'adresse *multicast* 224.0.0.2 (tous les routeurs *multicast* du sous-réseau).
- En réponse à ce message, le routeur demandeur envoie un message de demande d'adhésion spécifique au groupe qui vient d'être quitté (*Group specific query message*, type = 0x11 mais avec le champ *Multicast group address* renseigné du groupe *multicast* abandonné). En l'absence de réponse, le groupe est supprimé de sa liste d'adhésion et plus aucun message concernant ce groupe ne sera relayé vers le sous-réseau.

19.5.4 Les protocoles de routage *multicast*

Généralités

IGMP assure la diffusion des datagrammes *multicast* à l'ensemble des stations d'un sous-réseau local. Cependant, dans le réseau (Internet ou autre), le routage des datagrammes *multicast* doit

© Dunod – La photocopie non autorisée est un délit

être assuré de manière à économiser la bande passante. Plusieurs mécanismes peuvent être mis en œuvre :

– le *Floding* ou inondation, est très facile à mettre en œuvre puisque le routeur n'a aucune table d'acheminement à entretenir, mais cette méthode génère un trafic d'autant plus important que le réseau est grand ;
– le *Spanning Tree* permet de construire un chemin unique (arbre) entre une source (racine) et une destination (feuille) ;
– le *Reverse Path Broadcasting* (**RPB**) aussi appelé *Reverse Path Forwarding* est une amélioration des performances du *Spanning Tree*. RPB construit un arbre par groupe de *multicast*. Le principe est relativement simple quand un routeur reçoit un paquet sur une interface, il examine si l'interface d'arrivée est bien sur le chemin le plus court pour rejoindre la source (celle qui serait utilisée pour envoyer un datagramme *unicast* à la source). Si c'est le cas, le paquet est diffusé sur toutes les autres interfaces du routeur (inondation), sinon le paquet est détruit.

Les protocoles de routage multicast

DVMRP (*Distance Vector Multicast Routing Protocol*, RFC 1075) est un protocole vecteur distance destiné à assurer le routage *multicast*. Une variante de l'algorithme *Reverse Path Brocasting* est utilisée pour construire les tables de routage *multicast*. DVMRP est le complément réseau du protocole local IGMP (figure 19.49).

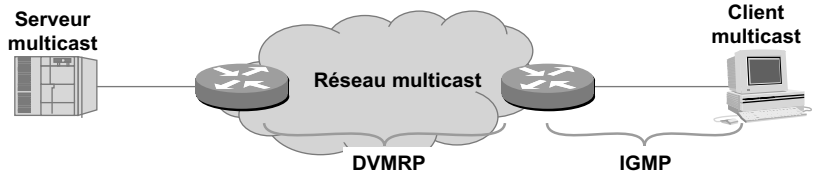


Figure 19.49 La complémentarité des protocoles IGMP et DVMRP.

L'arbre *multicast* établit des relations en « amont » et en « aval » entre les différents routeurs du réseau. L'arbre de diffusion est maintenu à jour selon une méthode dite élagage et greffe. Lorsqu'un routeur *multicast* n'a plus d'abonné pour un groupe (hôte final ou routeur aval), il émet un message dit *prune packet* pour informer en amont de l'inutilité de maintenir un lien de diffusion *multicast* pour ce groupe (élagage de la branche). Le routeur ne supprimera cette route qu'à l'échéance d'un *timer*. À l'inverse à la réception d'une demande d'adhésion, il émet un message dit *graft packet* pour reconstruire une route vers la source (greffe). Ce fonctionnement est illustré figure 19.50.

À l'instar de RIP, le protocole DVMRP échange ses tables de routage avec ses voisins DVMRP (message *route report* toutes les 60 s à l'adresse de diffusion 224.0.0.4). Les voisins DVMRP sont découverts par l'émission, toutes les 10 s, de messages *probe message*.

Issu des travaux du groupe IDRM (*Inter-Domain Multicast Routing*) de l'IETF, le protocole **PIM** (*Protocol Independant Multicast*) est essentiellement destiné à être mis en œuvre sur les grands réseaux comme Internet qui se caractérisent par des serveurs et des clients très dispersés. PIM se décline en deux versions, PIM DM (*Dense Mode*) et le PIM SM (*Spare Mode*, RFC 2362).

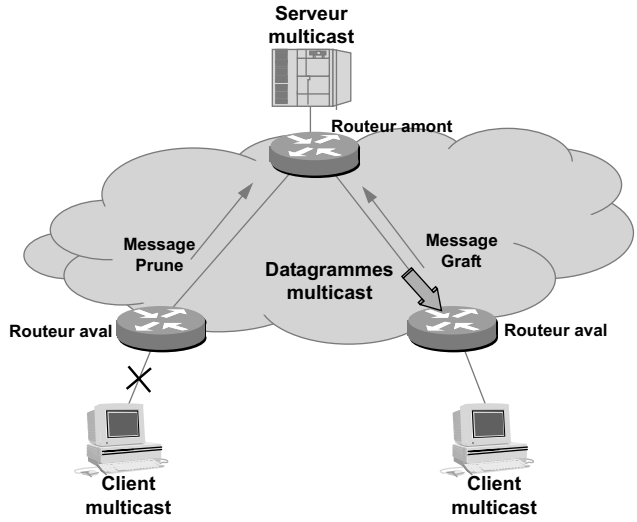


Figure 19.50 La diffusion de messages dans un réseau DVMRP.

Le PIM SM intègre son propre algorithme de routage *unicast* (indépendant du protocole de routage *unicast* utilisé dans le réseau). Les routeurs, d'un sous-réseau, en charge de la gestion du *multicast*, doivent explicitement rejoindre un groupe *multicast* en s'abonnant à un point de rendez-vous pour ce groupe (message « *Join* »). À un groupe *multicast* correspond un seul point de rendez-vous.

Internet et le multicast

La composante d'Internet qui assure la diffusion de messages en *multicast* sur le réseau est désignée sous le nom de **Mbone** (*Multicast Backbone*). Il s'agit d'un réseau virtuel reliant les différents routeurs *multicast* (mrouteurs) par des tunnels (tunnels *multicast*), mais le service rendu est du type datagramme.

Diverses applications sont offertes téléconférences, programmes radio, jeux... Un annuaire des sessions en cours permet aux utilisateurs de rejoindre un groupe de diffusion.

19.6 LES FONCTIONS ANNEXES DES ROUTEURS

19.6.1 Les routeurs multiprotocoles

Dans des environnements complexes, il arrive que plusieurs protocoles réseaux soient utilisés en même temps (IP, IPX...). Les routeurs capables d'assurer l'acheminement de données de différents protocoles sont dits routeurs multiprotocoles.

Dans ces environnements, se pose la question de la reconnaissance du protocole à router. Digital, Intel et Xerox ont résolu ce problème en introduisant dans la trame Ethernet (Ethernet v2) le champ Type de protocole (*Ethertype*). ISO identifie le protocole supérieur par les champs DSAP et SSAP de la trame LLC. Certaines implémentations de réseaux locaux utilisent la trame LLC mais des protocoles de niveau supérieur non ISO (Token Ring...). Pour résoudre le problème d'identification, une encapsulation supplémentaire a été introduite : l'encapsulation **SNAP** (*SubNetwork Access Protocol*). La figure 19.51 rappelle ces différents formats pour les réseaux de type Ethernet.

© Dunod – La photocopie non autorisée est un délit

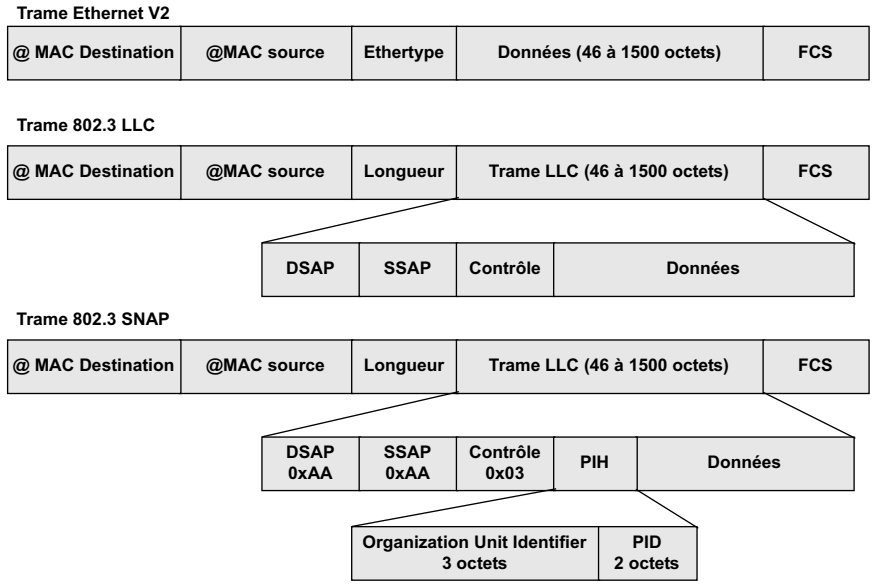


Figure 19.51 L'encapsulation SNAP.

À la réception d'une trame Ethernet, le routeur examine le champ Type, si la valeur est supérieure à 1 500, la trame est au format Ethernet v2, et le champ contient l'Ethertype du protocole transporté. Si la valeur est égale ou inférieure à 1 500 la trame est au format IEEE 802.3, le protocole supérieur est alors identifié par les champs SSAP et DSAP de la trame LLC (codage ISO). Si la valeur contenue dans ces champs est « 0xAA », la trame LLC encapsule une trame SNAP et le protocole est identifié par le champ **PIH** (*Protocol Identification Header*) dans le sous-champ **PID** (*Protocol_ID*) dont le codage correspond à celui du champ Type de la trame Ethernet v2.

Le sous-champ **OUI** (*Organization Unit Identifier*, 3 octets) contient l'identification du constructeur de la carte transporteur, c'est le code IEEE du fournisseur, il peut aussi désigner un organisme de normalisation (par exemple la valeur 0x00-80-C2 désigne l'IEEE 802.1). Ce champ est mis à zéro (0x00-00-00) pour les trames Ethernet v2.

19.6.2 La compression de données

Afin d'optimiser l'utilisation des liens, certains routeurs (et les ponts distants) utilisent la compression de données. Trois modes de compression sont généralement offerts :

– la compression des en-têtes (*Header*),
– la compression du champ données seul (*Payload*),
– la compression de la trame complète (*Link*).

La compression des en-têtes n'est intéressante dans le monde IP que si les paquets de données sont de très petites tailles (terminal Telnet, par exemple). La compression du champ données seul semble la solution la plus efficace. En effet, le champ en-tête non compressé optimise les performances des routeurs intermédiaires qui n'ont pas besoin de décompresser la trame entière ou l'en-

tête pour router correctement le paquet. Certains routeurs activent ou désactivent dynamiquement la compression en fonction de la nature des données à transmettre (données déjà compressées...).

La compression de données n'est utile que si le temps réel de transmission des données compressées est inférieur au temps d'émission des données non compressées. À partir d'un certain débit du lien, la compression pénalise le temps d'émission (temps CPU). Dans ce cas, la compression ne présente un intérêt que si on utilise un réseau facturé au volume (figure 19.52).

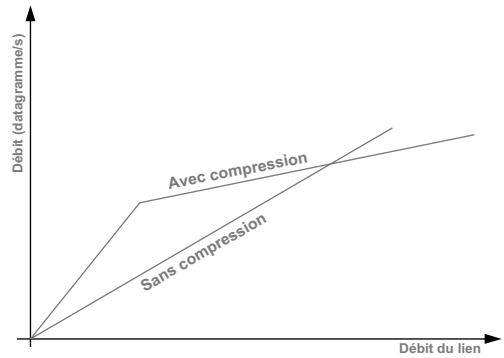


Figure 19.52 Efficacité de la compression en fonction du débit du lien.

19.6.3 Le routage à la demande (*Dial on Demand*)

Le routage à la demande est une technique mise en œuvre dans les petits routeurs (routeurs d'agence) n'ayant aucun lien permanent avec le réseau. Lorsque des données sont à transmettre (figure. 19.53), le *Dial on Demand* établit un lien commuté (RTC ou RNIS)

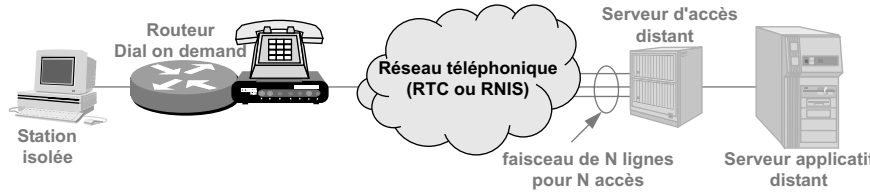


Figure 19.53 Principe du Dial on Demand.

Pour éviter les reconnexions successives, la connexion n'est rompue qu'à l'échéance d'un *timer* (*Idle timer*). Le serveur distant authentifie l'appelant par son numéro d'appelant ou un mot de passe de connexion. L'expansion du réseau Internet et les accès qu'il offre ont rendu obsolète ce mode de connexion à des ressources distantes.

19.6.4 La bande passante à la demande (*Bandwith on Demand*)

Ce service, similaire au précédent, établit une connexion (lien de débordement) avec un réseau numérique (RNIS) dès qu'un certain seuil (*Threshold*) de trafic, mesuré par la taille des files d'attente, est atteint sur le lien principal. La connexion est rompue dès que le trafic redescend en dessous de ce seuil (figure 19.54).

© Dunod – La photocopie non autorisée est un délit

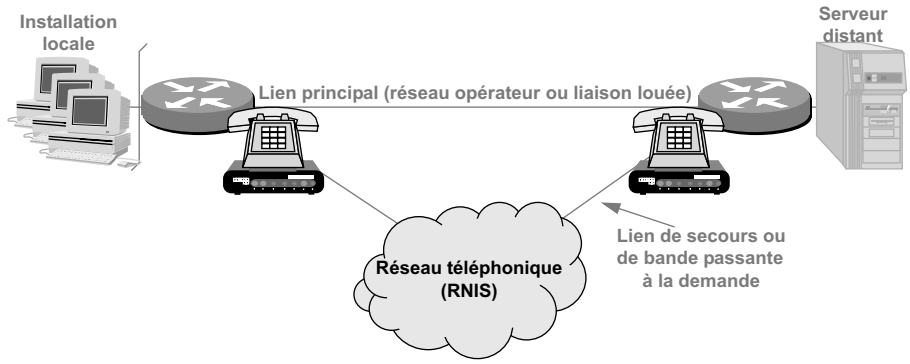


Figure 19.54 Principe du Bandwith on Demand.

Le *Bandwith on Demand* ou bande passante à la demande peut utiliser plusieurs canaux B. Aujourd'hui, ce type de raccordement est essentiellement utilisé en lien de secours d'une liaison permanente (liaison louée).

19.7 LES PASSERELLES APPLICATIVES

Les passerelles mettent en relation des systèmes totalement hétérogènes. Elles réalisent une adaptation des protocoles telle qu'une application d'un environnement A voit l'application distante de l'environnement *B*, comme si celle-ci appartenait au monde A.

La figure 19.55 représente une passerelle entre une messagerie ISO X.400 et la messagerie **SMTP** (*Simple Mail Transfer Protocol*) du monde Internet.

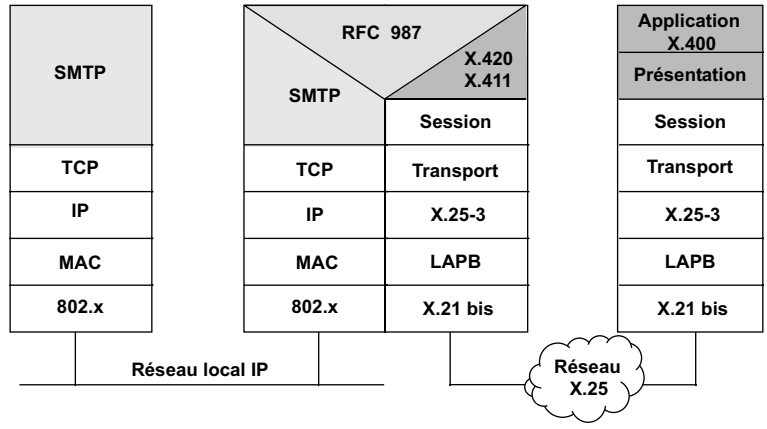


Figure 19.55 Exemple de passerelle applicative.

EXERCICES

Exercice 19.1 Protocole RIP/OSPF

Comparez les protocoles RIP et OSPF en complétant la figure 19.56.

	RIP	OSPF
Caractéristiques		
Type d'algorithme		
Métrique		
Métrique configurable		
Origine		
Architecture du réseau		
Type		
Nombre de routeurs		
Routeur maître		
Support des masques de longueur variable		
Performance		
Charge du réseau		
Périodicité des mises à jour		
Temps de convergence		
Mode de mise à jour		
Support de la qualité de service		
Sécurité		
Authentification		

Figure 19.56 Comparaison RIP/OSPF.

Exercice 19.2 Agrégation de routes

Supposons le réseau de la figure 19.57. Les trois aires raccordées à la zone *backbone* utilisent des adresses privées 10.0.0.0. Chaque aire peut comporter jusqu'à 16 sous-réseaux terminaux. Les adresses de sous-réseaux et les masques associés sont indiqués sur la figure.

1. Quel serait, en l'absence d'agrégation d'annonce, le nombre d'entrées dans la table du routeur de bordure d'aire du *backbone* ?
2. Quelles adresses et quels masques annoncent les routeurs de bordure d'aire ?
3. Dans quel ordre les adresses seront-elles inscrites dans la table du routeur de bordure de l'aire *backbone* ?

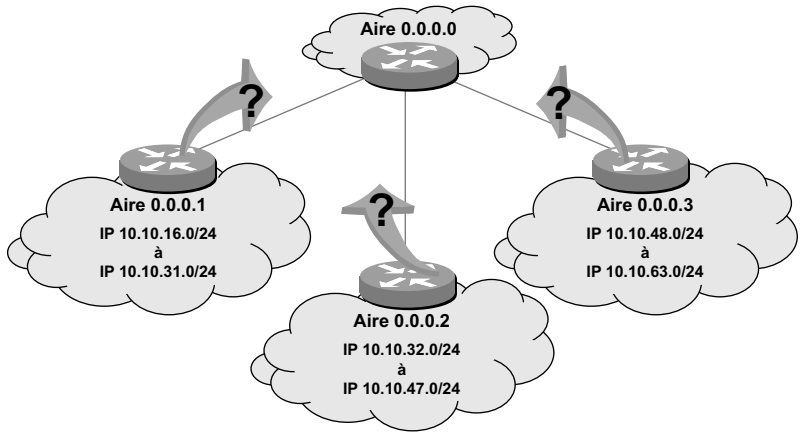


Figure 19.57 Les réseaux OSPF.

Exercice 19.3 Adresses *multicast*

Un groupe *multicast* est identifié par l'adresse IP *multicast* 224.16.21.5. À quelles adresses MAC répondra l'adaptateur Ethernet d'adresse *unicast* 08-00-02-2D-75-BD situé sur le sous-réseau 10.10.31.0 /24 ?

Exercice 19.4 Comparaison pont/routeur

Comparez un pont et un routeur en complétant la figure 19.58.

	Pont	Routeur
Configuration		
Transparence aux protocoles		
Sécurité (Filtre)		
Extension du réseau		
Trafic de service		
Broadcast		
Charge de travail (personnel)		

Figure 19.58 Comparaison pont/routeur.

Exercice 19.5 Masque de sous-réseau

Deux réseaux (A et B) utilisant le protocole TCP/IP sont reliés *via* un routeur. L'entreprise a défini le masque de sous-réseau : 255.255.0.0. Un utilisateur du réseau A sur la machine 100.64.0.102 se plaint de ne pouvoir joindre un correspondant d'adresse 100.64.45.102 du réseau B. Expliquez pourquoi, donnez une solution simple pour que ces machines puissent communiquer.

Exercice 19.6 Table de routage statique

Votre entreprise comporte quatre réseaux Ethernet d'adresses et de topologie indiquées par la figure 19.59.

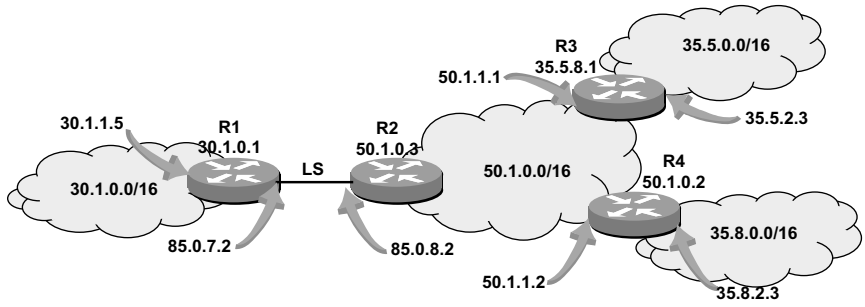


Figure 19.59 Plan d'adressage et tables de routage du réseau.

Le routeur R1 d'adresse 30.1.0.1 est relié au routeur R2 d'adresse 50.1.0.3 par une liaison privée spécialisée (LS) dont les adresses d'interface sont respectivement 85.0.7.2 pour le routeur R1 et 85.0.8.2 pour le routeur R2.

Le routeur R2 possède la même adresse d'interface sur le réseau 50.1.0.0/16 que son adresse de nœud soit 50.1.0.3.

Le routeur R3 relie directement les réseaux 50.1.0.0/16 et 35.5.0.0/16 par des interfaces ayant respectivement comme adresse 50.1.1.1 et 35.5.2.3.

De même, le routeur R4 relie directement les réseaux 50.1.0.0/16 et 35.8.0.0/16 par ses interfaces locales d'adresse respective 50.1.1.2 et 35.8.2.3.

1. À quelle classe d'adressage appartiennent les adresses de ce réseau ?
2. Existe t'il une autre manière d'écrire les adresses réseau et leur masque, donnez un exemple ?
3. Quelle est l'adresse à utiliser par le réseau 30.1.0.0/16 pour envoyer un datagramme à TOUS les hosts du réseau 35.8.0.0/16 ?
4. Établissez les tables de routage (routage fixe) de chacun des routeurs de ce réseau.

Remarque : pour noter les entrées des tables, on utilisera la syntaxe suivante : [@destination, prochain saut], On ne fera pas apparaître les informations de coût (métrique). Les données correspondant aux interfaces locales seront notées : [@IP, interface locale]. Les entrées locales seront toujours indiquées en tête de liste. On devra pouvoir « pinguer » les LS. Une route par défaut pourra être indiquée avec l'une des notations suivantes : « [0.0.0.0, prochain saut] ou [*, prochain saut] ».

Exercice 19.7 Réseau et qualité de service (QoS)

La méthode la plus utilisée aujourd'hui pour garantir aux applications une certaine qualité de service consiste à assurer à chaque type de flux un service différencié. La figure 19.60 en illustre le principe :

© Dunod – La photocopie non autorisée est un délit

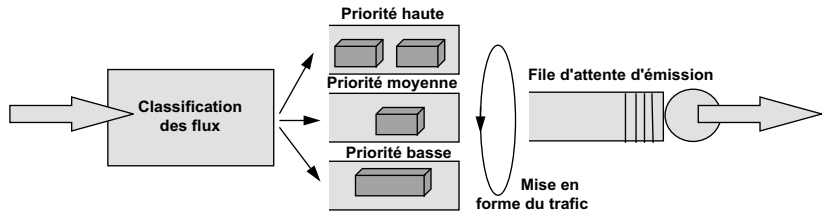


Figure 19.60 Traitement interne des flux.

Selon des critères définis par l'administrateur du réseau (@IP, Port...), les données sont placées dans une file d'attente spécifique. Les différents systèmes se différencient selon la manière dont sont lues les données que nous appellerons ici mise en forme du trafic ou ordonnancement, avant d'être mises dans la file d'attente d'émission.

Dans le système représenté précédemment, la bande passante est affectée aux files d'attente selon une pondération définie par l'administrateur réseau (**WRR**, *Weighted Round Robin*). Par exemple si la file d'attente de haute priorité a un poids de 5, celle de moyenne priorité 3 et celle de basse priorité 2, le système lira 5 blocs de données de la file 1, puis 3 blocs de la file 2 et enfin 2 de la file 3. Si une file d'attente est vide, le système passe immédiatement à la suivante.

Votre système informatique met en œuvre trois types d'application :

– Voix sur IP.
– Clients/serveur.
– Transfert de fichiers.

Votre administrateur réseau décide d'affecter respectivement la moitié de la bande passante aux applications voix, 30 % aux applications clients/serveur et seulement 20 % aux applications de transfert de fichiers, pour cela il affecte aux files d'attente les poids de 5, 3 et 2.

1. Dans ces conditions, si le débit du lien est 2 Mbit/s, calculez quelle est, *a priori*, la bande passante maximale et minimale susceptible d'être allouée à chacun des flux.
2. En admettant que chacun des flux soit caractérisé par une taille moyenne de blocs de données de 40 octets pour la voix, 256 pour les applications clients/serveur et 1 500 octets pour les applications de transfert de fichiers (pour simplification on négligera les données protocolaires) :

   a) Calculez la bande passante maximale et minimale réellement affectée à chaque type de flux. Que pensez-vous de votre réponse à la première question ?
   b) Déterminez les poids qui assureraient le respect de la bande minimale allouée à chaque flux.
   c) Imaginez un autre critère de lecture des files d'attentes.

Partie **IV**

La voix dans les réseaux

20 Introduction à la téléphonie 617
20.1 Principes généraux de la téléphonie 617
20.2 L'organisation du réseau téléphonique 618
20.3 L'établissement d'une communication téléphonique 620
20.4 L'évolution de la téléphonie, le RNIS 625
20.5 La téléphonie et la mobilité 643
20.6 Conclusion 653
EXERCICES 654

21 Installation d'abonné et réseau privé de téléphonie 655
21.1 Les autocommutateurs privés 655
21.2 L'installation d'abonné 662
21.3 Les réseaux privés de PABX 665
21.4 Principes des réseaux voix/données 675
21.5 La voix sur ATM 683
21.6 La voix sur le Frame Relay 685
21.7 La voix et téléphonie sur IP 687
21.8 Conclusion 703
EXERCICES 704

Chapitre **20**

Introduction à la téléphonie

20.1 PRINCIPES GÉNÉRAUX DE LA TÉLÉPHONIE

Historiquement, le transport de la voix est à l'origine des premiers réseaux de transmission. Utilisant le principe de la commutation de circuits, le réseau téléphonique public commuté (**RTPC**, ou simplement **RTC**, ou encore **PSTN** pour *Public Switched Telecommunication Network*) met en relation deux abonnés à travers une liaison dédiée pendant tout l'échange (figure 20.1). Bien que destiné au transfert de la voix, le réseau téléphonique permet aussi la transmission de données[1].

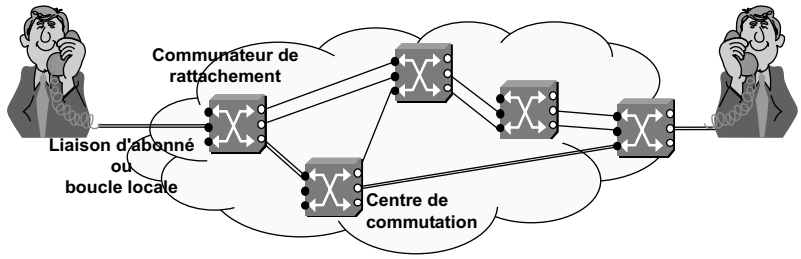


Figure 20.1 Principe du réseau téléphonique commuté.

La commutation de circuits ou commutation spatiale consiste à juxtaposer bout à bout des voies physiques de communication, la liaison étant maintenue durant tout l'échange. À l'origine, la mise en relation était réalisée manuellement par des opérateurs, la commutation automatique imaginée en 1889[2] aux États-Unis a été généralisée en France en 1970. La numérisation de la voix (1962) a

1. En France, le transport de données sur le réseau téléphonique n'est autorisé que depuis 1964.

2. La petite histoire rapporte que le premier commutateur téléphonique automatique a été imaginé par Strowger (1889) pour lutter contre son concurrent commercial (service de pompes funèbres). En effet, l'épouse de ce dernier opératrice au centre téléphonique local (Kansas City aux États-Unis) acheminait les appels, à destination d'un service de pompes funèbres, uniquement vers l'entreprise de son mari !

permis le multiplexage temporel des communications. La commutation spatiale a été, alors, remplacée par la commutation d'intervalles de temps (IT) ou commutation temporelle. Ce concept est illustré figure 20.2. En mettant en relation un IT d'une trame en entrée avec un IT d'une autre trame en sortie, la commutation temporelle émule un circuit. La communication étant *full duplex*, une bande passante de 64 kbit/s, dans chaque sens, est réservée durant toute la communication.

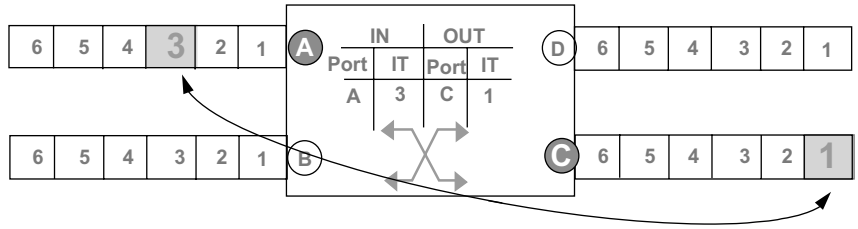


Figure 20.2 Principe de la commutation temporelle.

Les supports de transmission sont constitués de voies numériques multiplexées selon une hiérarchie appelée hiérarchie plésiochrone (**PDH**, *Plesiochronous Digital Hierarchy*). Malgré la numérisation du réseau, la liaison des abonnés résidentiels est restée essentiellement analogique. C'est le commutateur de rattachement qui réalise la conversion analogique/numérique et inversement de la voix (figure 20.3).

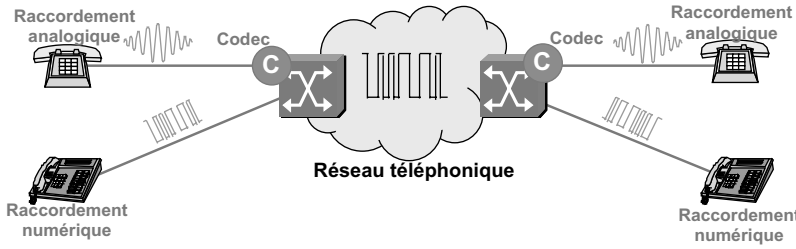


Figure 20.3 Les modes de raccordement.

20.2 L'ORGANISATION DU RÉSEAU TÉLÉPHONIQUE

20.2.1 L'architecture traditionnelle

Le réseau téléphonique traditionnel a une organisation hiérarchique à trois niveaux (figure 20.4). Il est structuré en zones, chaque zone correspond à un niveau de concentration et en principe de taxation. On distingue :

– Zone à autonomie d'acheminement (**ZAA**), cette zone, la plus basse de la hiérarchie, comporte un ou plusieurs Commutateurs à autonomie d'acheminement (**CAA**) qui eux-mêmes desservent des Commutateurs locaux (**CL**). Les commutateurs locaux ne sont que de simples concentrateurs de lignes auxquels sont raccordés les abonnés finals. La ZAA (Zone à autonomie d'acheminement) est un réseau étoilé, elle constitue le réseau de desserte ;
– Zone de transit secondaire (**ZTS**), cette zone comporte des Commutateurs de transit secondaires (**CTS**). Il n'y a pas d'abonnés reliés directement aux CTS ;

– Zone de transit principal (**ZTP**), cette zone assure la commutation des liaisons longues distances. Chaque ZTP comprend un Commutateur de transit principal (**CTP**). Au moins un Commutateur de transit principal (**CTP**) est relié à un Commutateur de transit international (**CTI**).

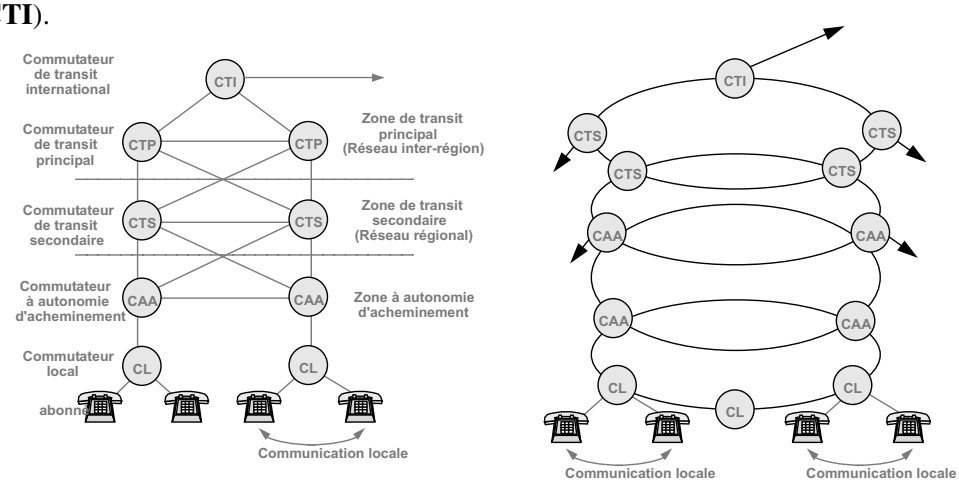


Figure 20.4 L'organisation du réseau téléphonique.

Le réseau étant partiellement maillé, plusieurs itinéraires sont généralement possibles pour atteindre un abonné. Afin d'optimiser l'utilisation des faisceaux, on distingue deux types de faisceaux : les faisceaux de premier choix et les faisceaux de second choix ; les faisceaux de second choix constituent des faisceaux de débordement. Pour un numéro donné, le faisceau de premier choix est déterminé de telle manière qu'il conduise l'appel vers le commutateur le plus proche de l'abonné appelé en empruntant les faisceaux de plus faible hiérarchie. Aujourd'hui, le réseau téléphonique évolue vers une architecture en boucle (figure 20.4) sur un transport SDH.

20.2.2 La gestion du réseau

La gestion générale du réseau discerne trois fonctions :

– **la distribution**, celle-ci comprend essentiellement la gestion (installation, mise en œuvre, maintenance) de la liaison d'abonné ou boucle locale (paire métallique) qui relie l'installation de l'abonné au centre de transmission de rattachement. Cette ligne assure la transmission de la voix (fréquence vocale de 300 à 3 400 Hz), de la numérotation (10 Hz pour la numérotation décimale et les fréquences de 697 à 1 633 Hz pour la numérotation fréquentielle) et de la signalisation abonné/réseau (boucle de courant, fréquences vocales...) ;

– **la commutation**, c'est la fonction essentielle du réseau, elle consiste à mettre en relation deux abonnés, à maintenir la liaison établie durant tout l'échange et libérer les ressources à la fin de celui-ci. C'est le réseau qui détermine les paramètres de taxation et impute le coût de la communication à l'appelant ou à l'appelé ;

– **la transmission**, c'est la partie support de télécommunication du réseau, cette fonction est remplie soit par un système filaire cuivre, par de la fibre optique ou par des faisceaux hertziens. Aujourd'hui, le réseau français est intégralement optique et numérisé, seule la liaison d'abonné est encore, la plupart du temps, analogique et sur support cuivre, notamment pour les abonnés résidentiels.

© Dunod – La photocopie non autorisée est un délit

20.3 L'ÉTABLISSEMENT D'UNE COMMUNICATION TÉLÉPHONIQUE

20.3.1 Principe d'un poste téléphonique

Établir une communication téléphonique consiste à mettre en relation deux terminaux téléphoniques. Pour cela, le poste téléphonique doit remplir plusieurs fonctions, chacune d'elle étant réalisée par un élément spécifique. Le terminal téléphonique élémentaire comporte cinq éléments (figure 20.5) :

- les crochets ou supports sur lesquels repose le combiné ; lorsque le combiné est soulevé les contacts ferment le circuit. Le commutateur de rattachement détecte un courant et en déduit que l'abonné désire entrer en communication. Une résistance ajustable permet d'ajuster ce courant à 30 mA. De même, lors du raccroché, le commutateur détecte l'ouverture de la boucle de courant. L'ouverture ou la fermeture de cette boucle permet, très simplement, au commutateur de rattachement de détecter le changement d'état du terminal (signalisation) ;
- le microphone ou capteur, constitué d'une simple membrane qui, sous l'effet de la pression acoustique (voix), fait varier la résistance interne de celui-ci (micro à grenaille de charbon). Ces variations de résistance entraînent des variations du courant dans la boucle de courant. Ce sont ces variations, proportionnelles à la pression sur la membrane (voix), qui constituent le signal analogique de voix transmis, après numérisation, à l'usager distant ;
- un écouteur, simple membrane métallique qui vibre selon les variations du courant dans un électro-aimant et restitue le son ;
- un cadran, celui-ci en provoquant l'ouverture de la boucle de courant (numérotation décimale) envoie des impulsions au commutateur. Celles-ci seront interprétées et permettront d'identifier l'appelé ;
- une sonnerie, alimentée en 50 Hz (80 V), alerte l'abonné distant et l'invite à décrocher, c'est le commutateur de rattachement qui envoie le signal 50 Hz lors d'un appel.

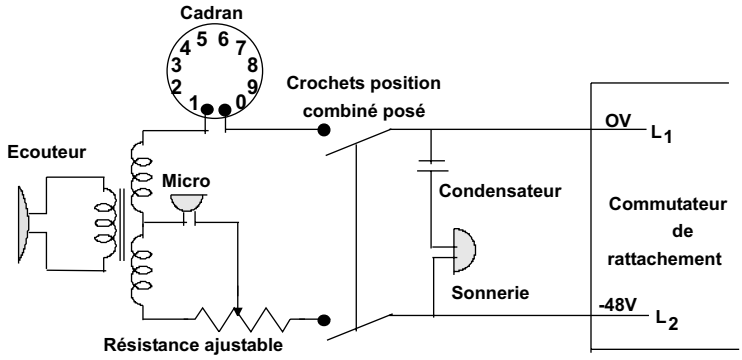


Figure 20.5 Le terminal téléphonique S63.

20.3.2 Principe du raccordement d'usager

L'usager est raccordé au réseau *via* une unité de raccordement (**URA**, Unité de raccordement d'abonnés). Celle-ci peut être locale ou distante (**URAD**, Unité de raccordement d'abonnés distants). Le commutateur de raccordement assure les fonctions de réception et de mémorisation de

la numérotation (enregistreur), celle-ci est analysée et traduite par un traducteur qui va définir les conditions de taxation et déterminer le routage. Enfin, le sélecteur recherche une ligne disponible (joncteur) et affecte les ressources (circuits ou IT). La figure 20.6 illustre ces différents éléments.

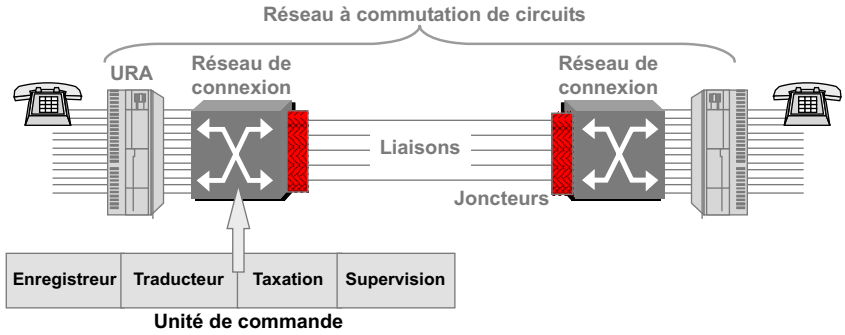


Figure 20.6 Principe du raccordement des abonnés.

20.3.3 La mise en relation Usager/Usager

La mise en relation de deux abonnés répond à un protocole qui organise le dialogue entre les terminaux d'usager et le réseau (signalisation Usager/Réseau). Elle comporte deux ensembles de mécanisme. Le premier correspond à un échange d'information hors communication destiné à établir celle-ci ou à libérer les ressources, c'est la signalisation ; le second à la communication téléphonique proprement dite.

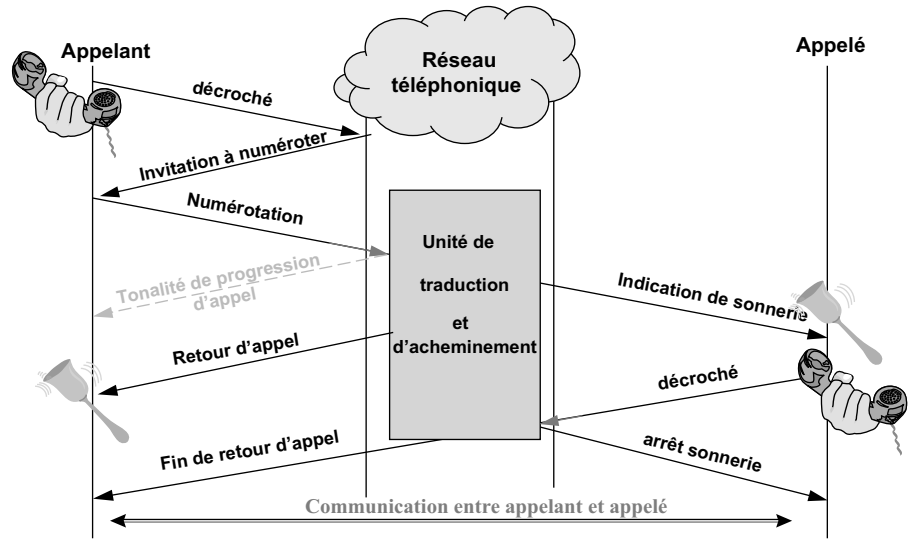


Figure 20.7 Le diagramme d'une communication téléphonique.

La figure 20.7 illustre les différentes étapes de la mise en relation de deux abonnés, celles-ci, au nombre de cinq, sont détaillées ici :

© Dunod – La photocopie non autorisée est un délit

1. décroché du combiné, détection de la boucle de courant, envoi de la tonalité d'invitation à numéroter (signal à 440 Hz, le « la » des musiciens) ;
2. numérotation, le numéro composé est mémorisé et décodé par le commutateur de rattachement. Le système établit le lien. Durant cet intervalle de temps, le demandeur recevait, avant le 18 octobre 1996, une tonalité dite de progression d'appel[3] ;
3. envoi du signal de sonnerie à l'appelé distant et attente du décroché de celui-ci. L'appelant reçoit le signal de retour d'appel appelé tout simplement « sonnerie » ;
4. le correspondant décroche. Le central de rattachement détecte le décroché (boucle de courant), il arrête les signaux de sonnerie, les signaux de retour d'appel et déclenche la taxation ;
5. l'échange d'information (voix ou données) peut commencer.

La fin de communication est détectée par le raccroché (ouverture de la boucle de courant). Notons deux variantes lors de l'appel : la première correspond à l'incapacité du réseau à écouler la demande, l'appelant en est alors averti par un message du style : « Par suite d'encombrement... », la seconde correspond à l'occupation de la ligne appelée, l'appelant a, alors en retour, une tonalité spécifique dite tonalité d'occupation.

L'intention d'établir une communication est détectée par le décroché du terminal. Que se passe-t-il si on décroche le combiné mais que cette action n'est suivie d'aucune numérotation (décroché malencontreux) ? La détection du décroché monopolise des ressources dans le commutateur de rattachement (enregistreur). Pour libérer ces ressources, il est nécessaire d'inhiber le poste dont l'usage restera interdit jusqu'à ce que celui-ci soit raccroché.

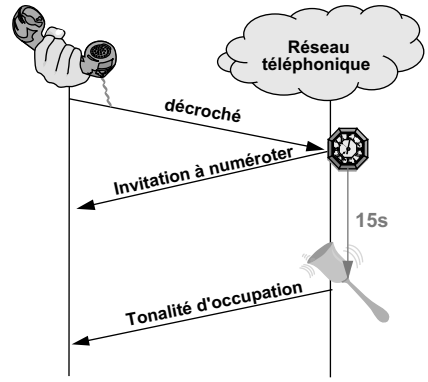


Figure 20.8 Le diagramme des événements lors d'un décroché malencontreux.

La figure 20.8 décrit les différentes étapes du décroché malencontreux, la signification du diagramme est donnée ci-dessous :

1. Lorsque l'appelant décroche le combiné, le réseau (le commutateur de rattachement) détecte la fermeture de la boucle de courant ;

3. Ce signal simulait le « bruit » généré par les commutateurs électromécaniques. Cette tonalité était destinée à faire patienter l'appelant pendant l'établissement du circuit. Avec les commutateurs électroniques de la dernière génération et l'utilisation d'une signalisation par canal sémaphore, la durée d'établissement du circuit est devenue très faible et ce signal n'avait plus de raison d'être.

2. il envoie à l'usager l'invitation à numéroter (signal à 440 Hz). Dans le même temps, il arme une temporisation ;
3. le demandeur n'effectuant aucune opération, à l'échéance du compteur (*timer*, de 15 à 20 s) le commutateur de rattachement inhibe le poste en lui envoyant la tonalité d'occupation (signal de décroché malencontreux) pendant environ une minute.

20.3.4 La numérotation

Le numéro d'abonné (numéro international au format E.164) correspond à l'identification du point d'accès au réseau (prise terminale). La numérotation permet à l'opérateur d'assurer l'acheminement de l'appel, le format de l'adresse, de type hiérarchique (figure 20.9), facilite la détermination de la route. Cependant la notion de portabilité, nouveau service offert par les opérateurs, détruit le lien entre numéro et situation géographique. Ce nouveau service nécessite un enrichissement de la signalisation et des accords entre opérateurs. Le numéro E.164 traditionnel comprend :

- la désignation de l'exploitant (**E**), ce numéro n'a de valeur que sur le territoire français, il doit être omis pour un appel de l'étranger[4] ;
- la zone d'appel (**Z**), la France est divisée en cinq zones ;
- le commutateur de rattachement désigné par le sigle **ABPQ**[5] ;
- enfin, les quatre derniers chiffres (**MCDU**, Milliers, Centaines, Dizaines, Unités) qui désignent l'abonné local.

Préfixe international	Indicatif Pays	Numéro national demandé		
		EZ	**AB PQ**	**MC DU**
Pour sortir du réseau national, en France 00	Par exemple France = 33	Exploitant Zone	Numéro du commutateur de rattachement	Numéro de la ligne d'abonné

Valeur E	Signification
0	Opérateur de boucle locale
1	Numéros d'urgence
2	Siris
3	Numéros spéciaux (téléservices)
4	Télétel 2
5	Omnicom
6	Esprit Telecom
7	Cegetel
8	France Télécom
9	9 Télécom

Figure 20.9 La structure d'un numéro d'abonné et valeur du préfixe E.

Il existe trois modes de génération des informations de numérotation. Le plus ancien correspond à la numérotation décimale ou analogique (33/66 ou 10 Hz), celle-ci est générée par le cadran de la figure 20.5. Ce dernier provoque des ruptures de circuit. Les numéros sont envoyés au commutateur de rattachement sous forme d'impulsions de 66 ms suivi d'un repos de 33 ms, d'où le nom de système 33/66. Le 1 correspond à une rupture, le 2 à deux... le 0 à dix ruptures (figure 20.10).

4. Le nombre d'opérateurs étant supérieur aux capacités de numérotation, l'ARCEP (Autorité de régulation des communications électroniques et des postes) a remis en vigueur l'utilisation du préfixe 16 suivi de deux chiffres. Exemple : 16 01 désigne Prosodie...

5. La signification d'ABPQ semble oubliée. Pour certains, ces chiffres désignaient les abonnés d'un même quartier reliés à un même central (ABPQ, Abonnés par quartier).

© Dunod – La photocopie non autorisée est un délit

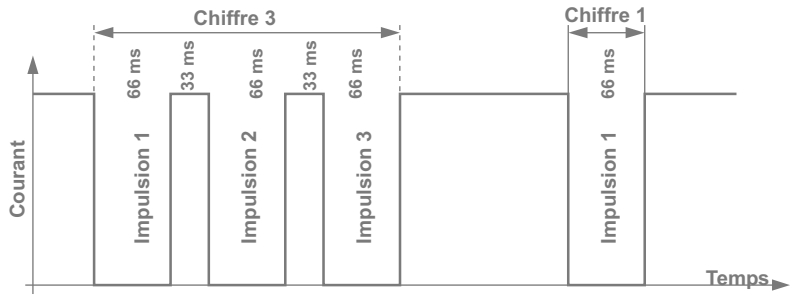


Figure 20.10 L'exemple de numérotation décimale de 31.

Aujourd'hui, sur les raccordements analogiques, la numérotation la plus utilisée est la numérotation fréquentielle ou vocale (multifréquentielle), normalisée par l'UIT (Q.23). Dans ce mode de numérotation, l'enfoncement d'une touche génère deux signaux de fréquences différentes transmis au central de rattachement (une fréquence haute suivie d'une fréquence basse, système dit **DTMF,** *Dual-Tone MultiFrequency*). Chaque combinaison de fréquences a été déterminée pour minimiser le risque qu'une combinaison de voix lui ressemble. Les postes comportent 12 ou 16 touches, les touches A, B, C, et D[6] peuvent être affectées à des fonctions particulières (figure 20.11). Certains postes téléphoniques fréquentiels ont la possibilité d'émettre une numérotation décimale.

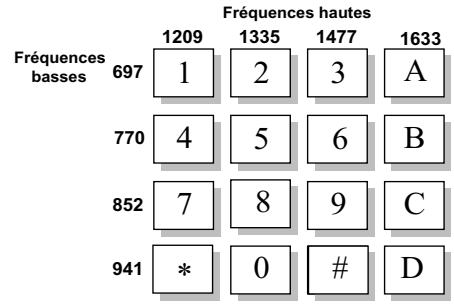


Figure 20.11 Le clavier des postes à fréquences vocales.

Enfin, avec la dernière génération de postes téléphoniques spécifiques dits postes numériques, la numérotation correspond à la transmission d'une valeur binaire sur la voie de signalisation. La numérotation peut être propriétaire (poste numérique propriétaire) ou normalisée (poste RNIS).

20.3.5 Les modes de signalisation

Dès le décroché et jusqu'au raccroché, de nombreuses informations gèrent la communication téléphonique. Ces informations constituent la signalisation. Lors de l'établissement d'une communication, des informations de signalisation sont échangées entre l'usager et le réseau : le décroché, l'invitation à numéroter, la numérotation, le retour d'appel, le décroché du correspondant..., cette signalisation est dite « signalisation Usager/Réseau ». D'autres, nécessaires à l'établissement du

6. Les touches A, B, C, D sont, en principe, réservées à des applications militaires.

circuit et à la supervision du réseau, n'intéressent que le réseau, c'est la signalisation réseau. Deux modes de transport des informations de signalisation sont utilisés en téléphonie.

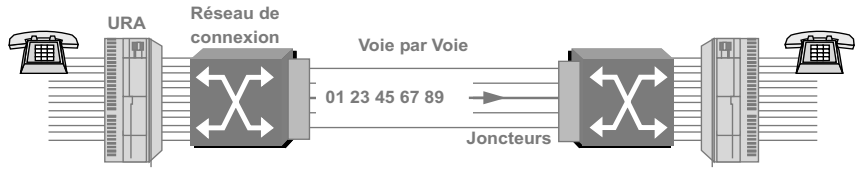


Figure 20.12 La signalisation voie par voie.

Dans la signalisation **voie par voie** (figure 20.12) ou signalisation **CAS** (*Channel Associated Signalling*), une voie de communication correspond une voie de signalisation, la signalisation est associée à la communication. Ce qui nécessite, pour qu'elle soit transmise, l'établissement préalable d'un circuit. Cette signalisation est dite en mode événement, c'est-à-dire qu'à un événement spécifique est associé un état électrique (impulsion...). La numérotation, nécessaire à l'établissement du circuit, ne peut qu'être transmise sur les fils de voix au fur et à mesure de la construction de la voie, ce qui évidemment allonge le temps d'établissement. La signalisation voie par voie peut être dans la bande (Amérique du Nord et Japon) ou hors-bande. Elle a pratiquement disparu des réseaux publics mais subsiste sur la ligne de raccordement d'un usager analogique et dans de nombreuses installations téléphoniques privées.

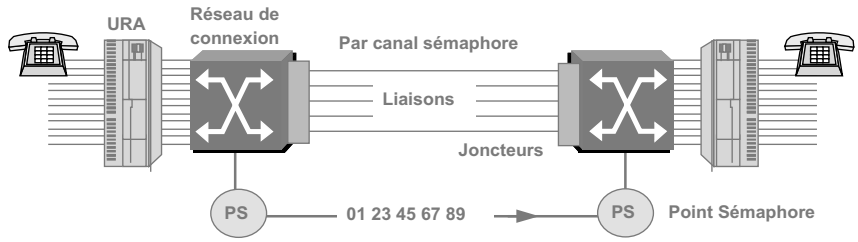


Figure 20.13 La signalisation par canal sémaphore.

La signalisation par **canal sémaphore** (figure 20.13) ou signalisation **CCS** (*Common Channel Signaling*) utilise un canal spécifique (multiplexage avec les voies de communication). Non dédiée à une communication particulière, elle signale tous les événements relatifs à un ensemble de circuits. La numérotation est acheminée sur le canal sémaphore en mode message. Le protocole de signalisation peut être normalisé ou propriétaire (protocole propre à un constructeur).

20.4 L'ÉVOLUTION DE LA TÉLÉPHONIE, LE RNIS

20.4.1 De l'accès analogique à l'accès numérique

La numérisation du réseau nécessite une conversion analogique/numérique en entrée du réseau et numérique/analogique en sortie. Un usager qui désire utiliser *n* communications téléphoniques simultanées doit être raccordé par *n* lignes (lignes groupées, les lignes groupées sont vues, pour le réseau, sous un même numéro). La numérisation autorise très simplement le multiplexage, d'où

© Dunod – La photocopie non autorisée est un délit

l'idée de réaliser des liaisons numériques de bout en bout, une seule ligne physique peut alors acheminer plusieurs communications téléphoniques (figure 20.14).

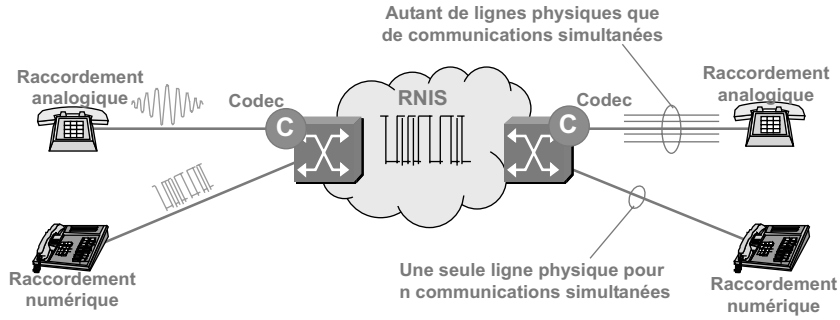


Figure 20.14 De l'analogique au numérique.

En réservant un IT (Intervalle de temps) à la signalisation (débit de 64 kbit/s), on peut l'acheminer, *via* un protocole de haut niveau, en mode message. De ce fait, la signalisation peut être enrichie et autoriser de nombreux services nouveaux, c'est le **RNIS** (Réseau numérique à intégration de service ou **ISDN**, *Integrated Service Digital Network*).

20.4.2 Le concept d'intégration de services

Le RNIS est une approche service du réseau téléphonique devenu alors le réseau unique qui permet, à partir d'un seul raccordement, de disposer à la fois de services voix (téléphonie), vidéo (visiophonie, téléconférence[7]), de transmission de données en mode paquet ou autre et de la transmission de l'écrit (télécopie). La figure 20.15 schématise cette évolution, en RNIS, si un télécopieur initialise un appel, seul le télécopieur de l'installation destination « sonne ».

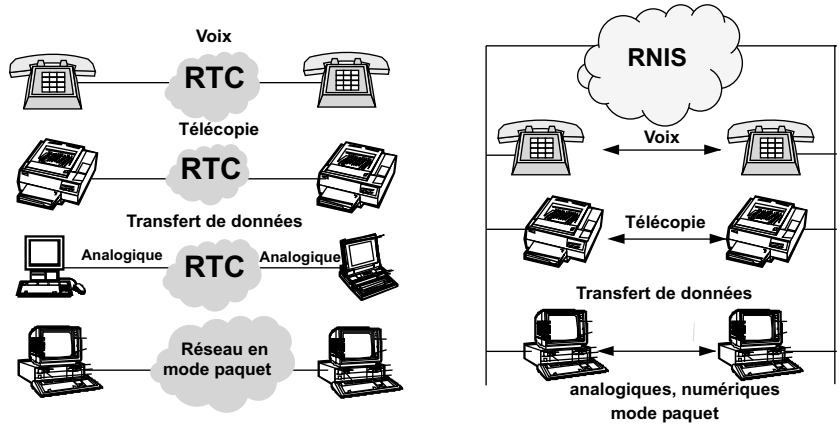


Figure 20.15 L'évolution des accès avec le concept RNIS.

7. La visiophonie est un service vidéo associé à téléphonie, les correspondants se voient durant la communication. La téléconférence consiste en l'organisation de conférences vidéo à partir d'un studio de télévision.

Le raccordement de terminaux différents (voix, données, images) sur une même ligne nécessite une signalisation spécifique et enrichie qui permette, à la fois, l'identification du terminal et le type de service requis. C'est ainsi, que le RNIS distingue les canaux de transmission (transport) de données ou canaux B établis appel par appel (circuits commutés), du canal de signalisation ou canal D établi de manière permanente et transportant les informations nécessaires à l'établissement du circuit (adresse, type de service invoqué...).

Lors de l'émission d'un appel, les données de signalisation sont acheminées sur le canal D. Elles comportent les informations en relation avec le numéro de l'appelé et le type de service invoqué... Ainsi, dans l'exemple de la figure 20.16, l'appel émis à partir du télécopieur de l'appelant invoquera un service de télécopie chez l'abonné distant. Seul alors un télécopieur répondra à cet appel. Le téléphone (service voix) de l'installation a bien reçu l'appel mais non concerné par le service invoqué, ne sonne pas.

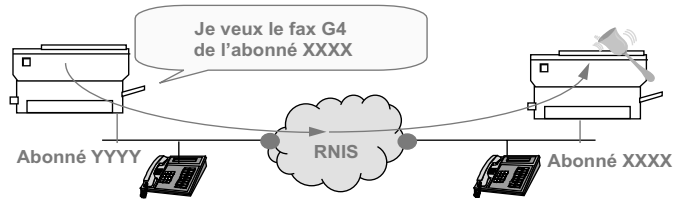


Figure 20.16 L'accès direct au service demandé.

20.4.3 La structure du réseau

Un terminal RNIS utilise deux connexions : une connexion commutée (canal B, *Bearer channel*) utilisée pour le transport des informations utilisateur à 64 kbit/s (voix, données et images) et une connexion permanente sur le canal de signalisation (canal D, *Data channel*) de 16 ou 64 kbit/s selon le type d'installation. Des débits plus importants peuvent être obtenus par agrégation de plusieurs canaux B, on parle alors de canaux H (*High speed channel*) qui offrent un débit de 384 kbit/s (H_0), 1 536 kbit/s (H_{11}) ou de 1 920 kbit/s (H_{12}). La figure 20.17 illustre le principe de raccordement d'un terminal au réseau RNIS.

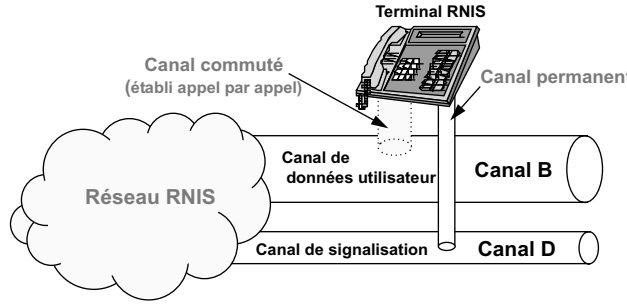


Figure 20.17 Les connexions d'un terminal RNIS.

La connexion permanente du terminal au canal de signalisation rend obsolète la notion de terminal occupé : le terminal peut toujours être alerté d'un appel entrant et recevoir, *via* le canal D, des

© Dunod – La photocopie non autorisée est un délit

messages (minimessages). Le RNIS est donc un système de transmission utilisant deux réseaux distincts : un réseau de transmission (commutation de circuits) et un réseau de signalisation (commutation de paquets). Les réseaux sont fonctionnellement différents[8]. Ils utilisent les mêmes capacités de transport (multiplexage) mais les commutateurs sont différents, bien que situés sur les mêmes sites. La figure 20.18 illustre ce concept.

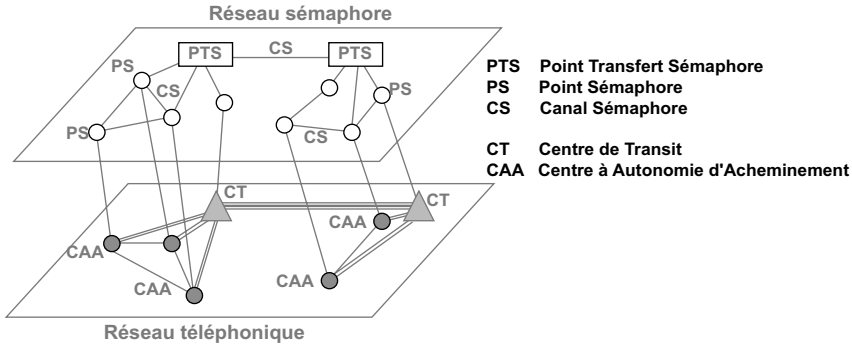


Figure 20.18 Le réseau téléphonique et réseau sémaphore.

20.4.4 Le raccordement d'usager

Les accès RNIS

L'accès au réseau RNIS s'effectue par l'intermédiaire d'interfaces normalisées appelées points de référence (recommandation I.411 de l'UIT) et dépendant du type de terminal à raccorder. Les terminaux n'accèdent pas directement au réseau, ils y sont raccordés via des interfaces. Selon le type d'abonnement au réseau, l'équipement d'interfaçage entre l'installation d'abonné et le réseau porte le nom de **TNR** (Terminaison numérique de réseau) ou de **TNL** (Terminaison numérique de ligne). La **TNA** (Terminaison numérique d'abonné) est un équipement facultatif, généralement un commutateur téléphonique privé (**PABX**, *Private Branched eXchange*). Lorsque l'installation d'abonné ne comporte pas de TNA, les points de référence S et T sont confondus.

Les divers points de référence (figure 20.19) sont, par ordre alphabétique, du privé vers le réseau public :

- **Point R**, interface pour les terminaux non RNIS, c'est notamment le cas des terminaux dotés d'une interface V.24/28, X.21, V.35...
- **Point S**, point d'accès universel pour les équipements compatibles RNIS,
- **Point T** matérialisant la limite entre le réseau public et l'installation d'abonné, c'est aussi la frontière de responsabilité entre l'opérateur et l'abonné,
- **Point U**, il symbolise la limite entre le réseau de transport et la liaison d'abonné.

8. Le réseau RNIS n'est pas un réseau indépendant de tout autre réseau, il est complètement intégré dans le réseau de l'opérateur et en particulier dans son réseau téléphonique traditionnel quand celui-ci subsiste.

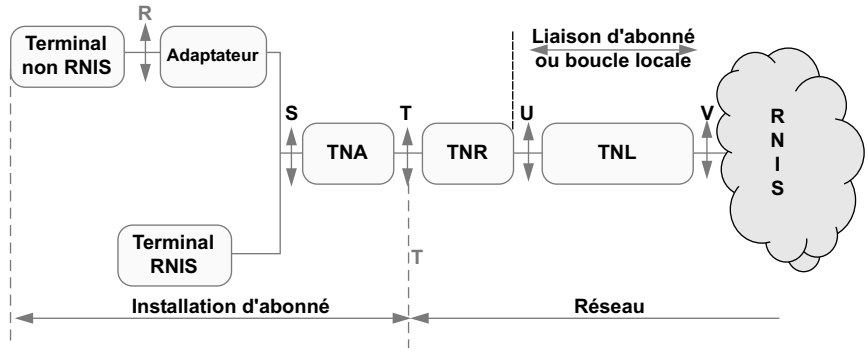


Figure 20.19 Les points de référence des accès au RNIS.

L'offre RNIS se décline selon la combinaison des trois types de canaux mis à disposition :

– les **canaux B** *(Bearer)* sont les canaux de transfert d'information, le débit nominal est de 64 kbit/s par canal ;

– le **canal D** (*Data*), à 16 ou 64 kbit/s selon le nombre de canaux B offerts, est dédié au transfert de la signalisation (protocole D). La bande non utilisée par la signalisation peut être utilisée pour transférer des données en mode paquet (accès aux réseaux X.25) ;

– les **canaux H** (*High Speed*), combinaison de n canaux B à 64 kbit/s, offrent un débit de $n \times 64$ kbit/s. On distingue les canaux H_0 à 384 kbit/s, H_{11} à 1 536 kbit/s et H_{12} à 1 920 kbit/s. Les différents canaux B constituant le canal H sont établis indépendamment les uns des autres, il n'y a donc aucune garantie qu'ils empruntent tous le même chemin (désynchronisation des données).

Selon le nombre de canaux offerts, on définit trois types d'accès, dont seuls deux sont disponibles en France :

– **T0**, ou accès de base (**BRI**, *Basic Rate Interface*), offre un débit de 192 kbit/s dont 144 utiles, soit 2 canaux B et un canal D à 16 kbit/s,

– **T1**, non disponible en France,

– **T2**, ou accès primaire (**PRI**, *Primary Rate Interface*) offre 15, 20, 25 ou 30 canaux B et un canal D à 64 kbit/s. Soit, pour 30 canaux B un débit de 2 048 kbit/s dont 1 920 utiles.

Les accès peuvent être regroupés en « groupement d'accès » (plusieurs accès pour un même site qui sont vus comme un seul faisceau). Le groupement d'accès de base est, en principe, limité à 6 accès de base.

L'installation d'abonné

Généralement, les terminaux RNIS sont reliés selon une topologie en bus. Si l'installation est directement connectée à la TNR, elle est dite à bus passif ; elle est dite à bus unique ou étoile de bus lorsque le (ou les bus) est (sont) raccordé(s) par l'intermédiaire d'un équipement local (TNA). La figure 20.20 représente ces différents modes de raccordement.

© Dunod – La photocopie non autorisée est un délit

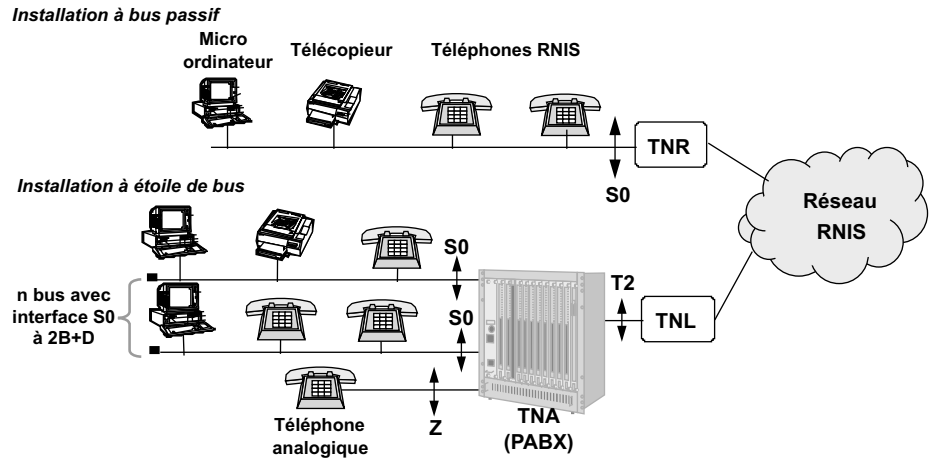


Figure 20.20 La structure des installations d'abonné.

20.4.5 Les services du RNIS

Les réseaux RNIS donnent accès à trois types de services : les services supports pour le transfert d'information (couches 1 à 3 du modèle OSI) ; les téléservices qui sont des services complets (téléphonie, télécopie...) correspondant aux couches 1 à 7 du modèle OSI (figure 20.21). Enfin, des compléments de services, optionnels et facturés en sus de l'abonnement, étendent les possibilités du service transport ou des téléservices.

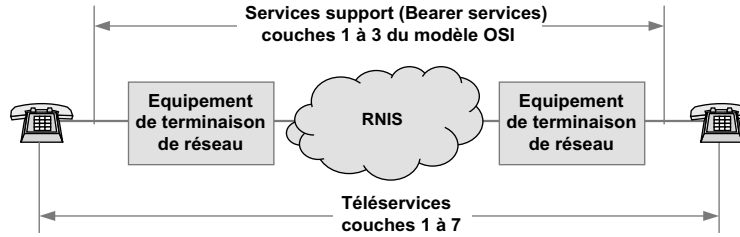


Figure 20.21 Le modèle OSI et services RNIS.

Le service support

Le service support est un service de transport d'information de bout en bout entre deux interfaces. Le RNIS offre trois types de service support : le service téléphonique, le service numérique sur canal B (transparent aux protocoles) et le mode paquet sur le canal D.

Le service téléphonique correspond aux services traditionnels existants sur le réseau téléphonique commuté, c'est-à-dire les services ne requérant qu'une bande analogique de 300-3 400 Hz. Dans ce type de service, dit de « qualité vocale », la continuité numérique n'est pas garantie de bout en bout, certaines artères empruntées peuvent être analogiques. C'est, par exemple, le cas d'un abonné RNIS appelant un abonné non RNIS (téléphonie à 3,1 kHz, télécopie groupe 3, modem audiofréquence, Minitel...). Ce service est désigné par le sigle **CCBNT** (Circuit commuté B non transparent). Le service numérique garantit une qualité numérique de bout en bout. Il est utilisé

pour les applications informatiques à faible ou moyen débit ($\leqslant$ 64 kbit/s), la télécopie groupe 4, la téléphonie 7 kHz, l'audio et la visioconférence. Ce service est désigné sous le nom de **CCBT** (Circuit commuté B transparent).

Les services CCBNT et CCBT sont offerts sur le canal B. C'est le terminal appelant qui effectue la demande de qualité de service en positionnant l'élément d'information « Mode de fonctionnement », du message d'établissement, à 16 pour le service CCBT ou à 32 pour le service CCBNT. Un appel téléphonique est toujours établi en CCBNT.

Toute la bande passante du canal D n'est pas utilisée intégralement pour la signalisation. Ce lien étant établi de manière permanente, la bande disponible peut être utilisée pour réaliser un accès permanent[9], à 9 600 bit/s, aux réseaux en mode paquet X.25.

Les téléservices

Les téléservices sont des services de bout en bout entre deux terminaux couvrant l'intégralité des fonctions des couches 1 à 7. La signalisation assure la compatibilité entre les terminaux vis-à-vis des services invoqués. C'est ainsi, par exemple, qu'à un appel entrant provenant d'un télécopieur groupe 3, seul répondra un télécopieur groupe 3. Les téléservices normalisés sont : la téléphonie 3,1 kHz, la téléphonie 7 kHz, le vidéotex (minitel), la télécopie groupe 3 et 4, la vidéoconférence... Ces services sont accessibles par un terminal RNIS (interface S) ou un terminal analogique *via* un adaptateur audiofréquences.

Les compléments de service

Les compléments de service correspondent essentiellement à un enrichissement de l'offre téléphonique, ils concernent le service support et les téléservices. Ces prestations optionnelles donnent lieu à facturation (abonnement ou appel par appel).

➤ Coût total, Indication de coût

L'usager peut obtenir, en fin de communication, le coût total de la communication ou, durant la communication suivre l'évolution du coût de celle-ci (Indication de coût). Ces prestations ne fournissent que le coût global exprimé en unités téléphoniques (UT) de la communication au temps, sans tenir compte des compléments de service éventuellement invoqués.

➤ Présentation d'appel, double appel, va-et-vient

Durant la communication, si un nouvel appel survient, l'usager en est averti (présentation d'appel). Celui-ci peut achever la communication en cours et prendre la nouvelle, ou mettre la communication en cours en attente et prendre la communication entrante (double appel). L'usager peut aussi passer alternativement de l'une à l'autre (va-et-vient). L'usager ne peut prendre une troisième communication, celle-ci lui est cependant présentée.

➤ Identification d'appel, non-identification, identification d'appel malveillant

Un appel entrant est présenté avec l'identification de l'appelé (Identification d'appel) sauf si l'appelant a souscrit au complément de service « non-identification d'appel ». L'identification d'appel malveillant permet à un usager de faire identifier par l'opérateur l'auteur d'un appel malveillant.

9. Ce service a été étudié au chapitre 14 § 14.1.3, *Les accès aux réseaux X.25*.

© Dunod – La photocopie non autorisée est un délit

➤ Portabilité

C'est la faculté dont dispose l'usager, durant un appel, de suspendre une communication et de reprendre celle-ci plus tard sur le même poste au même endroit ou sur le même poste déplacé dans l'installation ou encore sur un autre poste de la même installation. La suspension de l'appel n'interrompt pas la facturation. Elle est limitée à trois minutes.

➤ Renvoi du terminal, transfert d'appel national

Un utilisateur peut faire réacheminer ses appels sur un autre poste de l'installation (Renvoi d'appel) ou sur un autre poste d'une autre installation (Transfert d'appel national). Le renvoi d'appel peut être inconditionnel, sur occupation ou sur non-réponse.

➤ Minimessage (signalisation d'usager à usager)

Cette facilité permet aux usagers de s'échanger, en dehors de toute communication lors des phases d'établissement ou de libération de la communication, des messages de 32 caractères (minimessage).

➤ Services restreints

Ce complément de service permet de limiter l'usage d'un poste aux communications locales, de voisinage ou nationales.

➤ Sous-adresse

Cette information complète l'adresse du terminal, soit pour distinguer celui-ci, soit pour sélectionner sur celui-ci un service particulier (ex. : terminal multimédia). La sous-adresse peut contenir jusqu'à 40 caractères IA5. La sous-adresse est transportée de manière transparente par le réseau.

➤ Sélection directe à l'arrivée (SDA)

La sélection directe à l'arrivée permet de joindre directement un terminal de l'installation sans nécessiter le recours à un(e) standardiste. C'est l'équipement local de l'abonné (PABX) qui effectue la relation entre le numéro SDA appelé et le numéro interne du poste demandé. Généralement, ces deux numéros correspondent. Le numéro local attribué au poste correspond alors au MCDU du réseau public (quatre derniers chiffres du numéro public d'abonné).

Un numéro SDA est un service, le nombre de SDA d'une installation est indépendant du nombre de lignes de raccordement (canaux B) de l'installation. Les numéros SDA fournis peuvent être consécutifs ou disjoints. Soit, par exemple, pour une série de 100 numéros, les numéros M000 à M099 ou M000 à M0050 et M550 à M599 où M représente le chiffre des milliers.

20.4.6 La signalisation et le réseau RNIS

Généralités

Le RNIS utilise trois signalisations transportées dans deux protocoles (figure 20.22) :

- une signalisation usager/réseau ou protocole D ;
- une signalisation usager/usager pour les téléservices ;
- une signalisation interne au réseau transporté par un réseau de signalisation. Conforme à l'avis UIT ou CCITT N° 7, elle assure le transport de la signalisation protocole D (signalisation usager/réseau) et de la signalisation usager/usager.

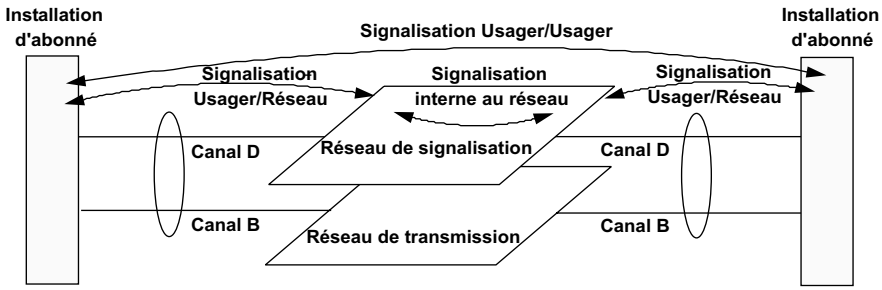


Figure 20.22 La signalisation et la transmission dans un réseau RNIS.

La signalisation Usager

➤ Généralités

Les données de signalisation (niveau 3 du modèle OSI) entre le réseau et l'usager sont échangées en mode paquet. Le niveau 2 utilise une variante de HDLC, le protocole **LAP-D** (*Link Access Protocol on the D channel*). Les terminaux RNIS sont reliés en bus multipoint, il est donc nécessaire de les distinguer. L'adressage des terminaux (**TEI**, *Terminal End point Identifier*) et la désignation du service requis (**SAPI**, *Service Access Point Identifier*) se substituent au champ Adresse d'HDLC (protocole en point à point). Hors ces différences, les fonctions de LAP-D sont similaires à celles d'HDLC.

La figure 20.23 montre l'encapsulation des données et l'organisation de la trame multiplexée pour un accès de base (2B+D), les différents champs seront expliqués par la suite. La trame multiplexée comporte en outre des bits d'écho du canal D (Bit E), des bits d'équilibrage de la composante continue (Bit L), des bits de synchro (Bit Q)...

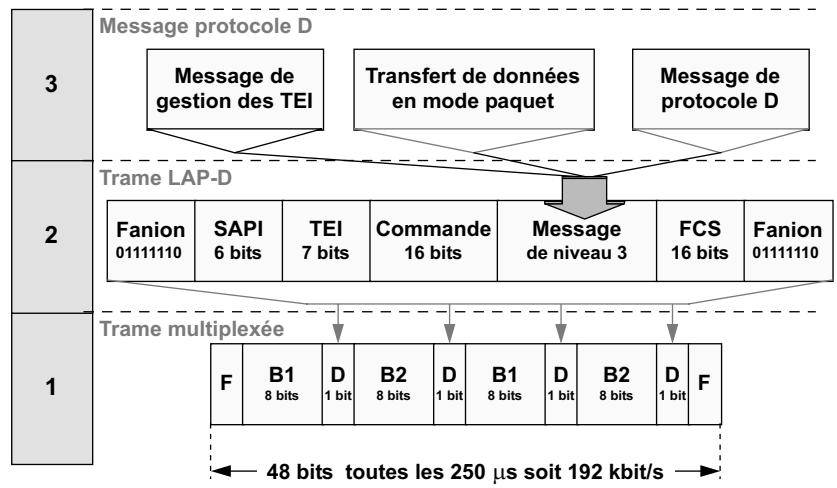


Figure 20.23 L'organisation générale de la trame multiplexée.

© Dunod – La photocopie non autorisée est un délit

➤ Adressage des terminaux (TEI/SAPI)

Dans une configuration multipoint, les terminaux sont donc en compétition pour l'accès au canal D. De ce fait, à l'instar des réseaux locaux, il est nécessaire :

– d'identifier chaque terminal (adresse terminal) ;
– de définir le protocole de niveau supérieur ici, le service invoqué ;
– de résoudre les confits d'accès (collisions).

Le champ adresse de LAP-D se subdivise en deux sous-champs (figure 20.22) :

– le sous-champ **TEI** (*Terminal End-Point Identifier*) sur 7 bits identifie le terminal proprement dit. Cette adresse est similaire à l'adresse MAC des réseaux locaux. Les TEI peuvent être attribués par le constructeur (TEI de 0 à 63) ou par le réseau. La TNR (Terminaison numérique de réseau) attribue dynamiquement les TEI de 64 à 126. Le TEI 127 est réservé à la diffusion de message. Lorsqu'un terminal à allocation automatique de TEI est connecté au bus, il demande au réseau de lui attribuer un TEI, alors qu'un terminal à affectation non automatique s'assure de l'unicité de son TEI. Un terminal multifonction peut utiliser plusieurs TEI, un par fonction ;
– le sous-champ **SAPI** (*Service Access Point Identifier*) sur 6 bits indique le type de message transporté dans le champ Information de la trame (identification du service requis). Les SAPI 32 à 47 sont réservés pour des usages nationaux, par exemple, en France le SAPI 32 est réservé au Télétex. La figure 20.24 présente les principaux SAPI utilisés.

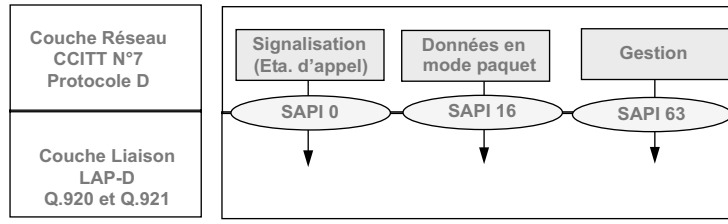


Figure 20.24 L'affectation des principaux SAPI.

➤ Les mécanismes d'accès au canal D et codage

Reliés en bus, les terminaux accèdent, au canal D, en compétition. Les conflits d'accès au canal D sont résolus par le protocole **CSMA/CR** (*Carrier Sense Multiple Access Contention Resolution*, accès multiple avec écoute de porteuse et résolution des collisions).

Le principe général de l'accès au canal D est similaire à celui utilisé dans les réseaux locaux de type « Ethernet ». Cependant, le support physique étant multiplexé, il peut y avoir une activité électrique sur celui-ci (canal B) alors que le canal D est libre. L'écoute doit se faire au niveau du canal et non du support. Pour détecter et prévenir une éventuelle collision, toutes les données émises sur le canal D sont retransmises par la TNR sur un **canal d'écho** (**canal E**, figure 20.25). La station vérifie en permanence que ce qu'elle reçoit sur le canal E correspond bien à ce qu'elle a émis sur le canal D. Si ce n'est pas le cas la station s'arrête (collision). En l'absence d'émission, un terminal émet des « 1 » (potentiel électrique 0). Lorsqu'il désire accéder au canal D, le terminal écoute celui-ci, s'il ne détecte aucune activité durant un certain délai (8 à 11 temps bits selon le message à émettre), il émet sa trame LAP-D.

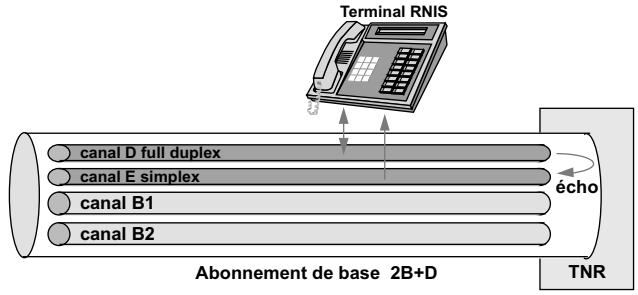


Figure 20.25 Le terminal émet sur le canal D et écoute l'écho sur le canal E.

Afin d'éviter que toutes les stations en conflit ne s'arrêtent, un mécanisme de résolution de la contention (CSMA/CR) assure qu'une station, et une seule, pourra poursuivre son émission. Le système repose sur le codage retenu pour les signaux électriques, les 0 logiques correspondent à l'émission d'une tension alternativement positive ou négative (élimination de la composante continue), tandis que les 1 logiques correspondent à une tension nulle. Ce codage, appelé codage pseudo-ternaire, est représenté figure 20.26.

La répétition, par le canal E, des données du canal D est telle que, pour tout 1 émis, le canal E retransmet un 1 (tension nulle), pour tout 0 émis, le canal E retransmet un 0. C'est-à-dire que l'émission d'un 0 par une station masque l'émission d'un 1 par une autre. Ce mécanisme, illustré figure 20.26, autorise la résolution des conflits d'accès. Au temps d'horloge 1, 2, 3 et 4 les signaux émis sur le canal E correspondent à ceux émis par les divers terminaux, ceux-ci poursuivent leur émission.

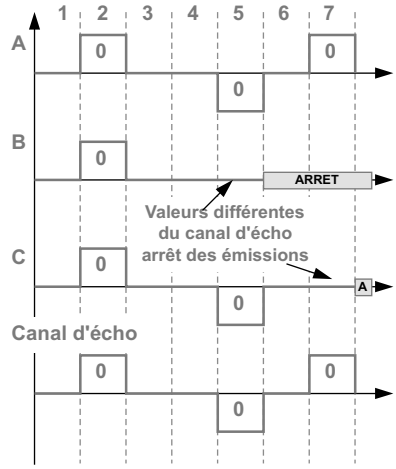


Figure 20.26 Le mécanisme de résolution des contentions.

Au temps 5, le canal E retransmet le 0 des stations A et C, la station B qui avait émis un 1 cesse ses émissions. Au temps 7, c'est la station C qui a un écho différent, elle arrête ses émissions. Seule, la station A continue d'émettre. Ce mécanisme ne peut fonctionner que si toutes les stations

© Dunod – La photocopie non autorisée est un délit

émettent le premier 0 de la trame avec la même polarité, sinon deux 0 de polarité inverse s'annuleraient (niveau électrique nul). De ce fait, la règle d'alternance des 0 n'est pas respectée et la valeur continue peut ne plus être nulle, des bits d'équilibrage sont alors insérés dans la trame.

Trame LAP-D	Fanion	00 SAPI	1 TEI
TEI = 1	01111110	00 000000	1 0 0 0 0 0 1
TEI = 2	01111110	00 000000	1 0 0 0 0 1 **0**
TEI = 5	01111110	00 000000	1 0 0 0 1 **0** 1
Canal E			0 0 0 0 0 1

La station 5 s'arrête
La station 2 s'arrête

Figure 20.27 La priorité au terminal de plus faible adresse.

Le mécanisme adopté favorise les terminaux de plus faible adresse (figure 20.27). Pour compenser la priorité ainsi octroyée, une station qui a réussi à transmettre devra écouter le canal durant un temps bit de plus (9, au lieu de 8, pour les messages de signalisation et 11, au lieu de 10, pour les transmissions de données).

➤ Le niveau 2 : LAP-D (UIT I.440/Q.920 et I.441/Q.921)

Le niveau 2 du RNIS est chargé d'assurer la transmission des trames entre un terminal et le réseau. Les fonctions assurées sont conformes au modèle de référence :

– ouverture et fermeture de session,
– détection et récupération des erreurs,
– numérotation des trames,
– contrôle de flux.

Hors l'adressage multipoint (adressage TEI/SAPI), le format de la trame LAP-D est similaire à celui du LAP-B (figure 20.28). Le protocole LAP-D utilise le format étendu (numérotation des trames modulo 128), la longueur maximale des trames est fixée à 260 octets.

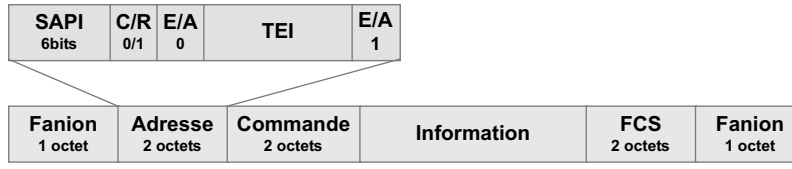


Figure 20.28 Le format de la trame LAP-D.

Le champ Adresse comporte les champs SAPI et TEI décrits plus haut. Le bit **E/A** (*End Address*, champ d'extension d'adresse) est à 0 dans le premier octet et à 1 dans le second (Fin du champ d'adresse). Enfin, le bit **C/R** (*Command/Response*) distingue les trames de commande (C/R = 0) des trames de réponse (C/R = 1).

LAP-D utilise les trames UI (*Unnumbered Information*) pour échanger des messages hors connexion (messages d'établissement, messages de gestion des TEI...). Le format du champ d'information est illustré en figure 20.29.

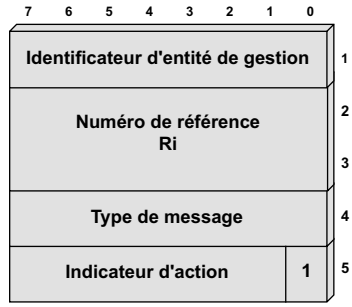


Figure 20.29 Le format des messages des trames UI.

La gestion des TEI

Les procédures de gestion des TEI comprennent les procédures permettant l'affectation, le contrôle et la suppression d'un TEI. Le format des messages de gestion des TEI a été fourni en figure 20.29, la signification et l'utilisation des différents champs sont indiquées dans la figure 20.30.

Messages	Identificateur d'identité	Référence interne (Ri)	Type de message	Indicateur d'action (Ai)
Demande d'identité U → R	0000 1111	0-65535	0000 0001	Ai = 127 tout TEI est acceptable
Identité affectée R → U	0000 1111	0-65535	0000 0010	Ai = 64 à 126 valeurs attribuées au terminal
Identité refusée R → U	0000 1111	0-65535	0000 0011	Ai = 64 à 126, valeurs refusées Ai = 127, pas de TEI disponible
Demande de contrôle d'identité R → U	0000 1111	Non utilisée mise à 0	0000 0100	Ai = 127, contrôler tous les TEI Ai = 0 à 126, valeur du TEI à contrôler
Réponse à contrôle d'identité U → R	0000 1111	0-65535	0000 0101	Ai = 0 à 126 valeur du TEI déjà affectée
Suppression d'identité U → R	0000 1111	Non utilisée mise à 0	0000 0110	Ai = 127, suppression de tous les TEI attribués ; Ai = 0 à 126 TEI à supprimer

Figure 20.30 Les codes des messages de gestion des TEI.

La figure 20.31 décrit un échange protocolaire d'affectation de TEI. Le terminal qui vient d'être raccordé au réseau lui demande de l'identifier (affectation d'un TEI, Type de message = 1). Le message est adressé à l'entité de gestion 63 (SAPI = 63), le champ Ai à 127 précise au réseau que toute valeur est acceptable par le terminal.

La référence d'appel (Ri) est un nombre aléatoire compris entre 0 et 65 535, elle permet de distinguer d'éventuelles demandes simultanées. Le réseau peut affecter une valeur (Type de message = 2) ; dans ce cas, le champ Ai contient la valeur affectée (TEI = 64 à 126), il peut aussi refuser l'affectation (pas de TEI disponible), le type de message est alors 11 et le champ Ai contient 127.

© Dunod – La photocopie non autorisée est un délit

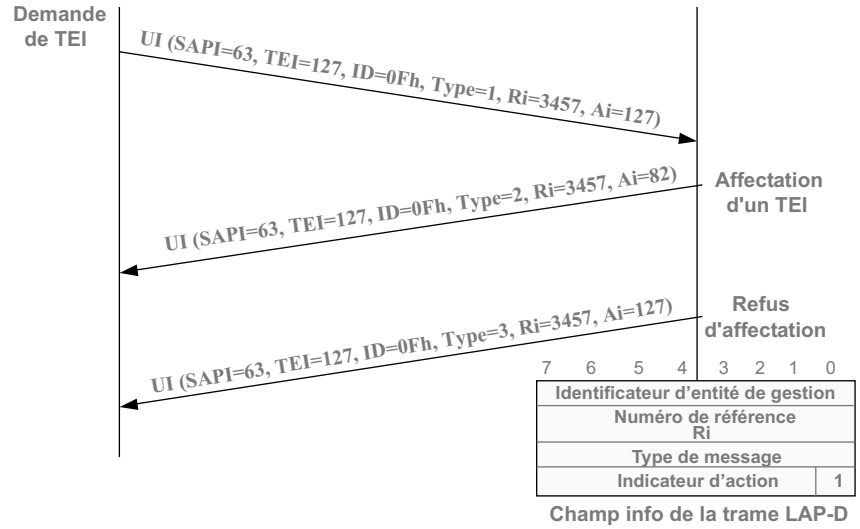


Figure 20.31 L'affectation d'un TEI à un terminal.

➤ Le niveau 3 : le protocole D (UIT I.450 et I.451)

Le protocole D gère les connexions (établissement, maintien et libération), il assure le transfert d'information usager/usager et la mise en œuvre des compléments de service. Le protocole D est véhiculé sur le canal D. La structure générale des messages est donnée par la figure 20.32.

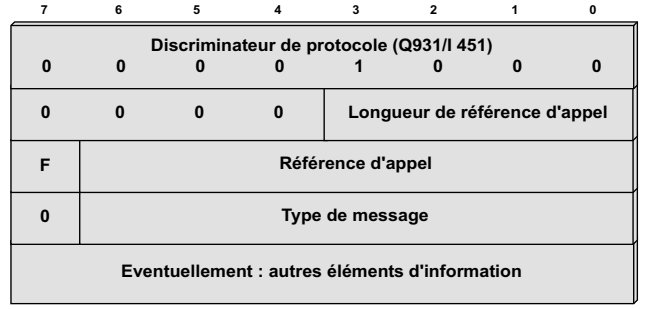


Figure 20.32 La structure du message.

Dans ce message, le premier octet est utilisé pour identifier le protocole Q.931 qui régit les échanges de messages usager/réseau. La référence d'appel identifie une connexion, elle n'a qu'une valeur locale (de manière similaire au NVL en X.25). Le bit F (fanion) permet de déterminer l'origine de l'appel (F = 0, message en provenance de l'origine d'appel ; F = 1, message en provenance du récepteur de l'appel). L'octet suivant identifie les différents types de message.

Les différents types de message sont :

– messages d'établissement d'appel (alerte, connexion, établissement...) ;
– messages d'information de l'appel (reprise, suspension...) ;
– messages de libération d'appel (déconnexion, libération, fin de libération) ;
– messages divers (information, facilité...).

L'étude détaillée de ces messages sort du cadre de cet ouvrage[10]. Cependant, citons par exemple, les éléments d'information d'un message d'établissement :

– mode de fonctionnement du support (parole, informations numériques...) ;
– identification de l'accès (accès de base, accès primaire, canal requis D ou B) ;
– compatibilité avec les couches supérieures (normes UIT ou CEPT) ;
– téléservice demandé (téléphonie, télécopie G3 ou G4, télétex, vidéotex, télex, application ISO...).

La figure 20.33 représente les échanges de messages pour un appel entrant ; les deux postes de l'installation y répondent (sonnent), le poste qui décroche en premier obtient la communication. À la réception de l'appel entrant, le réseau émet une trame UI, trame d'information non numérotée permettant l'envoi du message d'établissement à tous les terminaux (TEI 127) en mode non connecté. Les terminaux 64 et 65 répondent, ils émettent vers le réseau une demande de connexion (**SABME**, *Set Asynchronous Balanced Mode Extended*, niveau trame) et déclenchent la sonnerie du poste. Le réseau accuse réception de cette demande de connexion (**UA**, *Unnumbered Acknowledgement*). La connexion étant établie, les terminaux adressent une alerte au réseau, l'appelant reçoit une indication d'appel (retour de sonnerie).

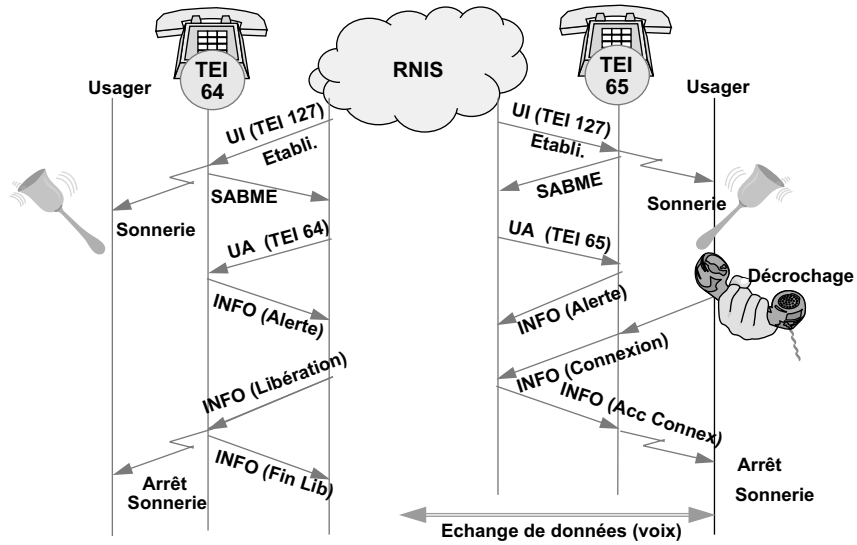


Figure 20.33 Le diagramme des échanges lors d'un appel entrant.

Un utilisateur décroche le poste 65 (TEI 65), une demande de mise en relation est émise (Demande de connexion). Le réseau accepte cette demande (ACC_Connex) et libère (LIB) le poste 64 (TEI 64). Celui-ci arrête la sonnerie et accuse réception de la libération (FIN_LIB). L'échange d'information a alors lieu entre l'appelant et le poste 65.

10. Pour illustrer le fonctionnement du protocole D, une analyse de trace du protocole D est fournie en exercice.

© Dunod – La photocopie non autorisée est un délit

La signalisation interne au réseau

➤ Objet

La signalisation interne au réseau par canal sémaphore ou système N° 7 (**SS7**, *Signaling System 7*) définit les protocoles d'échange d'information de signalisation dans un réseau numérique entre :

– deux commutateurs pour l'établissement, l'administration et l'arrêt des communications ;
– un commutateur et une base de données pour la fourniture de services spécifiques (réseaux intelligents).

➤ Mode de fonctionnement

La signalisation sémaphore est du type hors bande. Cependant, selon le type de relation établi entre les points de signalisation, on distingue 3 modes de fonctionnement (figure 20.34) :

– le **mode associé**, les commandes en relation avec les circuits entre deux commutateurs sont acheminées par un canal sémaphore reliant directement ces deux commutateurs ;
– le **mode non associé**, les commandes des circuits entre deux commutateurs transitent dans le réseau par des routes non prédéterminées ;
– le **mode quasi associé**, les commandes des circuits transitent par des nœuds (PTS, Point de transfert sémaphore) prédéterminés (routage fixe).

Le réseau SS7, hors panne ou incident, utilise le mode quasi associé ce qui, dans un réseau datagramme, permet de garantir le séquencement des informations.

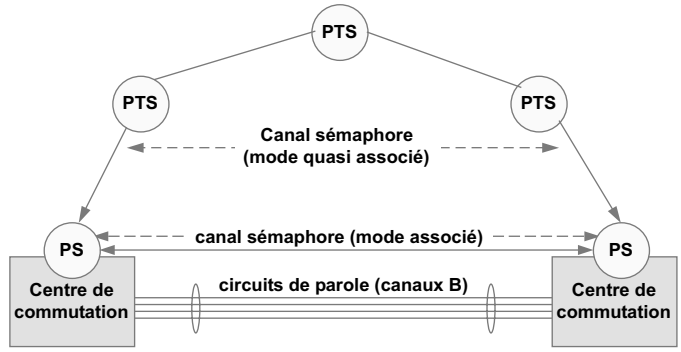


Figure 20.34 Les modes de fonctionnement d'un canal sémaphore.

➤ Architecture du système

La signalisation utilise une infrastructure de communication redondante qui forme le réseau de signalisation (voir figure 20.18). L'architecture du système de signalisation comporte deux sous-ensembles (figure 20.35).

Le sous-système de transfert de message (**SSTM**) ou **MTP** (*Message Transfer Part*) correspond aux couches 1 à 3 du modèle OSI. Le niveau 1 (SSTM1) définit le transport de l'information dans un canal à 64 kbit/s (IT16 d'un multiplex primaire à 2,048 Mbit/s). Le niveau 2 (SSTM2) assure le transfert fiable des messages entre équipements du réseau. Le protocole, semblable à HDLC, permet la détection et la reprise sur erreur des trames ainsi que le contrôle de

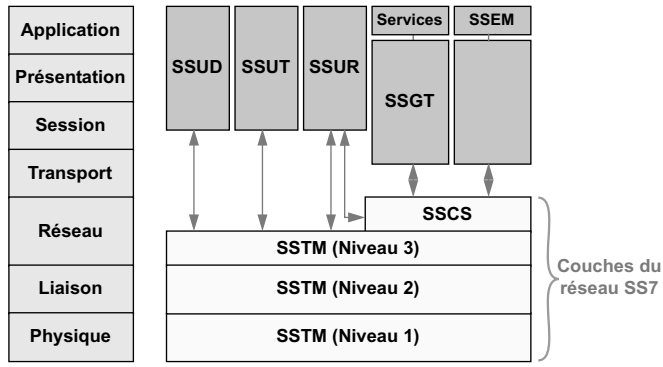


Figure 20.35 L'architecture du système 7.

flux. Le niveau 3 (SSTM3) assure l'acheminement des messages dans le réseau (routage, réseau en mode datagramme). Chaque **PS** (Point de signalisation) est identifié par un code (*Point Code* sur 14 bits), le routage est du type fixe, ce qui garantit le séquencement hors panne du réseau. La structure des messages de niveau 3 est donnée en figure 20.36.

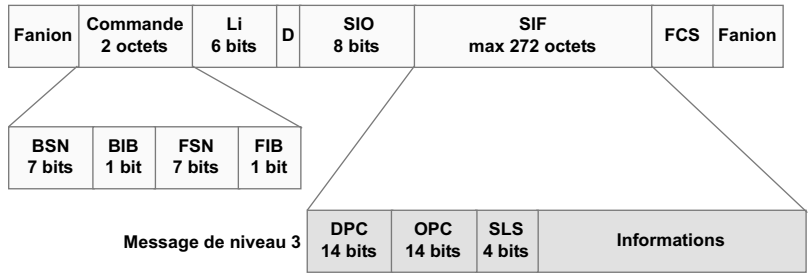


Figure 20.36 Le format général des messages SS7.

Les sous-systèmes utilisateurs (**SSU**) ou **UP** (*User Part*) comportent :

- le sous-système utilisateur de données (**SSUD**) assure la signalisation dans les réseaux à commutation de données en mode circuit. Ce sous-système n'est pas utilisé dans le RNIS ;
- le sous-système utilisateur téléphonique (**SSUT**) assure la signalisation des communications téléphoniques ;
- le sous-système utilisateur RNIS (**SSUR**) définit les procédures de commande d'appel dans le RNIS ;
- le sous-système de commande de connexion de signalisation (**SSCS**) permet l'échange de messages de signalisation hors mode circuit. Ce système constitue une interface entre le système de transport et le système de gestion et administration ;
- le sous-système de gestion des transactions (**SSGT**) permet d'assurer la mise en œuvre de compléments de service et de mécanisme de sécurité comme la gestion de groupes fermés d'usagers (GFU) ;
- le sous-système exploitation maintenance (**SSEM**) comporte les procédures de surveillance du réseau.

© Dunod – La photocopie non autorisée est un délit

La figure 20.36 représente la structure d'un message SS7. Le format général de la trame est similaire à celui d'HDLC (fanion, commande, FCS, transparence binaire). Le champ Commande comporte les informations nécessaires au contrôle de séquencement et à la reprise sur erreur :

- **BSN** (*Backward Sequence Number*, numéro de séquence arrière) indique le numéro de séquence de la trame acquittée. Ce numéro correspond au champ Nr d'HDLC ;
- **BIB** (*Backward Indicator Bit*), à 1, ce bit correspond à un acquittement négatif et à une demande de retransmission de la trame BSN ;
- **FSN** (*Forward Sequence Number*, numéro de séquence avant) indique le numéro du message transmis. Ce numéro correspond au champ Ns d'HDLC ;
- **FIB** (*Forward Indicator Bit*), à 1, il indique que la trame FSN est une retransmission ;
- **LI** (*Length Indicator*) sur 6 bits indique en puissance de 2 la longueur du champ d'information décomptée par groupe de 8 octets ($L = 8 \times 2^{LI}$) ;
- **D**, Disponible (2 bits) ;
- **SIO** (*Service Indicator Octet*) identifie le sous-système utilisateur requis, correspond à la notion de SAP (*Service Access Point*) ;
- **SIF** (*Signalling Information Field*) est le champ d'informations de signalisation limitée à 272 octets ;
- **DPC** (*Destination Point Code*) identifie le point sémaphore destination (adresse) ;
- **OPC** (*Originating Point Code*) identifie le point sémaphore source ;
- **SLS** (*Signalling Link Selection*) donne une indication supplémentaire pour assurer un partage de charge dans le réseau. Le routage se fait en prenant en considération les trois champs (DPC, OPC, SLS).

Le champ d'information comprend notamment l'identification de l'appelé et de l'appelant, les informations de taxation (catégorie du demandeur) et, selon le message, une série d'indicateurs.

L'évolution du RNIS

Ouvert en 1987 dans les Côtes-d'Armor et disponible sur tout le territoire depuis 1990, le RNIS n'a pas eu à ses débuts, en raison du coût de l'abonnement et de communications plus chères, un franc succès. Il n'a connu un réel développement que lorsque France Télécom a retiré de son offre commerciale professionnelle les raccordements MIC. Aujourd'hui, la tarification des communications est unique quel que soit le type de raccordement (RNIS ou analogique).

Évolution du RNIS bande étroite, le RNIS large bande (**B-ISDN**, *Broadband-ISDN*), s'appuyant sur la commutation de cellules (ATM[11]), devait offrir des débits allant de 155 à 622 Mbit/s et des téléservices du type vidéo haute définition auraient pu être disponibles. Cependant, si l'évolution du cœur de réseau vers un réseau de transport ATM s'est bien réalisée, les débits et les services offerts n'ont pas évolué. Aujourd'hui, Internet et son protocole TCP/IP semblent mieux placés aujourd'hui pour concrétiser le réseau multimédia du futur.

11. Voir chapitre 14, § 14.3.5.

20.5 LA TÉLÉPHONIE ET LA MOBILITÉ

20.5.1 Principes généraux

Le besoin d'alerter ou de communiquer avec une personne en déplacement a conduit aux concepts de messagerie unilatérale (alerte à personne ou *paging*) et de radiotéléphonie cellulaire.

Le *paging* consiste à envoyer par diffusion à un petit terminal de poche un bip sonore ou un petit message alphanumérique. La communication est unilatérale, le message est transmis par Minitel ou par l'intermédiaire d'une opératrice. De ce fait, les techniques mises en œuvre pour le *paging* sont simples.

Il n'en est pas de même de la téléphonie mobile qui, en plein essor, soulève de nombreuses questions notamment :

- la bidirectionnalité de la communication, le nombre de communications à établir en même temps ont conduit au concept de communication cellulaire. Une cellule est une zone dans laquelle les fréquences utilisées appartiennent à un même ensemble. Deux cellules adjacentes ne devront pas utiliser le même ensemble de fréquences (figure 20.37). La dimension limitée d'une cellule (portée radio) autorise la réutilisation des fréquences ;
- l'accès multiple et le partage du support (politique d'accès) ;
- la localisation du mobile en déplacement (itinérance ou *Roaming*) ;
- la possibilité pour le mobile en déplacement de maintenir la communication en cours (*hand-over* ou *handoff*) ;
- l'identification et la confidentialité des communications.

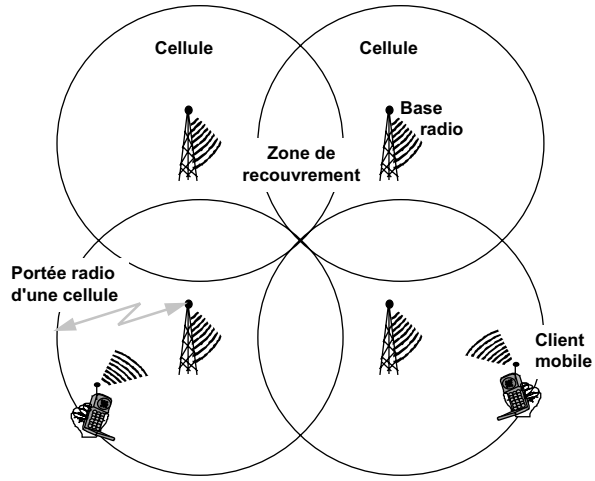


Figure 20.37 Principe d'un réseau cellulaire.

Structure générale d'un système de radiotéléphonie

La figure 20.38 décrit les différents composants d'un réseau de radiocommunication cellulaire de type **GSM** (*Global System for Mobile*, initialement Groupe spécial mobile).

© Dunod – La photocopie non autorisée est un délit

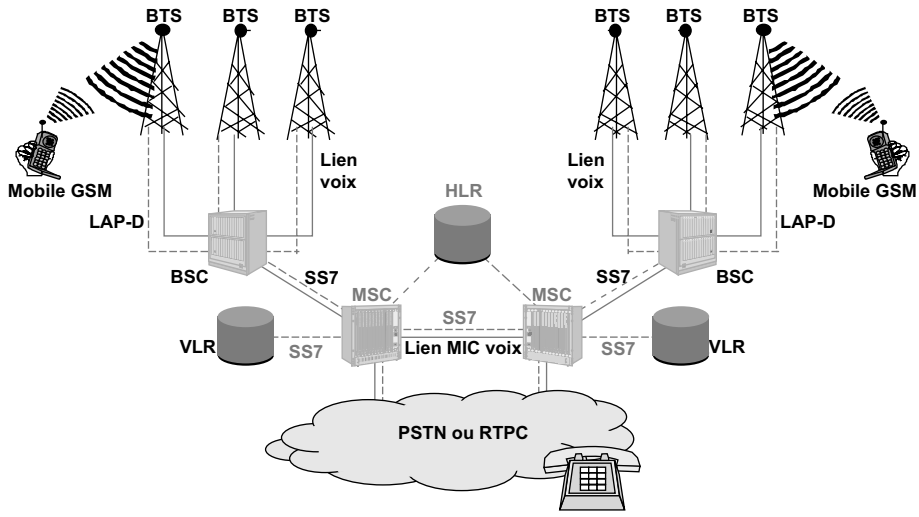


Figure 20.38 Principe d'un réseau GSM.

Un réseau de téléphonie mobile de type GSM comprend :

– des stations mobiles (**MS**, *Mobile Station* ou **mobile GSM**), qui doivent être identifiées et localisées par le système pour pouvoir établir une communication (appel sortant) et être alertées (appel entrant) ;
– un sous-système radio (**BSS**, *Base Station Subsystem*) comportant un ensemble de bases radio (**BTS**, *Base Transceiver Station*) ou interfaces air qui gèrent le trafic radio avec le mobile. La zone couverte par une base radio (BTS) constitue une cellule. Une station de contrôle gère un ensemble de BTS (**BSC**, *Base Station Controller*) ;
– un sous-système réseau (**NSS**, *Network SubSystem*) comprenant les commutateurs de cœur de réseau (**MSC**, *Mobile services Switching Center*) associés à une base de données locale (**VLR**, *Visitor Location Register*) et une base de données centrale ou registre des abonnés nominaux (**HLR**, *Home Location Register*).

Principe général de fonctionnement

Chaque BTS diffuse en permanence sur un canal de signalisation (**BCCH**, *Broadcast Control CHannel*) des informations générales sur le type de réseau auquel la cellule est rattachée. Lorsqu'un mobile est mis sous tension, il recherche (*scanning*) un canal BCCH (figure 20.39). Le mobile sélectionne alors la BTS (cellule) dont le niveau de réception est le plus élevé. Il acquitte le signal de BCCH, de cette cellule, sur le canal d'accès aléatoire de la cellule (**RACH**, *Random Access CHannel*) et s'y inscrit.

Le réseau lui attribue alors un canal de signalisation (**SACCH**, *Slow Associated Control CHannel*). Les données utilisateur de la HLR (base de données centrale) sont recopiées dans la VLR (base de données locale des visiteurs de la cellule). À la demande de la BSC, la HLR enregistre la localisation du mobile pour être en mesure d'y acheminer les appels entrants. En principe, la base HLR est unique par réseau (**PLMN**, *Public Land Mobile Network*).

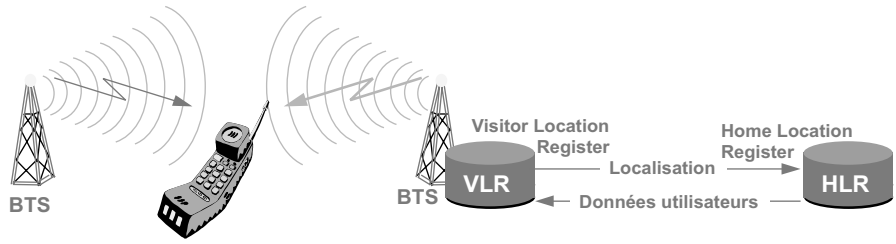


Figure 20.39 Principe de l'accueil d'un mobile dans une cellule.

20.5.2 La gestion de l'abonné et du terminal

On distingue plusieurs types de terminaux selon leur taille (terminaux portables et portatifs), leur bande de fréquences (GSM 900 MHz, DCS 1 800 MHz...). L'utilisation de systèmes portables miniaturisés, facilement « empruntables » et d'une interface air ont nécessité l'introduction de mécanismes d'identification garantissant une certaine sécurité et préservant l'anonymat des communications. C'est ainsi que les identifications de l'abonné et du terminal ont été dissociées.

L'abonné est identifié par un module spécifique dans lequel sont inscrites toutes les données propres à l'utilisateur (carte **SIM**, *Subscriber Identity Module*). Cette carte, délivrée par l'opérateur, mémorise un nombre important d'informations :

- des données propres à l'opérateur (réseau...) ;
- des données propres à l'utilisateur (identification, services optionnels, annuaire...) ;
- des données propres à l'usage du terminal (dernière zone de localisation, listes des réseaux utilisés...) ;
- les informations de sécurité (mots de passe utilisateur, compteurs d'erreur, clé de déblocage, clé d'authentification, clé de cryptage propre au terminal...) ;
- les minimessages reçus (**SMS**, *Short Message Service*)...

L'utilisation du portable est protégée par un mot de passe utilisateur demandé à l'initialisation du système (CHV1, *Card Holder Verification* ou code **PIN**, *Personnal Identity Number*), certaines fonctions ne sont accessibles qu'après l'introduction d'un mot de passe de second niveau (CHV2 ou PIN2).

La carte SIM permet de dissocier les données utilisateurs de celles du terminal et à l'opérateur de bloquer l'un indépendamment de l'autre. Le terminal est identifié par l'**IMEI** (*International Mobile Equipement Identity*). À chaque utilisateur est associé un numéro d'appel international (**MSISDN**, *Mobile Station ISDN*) par lequel l'abonné peut être appelé et un identifiant utilisé par le réseau pour le localiser (**IMSI**, *International Mobile Subscriber Identity*). Pour ne pas transporter dans le réseau l'identifiant personnel de l'utilisateur (confidentialité), lorsqu'un utilisateur est présent dans une zone, un identifiant temporaire lui est attribué (**TMSI**, *Temporary Mobile Station Identity*). La figure 20.40 illustre l'utilisation de ces identifiants lors d'un appel entrant depuis le réseau public commuté (RTC).

Le poste appelant numérote le MSISDN (06 xx xx xx xx), cet appel est acheminé par le réseau téléphonique fixe vers le commutateur du réseau de mobile le plus proche (MSC) qui fait office de passerelle entre les deux réseaux (**GMSC**, *Gateway MSC*). Le GMSC interroge le HLR pour

© Dunod – La photocopie non autorisée est un délit

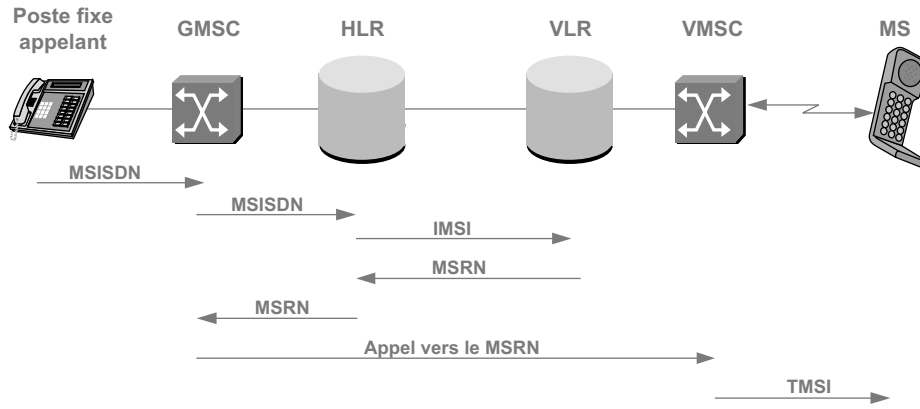


Figure 20.40 L'échange des différents identifiants.

connaître la localisation de l'appelé. Le HLR substitue au MSISDN le IMSI (N° attribué pour localiser l'appelé) et interroge la base VLR qui lui attribue alors un **MSRN** (*Mobile Station Roaming Number*), ce numéro permettant le routage des appels, est composé du code pays du VLR, de l'identifiant du VLR et du N° d'abonné. Le GMSC établit alors l'appel vers le **VMSC** (*Visited MSC*). Enfin, le VMSC établit l'appel vers le mobile en utilisant l'identité temporaire (TMSI).

L'affectation des canaux de communication est dynamique. Elle suit les procédures décrites ci-après. Lors d'un appel entrant, la base radio diffuse sur un canal d'appel (*paging*) l'identification de la station appelée. Le mobile qui reconnaît son identification accuse réception du message sur le canal de retour d'appel. La base radio affecte alors au mobile un canal de trafic (fréquence et IT). Lors d'un appel sortant, le canal de trafic n'est attribué par la base radio qu'après que l'appelant ait décroché. Cette technique dite du rappel du demandeur évite d'affecter des ressources à un appel non abouti.

20.5.3 L'interface radio

L'organisation cellulaire du réseau

On appelle cellule, la zone géographique couverte par un émetteur (figure 20.41). La taille des cellules doit tenir compte de nombreux facteurs, notamment :

– des conditions de propagation. Les systèmes de téléphonie mobile utilisent des fréquences de l'ordre du GHz, la propagation de telles fréquences se fait uniquement par onde directe. Les obstacles créent des zones d'ombre ;

– de la limitation de la puissance d'émission du mobile. Un des éléments essentiels de la téléphonie mobile est le poids du terminal, cette contrainte impose des batteries de faible capacité et donc, afin de disposer d'une autonomie suffisante, une puissance d'émission limitée ;

– du nombre potentiel de stations à accueillir vis-à-vis de la capacité d'accueil de la base radio. La bande de fréquence utilisée par les bases radio limite le nombre de canaux gérés par la station. Dans les zones à fort potentiel d'utilisateurs, il sera nécessaire de réduire la taille des cellules pour accueillir convenablement tous les mobiles de la zone. De ce fait, les cellules sont plus petites en zone urbaine qu'en zone rurale ;

– de la vitesse de déplacement du mobile. La gestion du *handover* est délicate, plus les zones sont petites vis-à-vis de la vitesse de déplacement du mobile, plus le changement de cellules est fréquent.

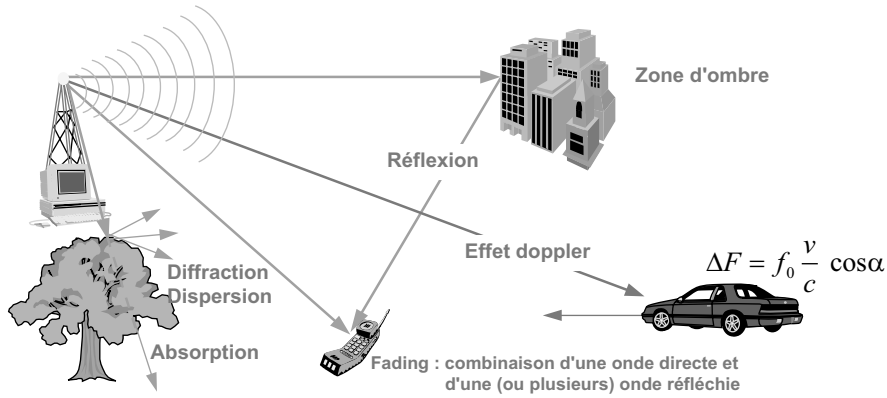


Figure 20.41 Les problématique des transmissions hertziennes.

La limitation du spectre radio et les capacités d'un émetteur à gérer un nombre élevé de canaux radio conduisent à étudier la réutilisabilité des fréquences (bandes allouées). Les schémas de réutilisation des fréquences doivent tenir compte à la fois des puissances d'émission et des interférences (deux zones utilisant les mêmes fréquences ne doivent pas se perturber). Différents schémas de réutilisation sont utilisés, la figure 20.42 illustre un système à 9 fréquences (facteur de réutilisation 1/9). Les installations sans fil (*cordless*) privées (résidentielles ou derrière un petit PABX) peuvent être monocellulaire.

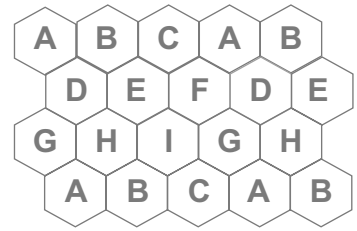


Figure 20.42 L'organisation des cellules utilisant 9 jeux de fréquence de base.

L'accès partagé au support

L'accès de multiples mobiles à une seule base radio (BTR) conduit à définir une technique d'accès au support partagé. Ces techniques relèvent du multiplexage. La téléphonie mobile utilise :

– l'**AMRF** (Accès multiple à répartition de fréquence, ou multiplexage fréquentiel ou **FDMA**, *Frequency Division Multiple Access*), une fréquence est allouée à chaque utilisateur. Ce système simple est cependant sensible au *fading* (combinaison d'ondes directes et réfléchies qui module la réception – effet d'évanouissement) ;

© Dunod – La photocopie non autorisée est un délit

– l'**AMRT** (Accès multiple à répartition dans le temps, ou multiplexage temporel ou **TDMA**, *Time Division Multiple Access*), un intervalle de temps (IT) est alloué à chaque station. Plus souple que la précédente, cette méthode nécessite des systèmes de synchronisation ;
– la combinaison des deux dernières techniques **F/TDMA**, plusieurs canaux avec chacun un IT par utilisateur. Cette technique permet de multiplier les capacités d'accueil d'une base, elle est utilisée dans le système **GSM** ;
– l'**AMRC** (Accès multiple à répartition de code ou **CDMA**, *Code Division Multiple Access*), une seule fréquence est utilisée et un code est attribué à chaque utilisateur. Cette technique est complexe mais accroît la capacité d'accueil des bases en simplifiant la gestion des fréquences.

Ces techniques ne permettent pas seulement l'accès simultané de plusieurs mobiles, mais aussi la gestion des différents trafics d'une même station (flux voix montant et descendant, signalisation...). Ces trafics sont répartis sur plusieurs canaux qui peuvent être en pleine bande ou à demi-bande par exemple :

– la voix peut être à pleine bande (compression 13 kbit/s) ou à demi-bande (6,5 kbit/s) ;
– les canaux de données peuvent à pleine bande offrir un débit de 9,6 kbit/s et à bande réduite seulement 4,8 kbit/s.

La gestion de la mobilité

La localisation (itinérance ou *Roaming*) permet au réseau de transmettre un appel (appel entrant) alors que l'appelant n'a aucune connaissance de la position géographique de l'appelé. Le principe en est simple, lors de la mise sous tension le mobile s'identifie. Le MSC (centre de gestion local) de la cellule d'accueil interroge alors la base de données centrale (HLR) pour obtenir les informations relatives au visiteur et les inscrit dans la base de données locale (VLR). Le MSC attribue alors un identifiant temporaire au visiteur et informe la HLR de la position de celui-ci.

En permanence la base radio (BTS) analyse la qualité du signal reçu (canal de trafic ou voie de signalisation). En fonction de la qualité du signal, la station décide de maintenir le lien ou d'effectuer le transfert vers une cellule voisine. Le centre de gestion local demande alors aux cellules voisines d'effectuer une mesure de champ sur le canal d'émission du mobile. En fonction des résultats obtenus, le centre de gestion détermine la cellule qui doit accueillir le mobile et donne l'ordre de transfert.

Le transfert intercellulaire est effectué sans interruption perceptible de la communication. Cependant, le temps de basculement n'est pas nul et reste un handicap au transfert de données, notamment en cas de déplacement à grande vitesse où les changements de cellules sont fréquents (TGV). Le transfert de données à partir d'une station mobile n'est fiable que lorsque le mobile est fixe !

De même, l'analyse de la puissance reçue par la BTS, du rapport signal à bruit et du taux d'erreur peuvent conduire la BTS à demander au mobile une éventuelle réduction de puissance d'émission afin d'une part de ne pas perturber les cellules voisines et, d'autre part d'économiser ses batteries.

Pour réduire le trafic de signalisation, les cellules ont été regroupées en aires de localisation. Une aire de localisation peut comprendre plusieurs dizaines de cellules. Tant que le mobile ne change pas d'aire de localisation, aucun message n'est envoyé à la VLR. Lorsque l'on cherche à joindre le mobile (appel entrant), un message de recherche est émis sur le canal de signalisation commun (**PCH**, *Paging CHannel*) de toutes les cellules de l'aire. Ce procédé est un compromis entre la recherche du mobile dans tout le réseau (diffusion du message dans plusieurs milliers de cellule) et

la recherche limitée à la cellule actuelle, cette dernière méthode imposant un transfert de données à chaque changement de cellule.

20.5.4 Description succincte des différents systèmes en service

Plusieurs produits de téléphonie mobile sont disponibles. Certains à usage résidentiel (Norme **CT1**, *Cordless Telephon 1 Generation*) sont d'un emploi courant et rien ne les distingue d'un combiné classique si ce n'est la mobilité dans la limite de portée radio de l'appareil. Ces postes utilisent généralement un système d'identification locale et de scanner pour éviter le piratage de la ligne, la borne fixe ne permet d'écouler qu'une seule communication. La bande de fréquence autorisée en France correspond à la fréquence intermédiaire des récepteurs de télévision, ce qui peut provoquer parfois des intermodulations.

Le **GSM** (*Global Service for Mobile communication*) constitue en France l'offre numérique dominante (Orange, SFR). L'intérêt essentiel de cette offre est la confidentialité absolue des communications tandis que l'identification de l'abonné par une carte à puce évite un usage frauduleux du poste mobile (en principe !). Devant le développement important de la téléphonie mobile, les opérateurs doublent le réseau en utilisant la norme **DCS 1800** (*Digital Cellular System* dans la bande des 1 800 MHz). Celle-ci constitue l'offre unique de Bouygues Télécom.

20.5.5 Le service transport de données sur la téléphonie mobile

La donnée en mode circuit sur le réseau GSM

Le service de données (fax, accès distant à un réseau, accès à Internet – **WAP**, *Wireless Application Protocol*) en mode circuit est disponible sur tout le réseau GSM. Les services accessibles dépendent du terminal GSM et de l'abonnement. Compte tenu des faibles possibilités des premiers récepteurs GSM, ceux-ci étaient plutôt utilisés comme interface mobile d'accès à un réseau (figure 20.43). Le canal voix étant optimisé pour le transfert de la voix, le débit maximal offert pour la donnée ne dépasse pas 14,4 kbit/s. Un système d'agrégation de canaux est envisageable (quatre au maximum). Les communications sont facturées au tarif voix, c'est-à-dire au temps.

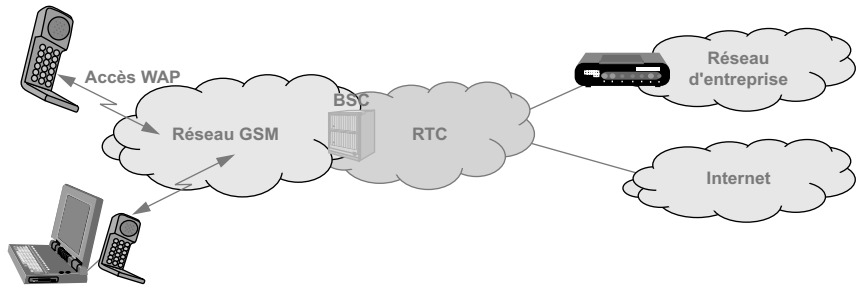


Figure 20.43 L'accès au service données sur un réseau GSM.

La donnée en mode paquet sur le réseau GPRS

Le **GPRS** (*General Packet Radio Service*) est un réseau IP utilisant l'accès radio du réseau GSM. La figure 20.44 représente la structure d'un réseau GPRS.

© Dunod – La photocopie non autorisée est un délit

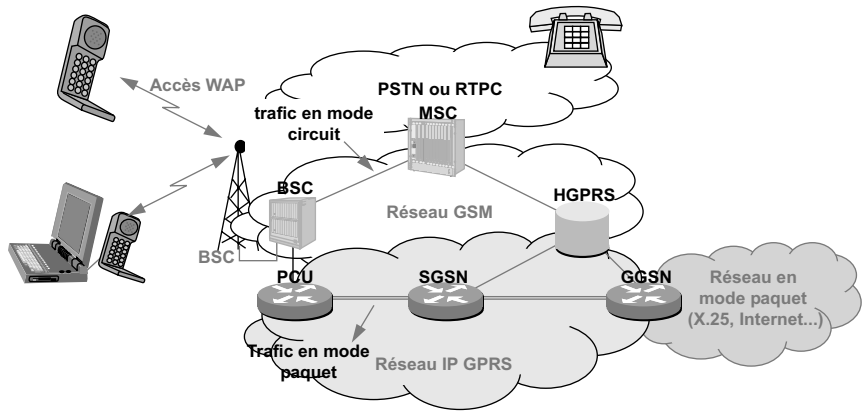


Figure 20.44 Structure d'un réseau GPRS.

Le réseau GPRS n'implique qu'une mise à jour du logiciel des éléments de base du réseau GSM (BTS et BSC) et l'introduction de nouveaux équipements dédiés réseaux mode paquet pour l'accès aux réseaux de données. Ces équipements sont :

– le **PCU** (*Packet Controler Unit*), implanté au niveau des contrôleurs de stations (BSC), assure l'adaptation des unités de données issues du mobile au format paquet et inversement ;
– le **SGSN** (*Serving GPRS Support Node*) est l'interface logique entre un abonné GSM et le réseau de données externe. C'est un routeur, il assure le routage des données et la gestion de la mobilité (enregistrement des abonnés, authentification du mobile droit d'accès, taxation...) ;
– le **GGSN** (*Gateway GPRS Support Node*) est le routeur d'accès aux autres réseaux de données ;
– un **RGPRS** (*Register GPRS*) est une base du type HLR dédié aux réseaux GPRS pour la gestion et la localisation des abonnés.

Le réseau GPRS offre un débit maximal de 114 kbit/s (regroupement de huit intervalles de temps). Il est perçu comme une solution transitoire dans l'attente des réseaux multimédias de la troisième génération devant offrir des débits allant jusqu'à 2 Mbit/s (**UMTS**, *Universal Mobile Telecomminication System*).

Alternative entre le GPRS et l'UMTS, **EDGE** (*Enhanced Data Rates for GSM Evolution*) permet, en utilisant une modulation 8PSK (modulation de phase à huit états, soit 3 bits par état) de tripler le débit du GPRS. Cependant le passage d'un réseau GSM à un réseau EDGE nécessite non seulement une mise à jour logicielle importante mais aussi le changement de la partie radio des BTS. Le GPRS permet, aux opérateurs ne disposant pas de licences UMTS, d'offrir à leurs abonnés des services similaires (voix, données, vidéo).

20.5.6 La mobilité et l'accès à Internet

Une nouvelle génération de téléphones portables « embarque » un navigateur allégé. Le protocole en mode circuit (GSM) ou mode paquet (GPRS) **WAP** (*Wireless Application Protocol*) autorise l'accès à Internet depuis un portable. Le débit réduit et la non-convivialité du terminal pénalise le développement du WAP.

Le WAP est un ensemble de protocoles permettant l'accès aux pages Web à partir d'un navigateur embarqué. La pile protocolaire représentée figure 20.45 est une adaptation de l'architecture TCP/IP aux contraintes des réseaux radios.

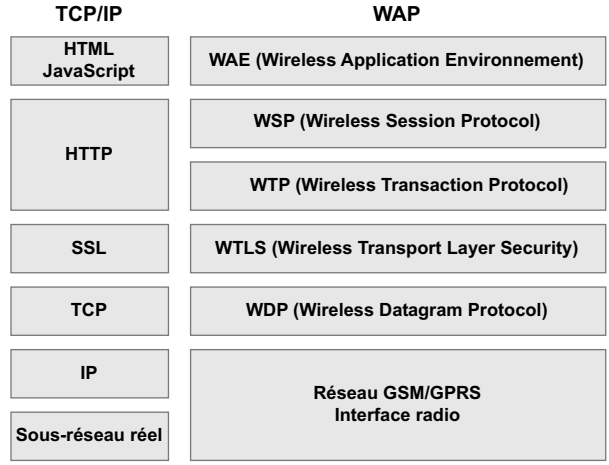


Figure 20.45 L'empilement protocolaire du WAP.

L'utilisation d'un navigateur allégé et d'un langage spécifique le **WML** (*WAP Markup Language*) dérivé de **XML** (*eXtensible Markup Language*) nécessite d'utiliser une passerelle de conversion pour assurer l'adaptation des requêtes et des formats (figure 20.46).

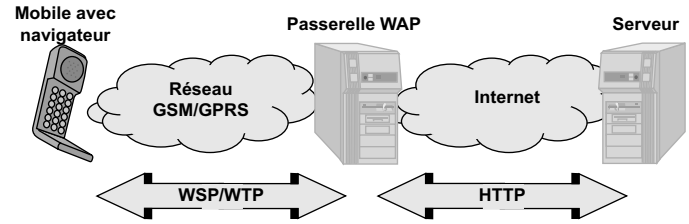


Figure 20.46 Le transfert d'une requête WAP.

Le Japon utilise un système similaire dit **i-Mode**. Le langage i-Mode étant directement dérivé de HTML, le service i-Mode ne nécessite pas l'utilisation de passerelle de compression de contenu. S'appuyant directement sur des réseaux GSM et GPRS, il demande peu de développement d'infrastructure, il constitue l'offre de Bouygues Télécom.

20.5.7 L'évolution des systèmes de téléphonie mobile, l'UMTS

En intégrant à l'origine les services multimédias à haut débit (2 Mbit/s), l'**UMTS** (*Universal Mobile Telecommunication System*) constitue l'évolution naturelle des systèmes de communication entre mobiles.

Les bandes de fréquences allouées à l'UMTS se situent autour des 2 GHz avec une largeur de bande de 230 MHz. L'accès au canal utilise la technique du **W-CDMA** (*Wide band CDMA*). Les débits offerts à une station sont directement en relation avec la taille d'une cellule :

© Dunod – La photocopie non autorisée est un délit

– de 144 à 384 kbit/s en zone rurale pour des mobiles dont la vitesse de déplacement est inférieure à 500 km/h (TGV) ;
– de 384 à 512 kbit/s en zone urbaine pour des vitesses de déplacement inférieures à 120 km/h ;
– jusqu'à 2 Mbit/s à moins de 10 km de la base radio.

Les chiffres ci-dessus s'entendent pour une utilisation du système en extérieur. Compte tenu des fréquences utilisées, les systèmes de téléphonie mobile sont en principe des systèmes *out-door*, c'est-à-dire des systèmes destinés à être utilisés en extérieur.

20.5.8 La téléphonie satellitaire

Du géostationnaire aux constellations de satellites

Le premier réseau de communication pour mobiles utilisant des liens satellites date de 1982 (Immarsat A). Le réseau utilise quatre satellites géostationnaires et environ 40 stations terrestres. Il couvre l'intégralité de la surface du Globe, sauf les pôles. Immarsat offre un service de téléphonie (voix, fax), de messagerie (messages courts du type *pager*) et de données (débit de 2,4 kbit/s à 64 kbit/s). Immarsat E est couplé au **GPS** (*Gobal Positionning System*), il offre un service de positionnement pour les navires en détresse (balise Argos).

Le système Immarsat n'intéresse qu'un segment très réduit de clientèle. En effet, des terminaux de plusieurs kilogrammes, des antennes de 80 à 90 cm et la nécessité de « viser » le satellite réservent ce système de communication à des usages professionnels (navires...)

En orbite géostationnaire (36 000 km), le temps bouche/oreille est de 240 ms minimum ce qui introduit une gêne dans l'interactivité des communications, d'où de nombreux projets reposant sur l'utilisation de satellites défilant en orbite basse.

Les systèmes à orbite basse

➤ Le système Iridium

D'origine Motorola, le projet initial de 77 satellites (d'où le nom du 77^{e} élément de la classification de Mendeleïev), Iridium a été réduit à 66 satellites répartis sur 6 plans orbitaux en orbite basse à environ 780 km d'altitude (**LEO**, *Low Earth Orbital*). Après une mise en service et un arrêt immédiat faute d'abonné, Iridium a été remis en service en mars 2001. Il offre des services de voix, données, fax et messagerie.

L'une des particularités essentielles d'Iridium est de permettre une communication intersatellite : les communications, entre deux mobiles, peuvent être acheminées directement dans le réseau Iridium sans emprunter de liens terrestres. Les communications sont établies en *full duplex* à 2,4 kbit/s (bande passante identique pour la transmission de données et les fax).

➤ Le système Globalstar

Globalstar, soutenu par Alcatel et France Télécom, utilise 48 satellites en orbite basse (1 410 km) répartis sur huit plans orbitaux. À la différence d'Iridium, les communications intersatellites ne sont pas possibles. Pour mettre en relation deux utilisateurs non desservis par le même satellite, Globalstar utilise les réseaux traditionnels des opérateurs terrestres.

Globalstar offre les mêmes services qu'Iridium mais autorise, en plus, une fonction de localisation de type GPS. Chaque satellite peut établir 28 800 communications simultanées.

	ICO	Globalstar	Iridium	Teledesic
Orbite	MEO	LEO	LEO	LEO
Altitude (km)	10 355	1 410	780	1350
Nombre de satellites	10 en service 2 en secours	48 en service 8 en secours	66 en service 6 en secours	288 en service 84 en secours
Nombre de plans orbitaux	2	8	6	12
Période de révolutiuon	358 mn	114 mn	100	110
Visibilité d'un satellite	115,6 mn	114 mn	11,1 mn	
Délai minimal de propagation (mobile, satellite)	34,5 ms	4,63 ms	2,60 ms	
Délai maximal	48 ms	11,5 ms	8,22 ms	
Faisceaux par satellite	61	163	48	576
Type d'accès	TDMA/FDMA/FDD	CDMA/FDMA/FDD	TDMA/FDMA/TDD	TDMA/SDMA/FDMA /ATDMA
Communication inter-satellite	Non	Non	Oui	Non
Masse du satellite	1925 kg	450 kg	700 kg	771 kg
Services offerts	Voix, données, fax, paging	Voix, données, fax, paging, messagerie, positionnement	Voix, données, fax, messagerie, positionnement	Voix, données, fax, paging, vidéo

Figure 20.47 Comparaison de quelques systèmes satellitaires.

20.6 CONCLUSION

Phénomène de ce début de XXI^{e} siècle, la mobilité envahit tous les domaines des télécommunications. Que ce soit en milieux professionnels ou privés, la connectivité des équipements et leur communication feront vraisemblablement l'objet de développements et d'applications que l'on ne peut encore imaginer.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 20.1 Capacité d'un autocommutateur

La capacité d'un autocommutateur d'un opérateur de téléphonie est de 5 000 erlangs. Ce commutateur dessert des abonnés résidentiels et professionnels à concurrence de 40 et 60 %. On sait, en outre, qu'un professionnel a un trafic à l'heure de pointe trois fois supérieur à celui d'un abonné résidentiel qui est supposé de 0,1 erlang. Quel est le nombre total d'abonnés desservis si la capacité du commutateur est utilisée à 100 % ?

Exercice 20.2 Itinérance

Lors d'un changement de cellule, votre communication téléphonique est interrompue alors que d'autres personnes déjà présentes dans la nouvelle cellule poursuivent leur communication. Quelle peut être la raison de cette interruption ?

Exercice 20.3 Système Iridium

Si la durée de révolution d'un satellite Iridium est de 100 min, quel est le temps moyen pendant lequel un poste terrestre mobile qui ne se déplace pas est pris en compte par un même satellite ?

Exercice 20.4 Schéma de réutilisation des fréquences

Un système de téléphonie cellulaire dispose de 240 fréquences. Sachant que les cellules ont un profil hexagonal et qu'une même fréquence ne peut être réutilisée dans une cellule adjacente, quel est le nombre de fréquences disponibles pour une cellule (accès FDMA) ?

Exercice 20.5 Protocole D (Q.931)

La trace reproduite figure 20.48 correspond au renvoi du terminal actif vers le terminal 01 23 45 67 89. L'analyseur a décodé les messages LAP-D, et fourni la signification et le contenu du champ d'information (protocole D). Indiquez pour chacun des messages, la signification des éléments d'information.

L	Horodatage	Origine	SAPI	TEI	C/R	Type trame	Contenu du message
1	01:06:34–678	Net	0	127	1	UI	Orig Q.931 Etablissement
			Mode de fct support				: 80 90 A3
			Identification canal				: 81
			Comp. Couches sup				: D1 81
2	01:06:34–714	Usr	0	64	0	SABME	
3	01:06:34–885	Net	0	64	0	UA	
4	01:06:34–933	Usr	0	64	0	INFO	Dest Q.931 Libération
			Cause				: 87 90
			Facilités				: 00 2A 32 32 23
			Mode de fct usager				: 80
			Numéro appelé				: 80 30 31 32 33 34 35 36 37 38 39
5	01:06:34–974	Net	0	127	0	RR	

Figure 20.48 Message de renvoi d'un poste téléphonique RNIS. Dans les traces « L » représente le numéro de ligne auquel il est fait référence dans les corrections.

Chapitre **21**

Installation d'abonné et réseau privé de téléphonie

21.1 LES AUTOCOMMUTATEURS PRIVÉS

21.1.1 Généralités

Un autocommutateur privé de téléphonie, **PABX** (*Private Automatic Branch eXchange*) est l'interface entre le service de téléphonie de l'entreprise et un réseau téléphonique (public ou privé). Il est chargé de mettre en relation, à la demande de l'un des correspondants, des postes téléphoniques (commutation de circuits), que les deux correspondants soient derrière le PABX (communication interne à l'entreprise) ou que l'un d'eux soit sur un autre réseau téléphonique public (RTC ou RNIS) ou privé.

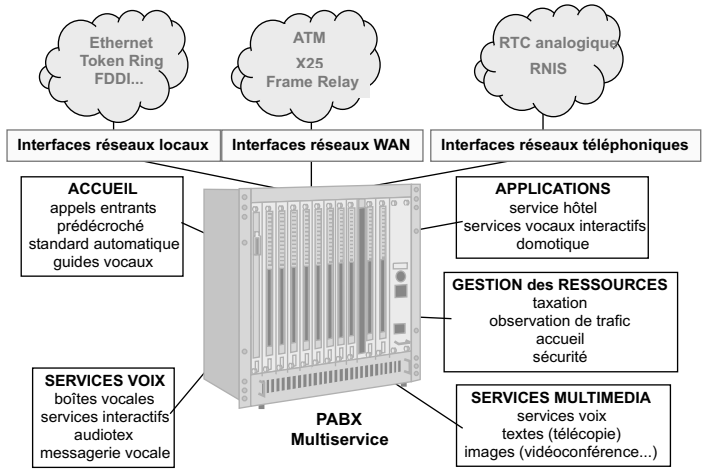


Figure 21.1 Le PABX au cœur des services d'entreprise.

La variété des services offerts par les PABX conduit à les intégrer de plus en plus au système d'information de l'entreprise, l'aboutissement de cette évolution se concrétise par l'introduction de

la voix sur IP. La figure 21.1 illustre la richesse fonctionnelle des PABX numériques multiservices de dernière génération.

21.1.2 Architecture d'un PABX

Un PABX numérique comporte essentiellement un réseau de connexion (commutation temporelle) qui, sous le contrôle de l'unité de contrôle (UC), établit une connexion temporaire entre le demandeur et le demandé. Cette connexion est établie en fonction de données usager (droits de l'usager, restrictions diverses, facilités offertes...). La figure 21.2 illustre l'architecture simplifiée d'un PABX.

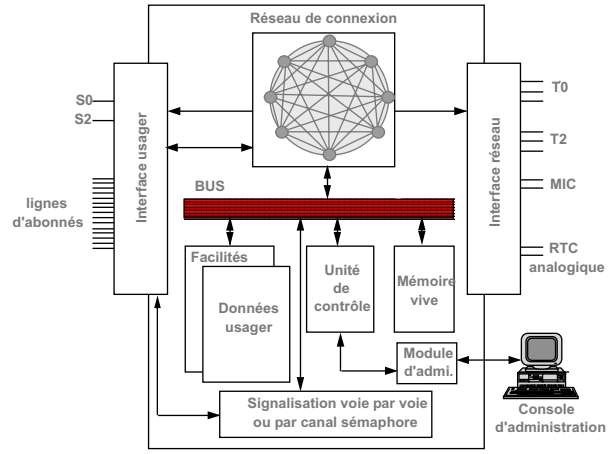


Figure 21.2 L'architecture interne d'un PABX.

L'analyse de la numérotation est l'une des tâches essentielles du logiciel de gestion des PABX. La numérotation permet à l'unité de contrôle :

- de mettre en relation un usager demandeur et un usager demandé (correspondance entre un numéro logique – numéro d'appel – et un port physique de l'interface usager) ;
- de diriger l'appel vers telle ou telle ligne extérieure (préfixe de prise de ligne) ;
- d'accorder à l'usager certaines facilités (renvoi, verrouillage du poste...).

L'ensemble des règles de gestion, en relation avec la numérotation, constitue **le plan de numérotation.**

21.1.3 Les téléservices et applications vocales offerts par les PABX

Les téléservices

Les techniques numériques, mises en œuvre dans les autocommutateurs numériques, ont permis d'offrir aux utilisateurs des services complémentaires facilitant, ainsi, la communication générale dans l'entreprise. Les services supportés dépendent essentiellement du constructeur. Cependant, les facilités de base sont implémentées sur tous les systèmes. Ce sont notamment :

- les techniques de renvoi (renvoi immédiat, renvoi sur non-réponse ou renvoi différé, renvoi sur occupation) ;
- la supervision et le filtrage des postes (relation secrétaire/patron) ;

– le multitouche qui autorise la prise d'un second appel et le double appel. Ces deux facilités permettent le va-et-vient entre les correspondants et la conférence à trois ;
– le multiligne c'est-à-dire plusieurs lignes chacune dotée du même numéro (mono-annuaire) ou de numéros différents (multi-annuaire) ;
– les groupements d'interception, ensemble d'utilisateurs réunis en un groupe de communication. Toute communication, à destination d'un membre du groupe, peut être interceptée par tout membre du groupe ;
– l'annuaire collectif qui autorise notamment l'appel par le nom et chez l'appelé l'affichage du nom de l'appelant. Certains constructeurs proposent un annuaire extérieur. Cette facilité permet, lors des appels entrants de substituer au numéro d'appelant un nom ;
– la numérotation abrégée collective ou personnelle ;
– le rappel automatique sur poste occupé. Cette facilité permet le rappel automatique d'un correspondant occupé lorsque celui-ci aura terminé la communication en cours ;
– le transfert d'appel au sein de l'entreprise ou vers l'extérieur, si cette dernière facilité est autorisée ;
– les groupes de diffusion : cette technique permet de diffuser, à partir d'un poste maître, un message sur un ensemble de postes téléphoniques sans que les correspondants aient décroché (recherche de personnes, messages de sécurité...) ;
– l'interphonie (mise en relation d'usager sans décrochage du poste).

L'usage de ces facilités ne s'est véritablement développé qu'avec l'apparition des postes numériques[1] avec afficheur et touches programmables. Notons que la numérisation complète du réseau téléphonique et l'utilisation d'une signalisation par canal sémaphore (RNIS) permet, à certains opérateurs, d'offrir sur des postes téléphoniques analogiques résidentiels certaines facilités autrefois réservées aux installations numériques.

Les applications vocales

Ces applications ont pour objet de faciliter les relations de l'entreprise avec le monde extérieur. Parmi ces applications, la plus utilisée est la **messagerie vocale**. Celle-ci permet à un correspondant de déposer un message pendant l'absence de l'appelé (service de communication différée).

Quand le numéro d'un destinataire n'est pas connu ou n'est pas diffusé, le **standard automatique** substitue, à l'opératrice, un ensemble de guides vocaux pour acheminer l'appel vers le destinataire (service de mise en relation automatique). Cette application peut véritablement faciliter l'acheminement des appels, mais elle doit faire l'objet d'une étude sérieuse pour éviter d'avoir à parcourir une arborescence trop développée qui dissuade l'appelant. La figure 21.3 illustre le mécanisme du standard automatique.

Les **serveurs audiotex** permettent l'automatisation du traitement des demandes répétitives d'information. Fondés sur le même principe que les standards automatiques, les serveurs audiotex sont constitués d'une série de guides vocaux qui conduisent l'utilisateur, à travers une arborescence, vers le renseignement qu'il désire obtenir (service de diffusion d'information).

1. Attention, il ne faut pas confondre postes numériques et postes Numéris. Ces derniers sont étudiés pour être raccordés directement au réseau Numéris (interface So). Les premiers, généralement beaucoup plus riches en fonctionnalité, sont spécifiques à un constructeur, on les appelle aussi postes dédiés.

© Dunod – La photocopie non autorisée est un délit

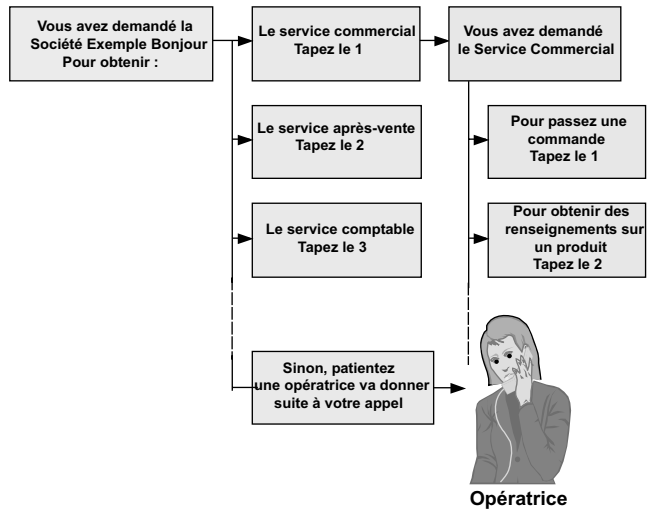


Figure 21.3 Principe du standard automatique.

Les **serveurs vocaux interactifs** ont pour objectif l'automatisation du traitement de demandes répétitives d'informations par des transactions personnalisées. La première application est, par exemple, utilisée par les organismes bancaires pour informer leurs clients sur l'état de leur compte. La seconde utilise les postes téléphoniques comme terminal de saisie d'une application informatique. Ce service, généralement mis en œuvre par les sociétés de vente par correspondance, est illustré par la figure 21.4.

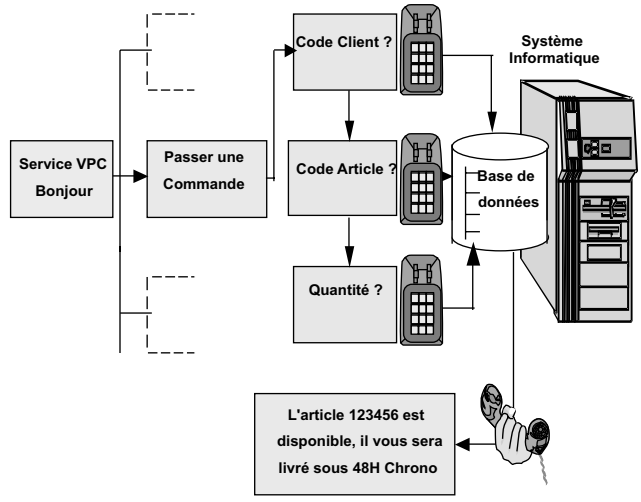


Figure 21.4 Exemple d'application sur serveur vocal interactif.

Ces diverses applications consistent à associer une touche (téléphone numérique) ou une fréquence (téléphone à numérotation fréquentielle) à une commande. Les fréquences audio sont transmises en transparence sur la liaison voix (RTC) ou dans l'IT voix (canal B du RNIS).

L'intégration Téléphonie/Informatique

➤ Le CSTA (*Computer Supported Telephony Applications*)

Ayant pour origine les travaux de DEC, le concept de **CTI** (*Computer Telephony Integrated*) organise les échanges entre un PABX et un ordinateur. Il a donné naissance à la norme CSTA publiée par l'ECMA dont le concept est illustré figure 21.5.

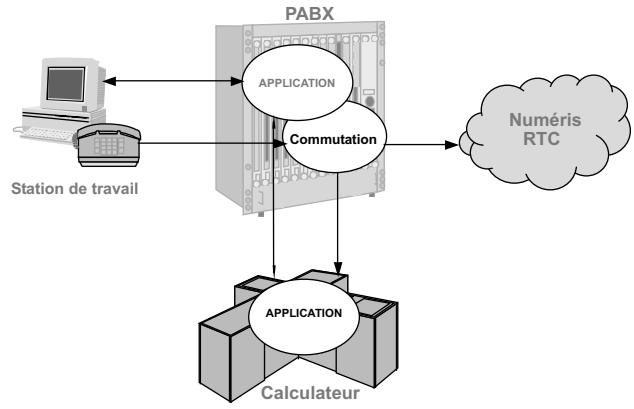


Figure 21.5 Principe du CSTA.

La recommandation CSTA décrit un ensemble de services qui organisent le dialogue de la couche application du modèle OSI entre un serveur CTI et un PABX. Contrairement au concept *CallPath* d'IBM qui spécifie un service d'API conforme à l'architecture SAA d'IBM, la recommandation CTSA ne précise aucune **API** (*Application Programming Interface*). S'appuyant sur les concepts du RNIS et notamment de la signalisation SS7, CSTA cantonne le PABX aux fonctions de commutation de circuits et reporte les fonctions intelligentes sur l'ordinateur.

L'association ordinateur/téléphonie a connu un développement important, surtout dans l'accueil téléphonique. Dans l'exemple de la figure 21.6, l'ordinateur exploite le numéro d'appelant et affiche automatiquement, sur l'écran de l'ordinateur et avant que le poste téléphonique ne soit décroché, les informations relatives au demandeur.

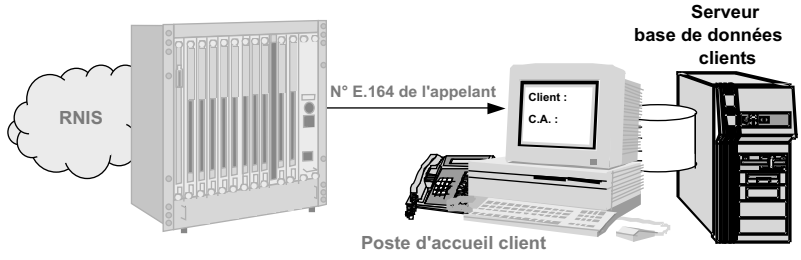


Figure 21.6 Principe d'un accueil fondé sur CSTA.

➤ Les API TAPI et TSAPI

D'origine Microsoft, les API **TAPI** (*Telephony Application Programming Interface*) ou Novell et AT&T **TSAPI** (*Telephony Services Application Programming Interface*) permettent de dévelop-

© Dunod – La photocopie non autorisée est un délit

per, sur micro-ordinateur, des applications qui accèdent, au moyen de la souris et du clavier, aux fonctions essentielles du PABX (figure 21.7) telles que :

– l'annuaire et la numérotation automatique,
– l'interception d'appel,
– la supervision de poste,
– la consultation de messagerie,
– l'établissement de statistiques téléphoniques personnelles.

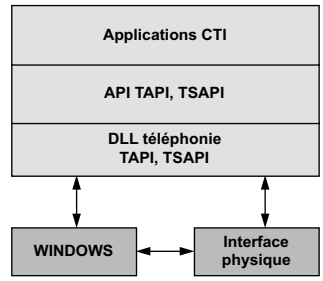


Figure 21.7 L'architecture générale du concept CTI sur micro-ordinateur.

TSAPI et TAPI ont des fonctionnalités similaires mais adoptent des approches différentes (convergence avec TAPI 2.0). TSAPI distribue les services téléphoniques sur le réseau local via un serveur de téléphonie. TAPI relie directement le poste de travail à l'autocommutateur (figure 21.8).

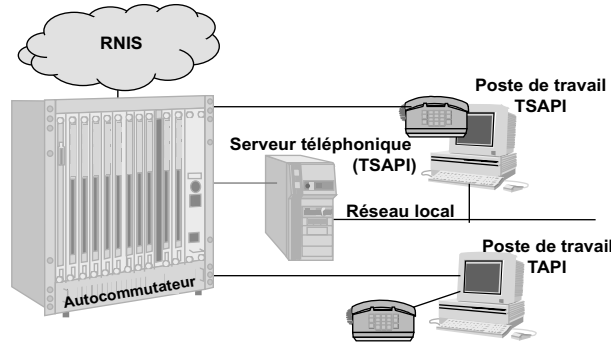


Figure 21.8 Principe général de TSAPI et de TAPI.

Une API Java, JTAPI permet aux applications développées en Java d'accéder aux services téléphoniques et de les enrichir de nombreuses fonctionnalités informatiques. JTAPI s'appuie sur les API TSAPI et TAPI.

La visiophonie

Ce n'est qu'avec l'apparition du RNIS et de ses canaux B à 64 kbit/s que la transmission simultanée de l'image et de la voix a été réalisable. Cependant, l'expérience de Biarritz (1986), avec quelque 1 500 foyers raccordés, a conduit, à l'époque pour des raisons économiques, à l'abandon de la généralisation de ce service.

La visiophonie, longtemps limitée à la communication au sein de l'entreprise, s'étend, aujourd'hui, à l'ensemble de moyens de téléphonie (résidentiel et mobile). Le poste visiophone est composé d'une caméra et d'un écran intégré au poste téléphonique. Associée à un micro-ordinateur, la visiophonie permet l'affichage de l'image dans une fenêtre.

Une série de normes, regroupées dans la recommandation H.320, régit la compression de l'image et de la voix, la transmission des informations et la signalisation d'usager à usager. Elle détermine les conditions d'interfonctionnement des terminaux de visiophonie. Cet ensemble de normes assure le partage de 1 à *n* canaux B. La qualité et les modalités de compression d'image sont essentiellement définies par les normes **CIF** (*Common Intermediate Format*, 352 points, 288 lignes) et **QCIF** (*Quarted Common Intermediate Format*, 176 points et 144 lignes).

Le codeur (Codec H.261) effectue une prédiction temporelle (estimation du mouvement par bloc de 8×8 pixels dans un espace de 47×47 pixels). Seule, la différence entre l'image prédite et l'image réelle est codée et transmise. La figure 21.9 cite les principales normes utilisées par la visiophonie.

Normes	Objet
Codage et décodage des images animées	
H.261	Autorise des débits multiples de 64 kbit/s (appelé encore norme P64 avec $1 \leqslant p < 31$
Gestion du système et signalisation	
H.221	Multiplexage et démultiplexage de 1 à 6 canaux B
H.230	Pour le contrôle et l'identification
H.242	Pour la communication et la reconnaissance entre deux terminaux
H.321	Pour la définition et la structure des trames
Codage et décodage du son	
G.711	Son de qualité normale (3,4 kHz numérisés à 64 kbit/s)
G.722	Son de qualité supérieure (7 kHz numérisés à 64 kbit/s)
G.728	Son de qualité normale (3,4 kHz compressés à 16 kbit/s)
Services associés	
H.233	Codage des sécurités
T.120	Gestion des transferts de fichiers sur le RNIS

Figure 21.9 Les principales normes de la visiophonie.

21.1.4 PABX et transmission de données

Au centre de la communication d'entreprise, les constructeurs de PABX ont très vite intégré à leur autocommutateur des fonctionnalités données (figure 21.10). La numérisation des PABX et la mise à disposition d'interface LAN (Ethernet, Token Ring...) ont engendré, non seulement, la banalisation du câblage mais autorisé une véritable interconnexion des LAN *via* un lien numérique ou des liens MIC (interface G.703, G.704). Ce dernier moyen, réalisant, *via* une régie, l'agrégation de *n* canaux de 64 kbit/s constitue les prémices d'une intégration voix/données (IT^2 voix et IT données sur le même support).

La mise à disposition d'accès X.25 *via* les canaux D (9,6 kbit/s) et B (64 kbit/s) a doté l'autocommutateur de fonctionnalités de commutateur de paquets X.25. Cependant, les besoins voix et

2. IT, intervalle de temps.

© Dunod – La photocopie non autorisée est un délit

données n'ont pas connu une évolution similaire. De ce fait, les investissements sont restés désynchronisés, et le PABX traditionnel n'a pas réussi à devenir le nœud de communication voix, données et images de l'entreprise. Les techniques sont restées disjointes.

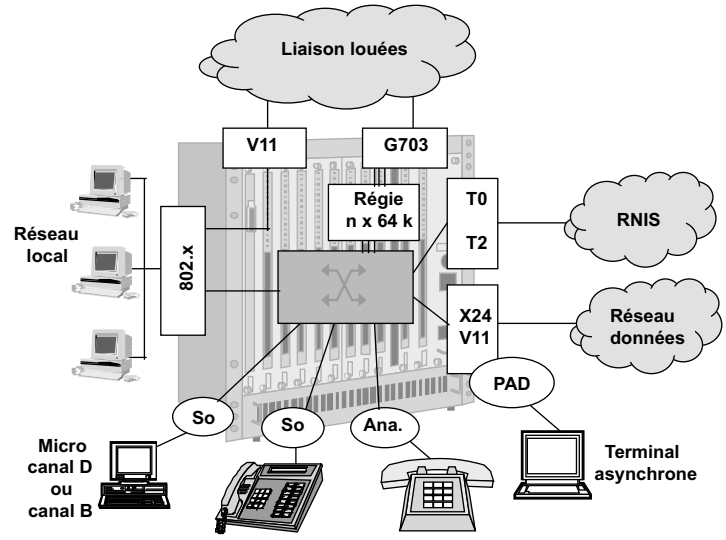


Figure 21.10 Le PABX et la transmission de données.

Si la convergence voix/données n'a pas eu lieu par la voix, les réseaux données ont réussi cette intégration (voir § 21.4).

21.2 L'INSTALLATION D'ABONNÉ

21.2.1 Généralités

L'installation de téléphonie privée prolonge dans l'entreprise les services téléphoniques du réseau public. La définition d'une installation téléphonique comporte trois phases (figure 21.11).

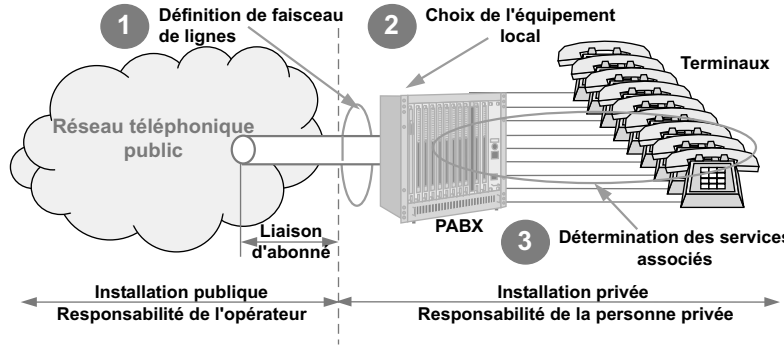


Figure 21.11 La définition de l'installation de téléphonie privée.

Les deux premières, d'ordre technique, consistent à dimensionner l'installation (équipement local, raccordement au réseau public). La troisième, d'ordre organisationnel, cherche à définir les services à offrir à chaque utilisateur.

Le choix de l'équipement local est essentiellement dicté par la nature des services à offrir aux utilisateurs, du nombre de postes à raccorder et de la puissance de commutation nécessaire. Le dimensionnement du PABX nécessite d'estimer le trafic à écouler, ce trafic s'exprime en erlang[3]. Il est en relation directe avec la nature de l'entreprise, un centre d'appel demande, pour un même nombre de postes, une puissance de commutation plus importante qu'un établissement industriel. À défaut de renseignement statistique sur le trafic téléphonique d'une entreprise (hors centre d'appel), on formule l'hypothèse suivante (valeurs statistiques admises par la profession) : le trafic d'un poste, à l'heure de pointe, est évalué à 0,12 erlang se répartissant comme suit :

– 0,04 erlang en trafic sortant,
– 0,04 erlang en trafic entrant,
– 0,04 erlang en trafic interne à l'entreprise.

21.2.2 Le dimensionnement du raccordement au réseau de l'opérateur

La spécialisation des lignes

On appelle liaison d'abonné (boucle locale), la ligne entre le réseau public (commutateur de rattachement) et l'installation d'abonné. On distingue trois types de lignes (figure 21.12) :

– les lignes **SPA** (Spécialisées arrivée point A), ce sont des lignes qui ne peuvent acheminer que des appels sortants (vers le réseau de l'opérateur ou point A) ;
– les lignes **SPB** (Spécialisées arrivée point B), ce sont des lignes qui ne peuvent acheminer que des appels entrants (vers l'installation d'abonné ou point B) ;
– les lignes **mixtes**, ce sont des lignes qui acheminent indifféremment les appels entrants ou sortants, elles sont à la fois SPA et SPB.

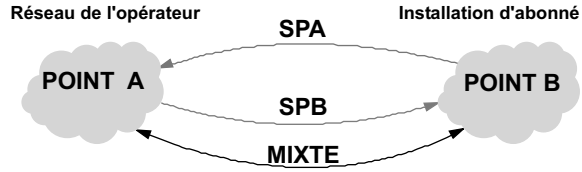


Figure 21.12 Les différents types de lignes.

On désigne par faisceau un ensemble de lignes de mêmes caractéristiques (faisceau de lignes SPA, faisceau de lignes SPB ou faisceau de lignes mixtes).

La spécialisation des lignes interdit la saturation des lignes par un type d'appel. Les appels sortants, limités par le nombre de SPA, ne peuvent occuper toutes les lignes téléphoniques de l'entreprise. Celle-ci, par la limitation des appels sortants (personnel de l'entreprise) favorise ainsi

3. Rappelons que l'erlang mesure l'intensité de trafic.

© Dunod – La photocopie non autorisée est un délit

les appels entrants (clients). Dans une telle conception, les lignes mixtes sont généralement vues comme des lignes de débordement.

Le dimensionnement des faisceaux de lignes

Généralement la potentialité d'appels simultanés (n) est supérieure aux ressources disponibles (m). Dans ces conditions, l'appel $m+1$ sera refusé. Le dimensionnement d'un faisceau consiste à déterminer, en fonction du trafic à écouler et d'une probabilité de refus par manque de ressource, quel est le nombre de circuits nécessaires. Erlang a établi que la probabilité ***p*** de refus d'appel, appelée aussi facteur de blocage, par suite d'encombrement pour un trafic à écouler de ***E*** erlang, dans un système possédant ***m*** lignes est donnée par la relation :

$$p = \frac{E^m/m!}{\sum_{k=0}^{k=m} E^k/k!}$$

Cette formule a permis d'établir des abaques de dimensionnement appelés abaques d'Erlang, dont une forme est représentée figure 21.13.

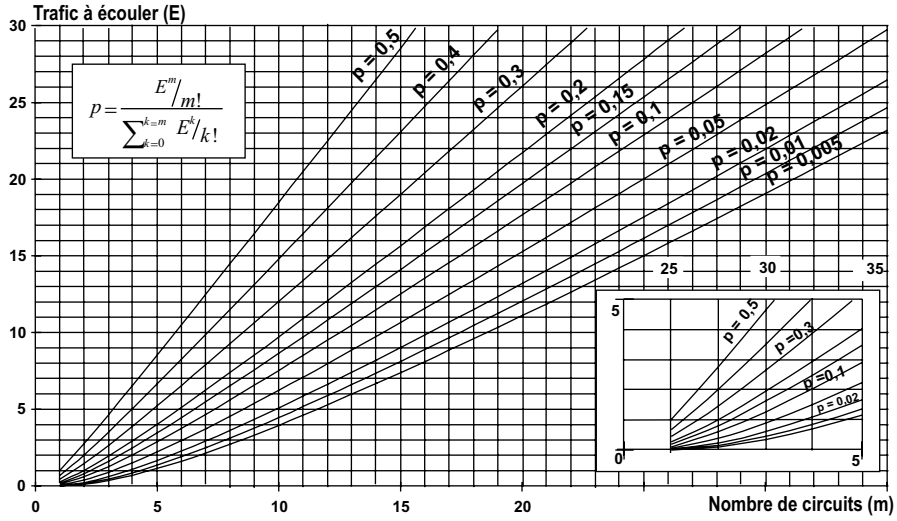


Figure 21.13 L'abaque d'Erlang (modèle à refus).

Le dimensionnement consiste à affecter à chaque faisceau un nombre de lignes suffisant pour écouler un certain trafic (exprimé en erlang) avec une certaine qualité de service. La méthode a été abordée au chapitre 5 (*Mutualisation des ressources*). Appliquée à la téléphonie, la définition du faisceau consiste, généralement, à déterminer le nombre de lignes SPA et SPB dans des conditions de services différentes.

En principe, dans les entreprises, les appels sortants et entrants subissent un traitement différent. Les appels sortants, ceux du personnel vers l'extérieur, sont, en cas de manque de ressource, systématiquement refusés. En ce qui concerne les appels entrants (ceux des clients), ils peuvent être refusés par manque de ressource (ligne non disponible), mais aussi mis en attente lorsque le correspondant demandé est déjà en communication. Ce procédé monopolise une ressource en arrivée

et n'écoule aucun trafic. Dans ces conditions, la probabilité p_a pour qu'un nouvel appel entrant soit refusé par manque de ressource est plus importante. Cette probabilité est donnée par la relation (modèle dit à attente) :

$$p_a = \frac{(E^m/m!) \cdot \left(\dfrac{m}{m-E}\right)}{\left(\displaystyle\sum_{k=0}^{k=m-1} E^k/k!\right) + \left[(E^m/m!) \cdot \left(\dfrac{m}{m-E}\right)\right]}$$

Généralement, les lignes SPA sont définies selon le modèle à attente et les lignes SPB selon le modèle à refus. Notons que le modèle d'Erlang est un modèle pessimiste, le nombre de lignes sera toujours arrondi au nombre entier inférieur.

21.3 LES RÉSEAUX PRIVÉS DE PABX

21.3.1 Principes généraux

La volonté de maîtriser les coûts et d'harmoniser, au sein de l'entreprise, l'ensemble des services a conduit les responsables télécoms des entreprises à réaliser l'interconnexion de leur parc de PABX (Réseaux privés à intégration de services ou **RPIS**).

Interconnecter deux ou plusieurs PABX consiste à les relier par un ensemble de liens privés (faisceau) ou publics loués afin d'acheminer, sans transiter par le réseau public, les appels téléphoniques inter-établissement (figure 21.14).

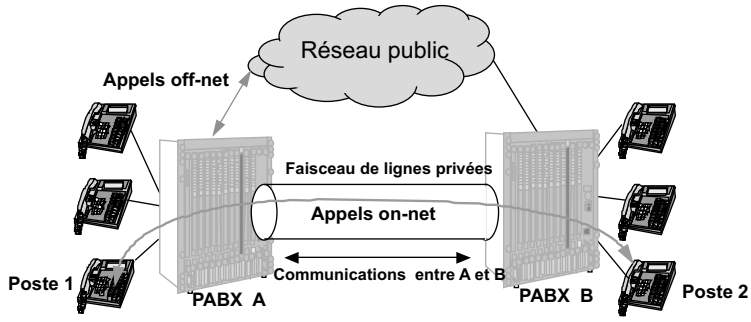


Figure 21.14 Principe d'un réseau privé de PABX.

Dans ce mode de fonctionnement, un préfixe de numérotation (souvent le 0) permet d'identifier les appels destinés à être acheminés par le réseau public (**appels *off-net***). Les appels internes au réseau (**appels *on-net***) sont établis en utilisant un plan de numérotation propre à l'entreprise. Une table, dite table d'acheminement (table de routage), configurée manuellement dans chaque PABX, achemine l'appel vers le faisceau qui relie le PABX de l'appelant au PABX de l'appelé.

Généralement, le plan de numérotation interne à l'entreprise utilise les quatre derniers chiffres du numéro SDA (MCDU[4]) de celle-ci. Les numéros publics (série SDA) sont fournis par l'opérateur, l'entreprise n'a aucune maîtrise sur les numéros accordés. Dans ces conditions, il est non

4. MCDU, Millier Centaine Dizaine Unité, désigne les quatre derniers chiffres du numéro E.164 de l'installation de l'abonné (ZZ ABPQ MCDU) ; SDA, Sélection directe à l'arrivée.

© Dunod – La photocopie non autorisée est un délit

seulement difficile mais aussi dangereux (changement de séquence SDA) de réaliser une numérotation homogène à partir de ces seuls chiffres sur l'ensemble des sites constituant le réseau. Pour éviter d'adopter une numérotation interne différente de la numérotation externe (numéro interne différent du MCDU), chaque site est généralement identifié par un préfixe utilisé pour le routage des appels. La figure 21.15 présente un exemple de réseau utilisant un plan de numérotation global et homogène pour toute l'entreprise. Le préfixe 2*x* est utilisé pour distinguer les appels *on-net* (2*x*) des appels *off-net* (préfixe 0). Dans notre exemple, le chiffre *2*, premier chiffre du préfixe indique un appel *on-net* et le deuxième chiffre (*x*) identifie le site distant.

Table d'acheminement du PABX 21

Numéro	Faisceau
22*	B
23*	E
24*	B
25*	A
22*	E
23*	B
...	

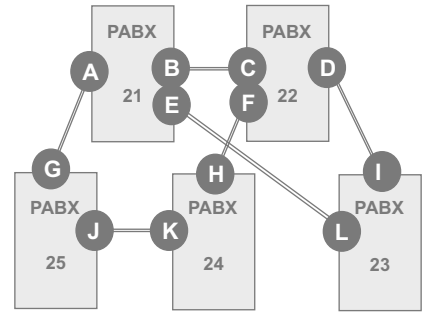


Figure 21.15 Principe d'un plan de numérotation privé.

En cas d'occupation d'un faisceau, un faisceau de débordement peut être spécifié. Par exemple, si toutes les lignes du faisceau B sont occupées, il est possible d'acheminer le trafic à destination du site 22 en transitant par le site 23 (faisceau E). Dans certains réseaux, pour garantir qu'un appel pourra aboutir (taux de service important), le réseau public peut être programmé comme faisceau de débordement. Dans ce cas, une table locale dite table de transformation de numérotation assure la traduction entre le numéro interne de l'appelé et son numéro sur le réseau public.

Lorsque l'un des PABX mis en réseau ne dispose d'aucun accès sur le réseau public, il est complètement asservi à un autre PABX du réseau. Il ne constitue alors qu'une simple unité de raccordement d'abonnés déportée (**URAD**). Cette relation entre deux PABX est dite siège/satellite. C'est l'ordinateur siège qui gère les communications (établissement, restrictions utilisateurs...) et établit la taxation.

Indépendamment des économies réalisées par la gratuité des communications internes au réseau (appels *on-net*), une économie sur les appels « longue distance » vers des usagers non raccordés au réseau privé peut être réalisée. En confiant, au PABX le plus proche de l'appelé, le soin d'établir la communication, celle, demandée par un abonné du PABX B de la figure 21.16 vers un abonné du réseau public, en zone de taxation locale du PABX A, conduit à la facturation au PABX A d'une communication locale en lieu et place d'une communication longue distance au PABX B.

La réalisation d'un réseau privé de PABX soulève les difficultés suivantes :

– détermination de la capacité du faisceau d'interconnexion. Ce problème a été abordé et les méthodes de résolution (loi d'Erlang) ont été étudiées précédemment ;

– l'hétérogénéité des PABX. Indépendamment des normes qui diffèrent d'un pays à un autre (raccordement, compression de la voix...), les constructeurs utilisent des protocoles de signalisation propriétaires et des services spécifiques. La réalisation d'un réseau de PABX se trouve

généralement confronté à un existant hétérogène. La qualité de service offerte aux utilisateurs est alors réduite au plus petit dénominateur commun ;

– le choix des liaisons entre les différents PABX, liaison analogique (**LIA,** Liaison inter-automatique) ou numérique (**MIC**). La première ne convient que lorsque le nombre de liens à établir entre deux sites est faible (2 à 3) et que les éléments à relier sont proches (interne à l'établissement).

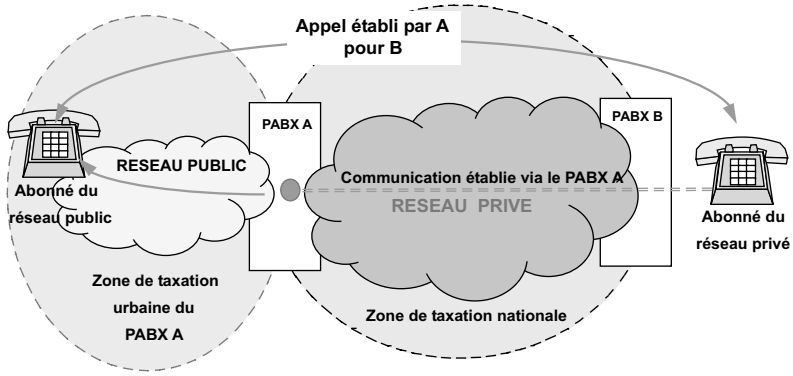


Figure 21.16 Principe de l'aboutement de réseau.

21.3.2 La signalisation et type de liens

La signalisation téléphonique est constituée d'un ensemble d'informations décrivant l'état de la ligne (libre, occupée...), la numérotation (signal d'enregistreur) et éventuellement les téléservices associés (figure 21.17). La signalisation peut être de type voie par voie (à chaque canal est associée une voie de signalisation) ou par canal sémaphore. La signalisation est alors commune à tous les canaux, elle est dite aussi signalisation en mode message (ex. : SS7).

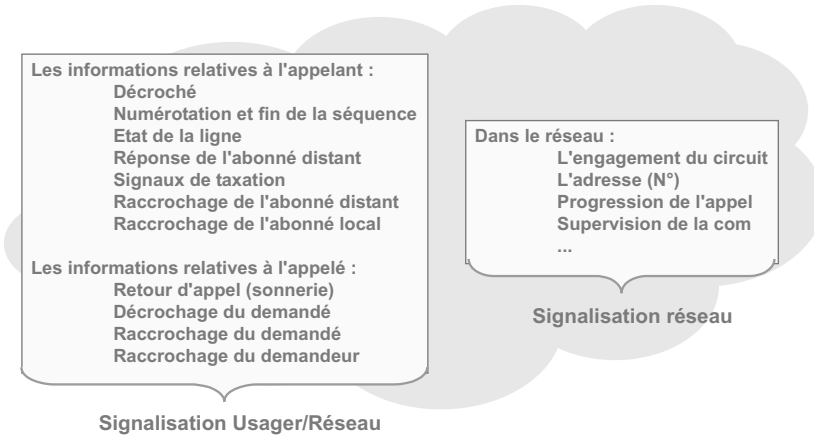


Figure 21.17 Les exemples d'événement de signalisation.

© Dunod – La photocopie non autorisée est un délit

La signalisation voie par voie sur lien analogique

Le principe général des liaisons analogiques entre PABX (LIA, Liaison inter-automatique) est illustré par la figure 21.18. Les informations de voix et la signalisation sont séparées. La signalisation est dite **RON/TRON** (Réception et transmission ou **E&M**, *Earth & Mouth*). Les fils voix sont généralement désignés fils AB. Une liaison LIA n'achemine qu'une communication téléphonique et la signalisation de cette communication (signalisation voie par voie). Il faut autant de LIA entre les PABX raccordés que de communications téléphoniques à écouler simultanément.

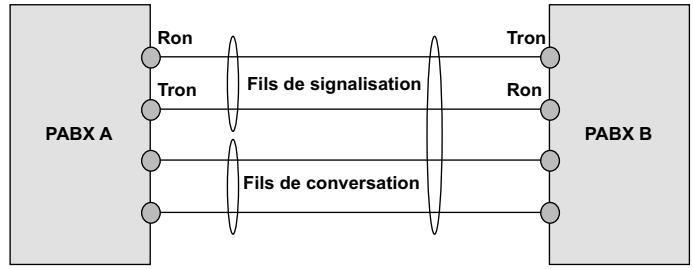


Figure 21.18 Principe d'une liaison LIA et de la signalisation RON/TRON.

Dans ce schéma de principe, les informations d'état de la liaison comme par exemple la prise de ligne sont transmises par les fils RON/TRON. L'invitation à numéroter et le retour de sonnerie sont transmis sur les fils voix. Selon le nombre de fils utilisés, le mode de signalisation d'état (niveaux de tension, impulsions de tension, impulsions à 50 Hz...), on distingue 4 types de LIA :

- **LIA à changement d'état**, les différents événements sont signalés par le potentiel des fils RON et TRON. Des polarités permanentes sont maintenues pendant toute la durée de la communication sur les fils RON/TRON. La numérotation est transmise par coupure du fil TRON ou en numérotation multifréquentielle (Q.23) sur les fils voix ;
- **LIA à impulsions codées**, les différents événements sont représentés par des impulsions de 48 V calibrées en durée. La durée de l'impulsion est significative de l'état à signaler, la prise de ligne est, par exemple, signalée par une impulsion de 100 ms. La numérotation est transmise par coupure du signal positif sur le fil TRON de l'émetteur (numérotation décimale) ou sur les fils voix (numérotation fréquentielle ou Q.23) ;
- **LIA à impulsions codées 50 Hz**, ce type de LIA n'utilise que 2 fils. La signalisation est transmise sous forme d'impulsions codées (50 Hz, 70 V). De même, la numérotation est envoyée sous forme d'impulsions à 50 Hz (50/50 ms) ou en Q.23 ;
- **LIA à courant continu**, seuls deux fils sont utilisés. Ils servent à la parole et à la signalisation. Ce type de raccordement est en principe utilisé pour les liaisons d'abonnés. Les différents états (prise de ligne et libération) sont détectés par ouverture ou fermeture de la boucle de courant. La numérotation est décimale (impulsions de numérotation 33/66 ms) ou fréquentielle (Q.23).

Les LIA à changement d'état ou à impulsions codées peuvent être à 2 ou 4 fils RON/TRON et à 2 ou 4 fils conversation (2 fils conversation émissions, notés fils CD et 2 fils de conversation réceptions, notés fils AB). Ces systèmes supportent la signalisation de type COLISEE[5] et SOCOTEL

5. Ensemble de signaux (impulsions calibrées), d'origine France Telecom, décrivant tous les événements d'une communication téléphonique.

multifréquences (Q.23). La figure 21.19 illustre une liaison entre PABX réalisée à l'aide d'une LIA de type V.

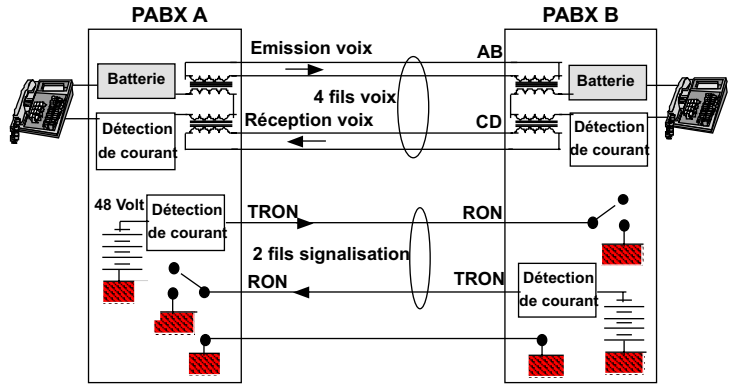


Figure 21.19 La liaison LIA à changement d'état de type V.

En fonction de l'emplacement des sources d'alimentation (48 V) de la signalisation, les LIA sont classées en type (LIA de type I à V). Les LIA de type V sont les plus utilisées. Le passage de la liaison voix de 2 en 4 fils provoque, en cas de désadaptation d'impédance, un phénomène d'écho très perturbant qu'il convient d'éliminer. L'UIT prescrit l'utilisation de dispositifs d'annulation d'écho dès que le temps de transit dans le réseau est supérieur à 24 ms.

La signalisation voie par voie sur lien numérique

Le principe d'une liaison numérique est représenté par la figure 21.20. Une liaison de ce type comporte 4 fils (une paire émission et une paire réception). Chaque IT de la trame multiplexée est affecté à un canal voix. La signalisation de chaque voie (signalisation voie par voie) peut être transportée dans un IT dédié (signalisation hors bande) ou dans la même voie que la communication (signalisation dans la bande). Cette signalisation est dite **signalisation CAS** (*Channel Associated Signaling* ou signalisation par canal associé).

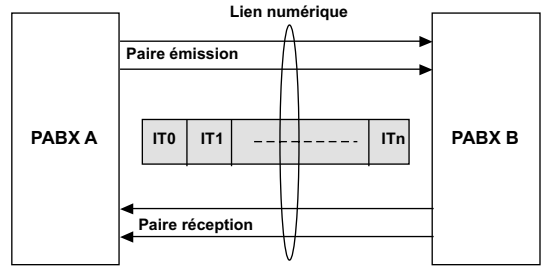


Figure 21.20 Principe d'une liaison numérique.

Deux types de trames multiplexées peuvent être utilisés. Elles diffèrent par le nombre d'IT qui les compose et le mode de signalisation utilisé :

– la trame européenne ou **E1** comporte 32 IT de 64 kbit/s. Couramment appelée trame MIC, elle assure un débit utile maximal de 1 920 kbit/s ;

© Dunod – La photocopie non autorisée est un délit

– la trame nord-américaine (utilisée aussi au Japon) ou **T1** comporte 24 IT de 64 kbit/s pour un débit total de 1 544 kbit/s et utile de 1 536 kbit/s.

L'organisation de ces trames a été vue au chapitre 13, nous ne ferons ici qu'en rappeler le principe. La signalisation comporte deux types d'informations, celles relatives à la structure de la trame (ou signalisation de supervision) et celles en rapport avec l'état de chaque canal téléphonique (signalisation voie par voie ou CAS).

La trame de base T1[6] (trame G.733, aussi notée DS1 à DS12), représentée figure 21.21, comprend 24 IT (DS0) de 8 bits (192 bits). La multitrame de premier niveau regroupe 12 trames de base. Chaque trame de base est précédée d'un bit (bit de tramage constituant la signalisation de supervision). Ces 12 bits forment un mot (**mot SF**, *SuperFrame*) représentant la séquence binaire « 100011001100 » et identifiant la trame.

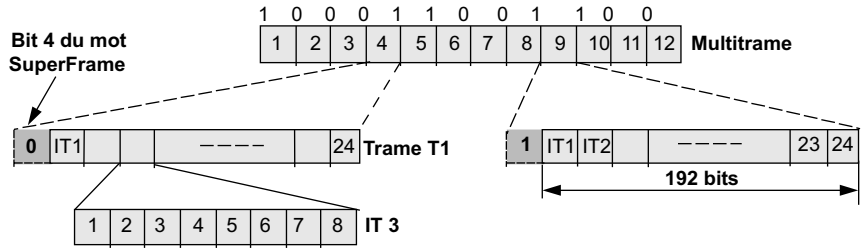


Figure 21.21 L'organisation de la multitrame T1 (G.733).

La signalisation téléphonique de chacune des voies est réalisée par vol, toutes les 6 trames, du bit de poids faible dans l'IT voix correspondante (un bit de signalisation est substitué au bit d'information, c'est une signalisation dans la bande).

L'organisation de la trame E1 (G.732) est représentée figure 21.22. Elle comporte 32 IT dont deux sont utilisés pour la signalisation (signalisation hors bande). L'IT0 de chaque trame est dédié à la supervision de la trame (identification du début de la trame) et à sa gestion. L'IT16 est utilisé pour la signalisation de chaque voie (signalisation CAS).

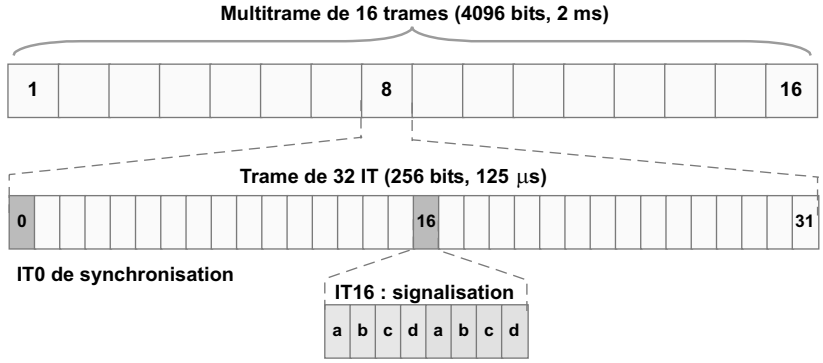


Figure 21.22 L'organisation de la multitrame E1 (G.732).

6. T*x* désigne le canal de transmission, DS*x* le format des données.

La signalisation (figure 21.23) de chaque IT sur 4 bits (bit a, b, c et d) est transportée dans l'IT16 de chaque trame. Chaque IT16 transporte la signalisation de deux voies.

***Time Slot* 16 (IT 16)**								
Trame 0	**Trame 1**		**Trame 2**		**Trame n**		**Trame 15**	
MVM Mot de verrouillage Multitrame	abcd IT1	abcd IT17	abcd IT2	abcd IT18	abcd IT*n*	abcd IT*n*+16	abcd IT15	abcd IT31

Figure 21.23 L'organisation de l'IT6.

Mise en place lors de la transition de la téléphonie analogique vers la téléphonie numérique, la signalisation CAS traduit et transporte la signalisation analogique. De ce fait, elle ne comporte que les événements relatifs à la gestion de la ligne (prise de ligne, état occupé...). Une impulsion de la signalisation analogique est traduite par le positionnement à 1 du bit « *a* » durant 150 ms. La figure 21.24 illustre la gestion des bits *a* et *b* (signalisation R2 ou Q.421) qui est une transposition numérique de la signalisation RON/TRON. La numérotation par impulsion (33/66) est transportée en émission par le bit « *a* », alors que la numérotation DTMF (Q.23) est acheminée en transparence sur le canal de voix.

Fonction	**Émission**		**Réception**	
	a	**b**	**a**	**b**
Repos	1	0	1	0
Prise de ligne	0	0	1	0
Invitation à numéroter	0	0	1	0
Impulsions de numérotation	0/1/0	0	1	1
Réponse	0	0	0	1
Raccrochage du demandé	0	0	1	1
Libération avant établissement	1	0	1	1
puis			0	1
Impulsions de taxation	0	0	0/1/0	

Figure 21.24 La gestion du bit a.

La signalisation par canal sémaphore sur lien numérique

La signalisation par canal sémaphore ou signalisation **CCS** (*Common Channel Signaling*) utilise un canal dédié (IT 24 de la trame T1, IT 16 de la trame E1) pour signaler tous les événements relatifs aux communications établies sur la trame (signalisation, en mode message, commune à tous les IT). Les protocoles utilisés sont des protocoles enrichis de type protocole D, CCITT N°7 (SS7) ou propriétaire (l'IT est alors dépendante du constructeur).

La signalisation par canal sémaphore est adoptée par tous les constructeurs. Cependant, les PABX multiservices offrent aux utilisateurs des fonctionnalités plus riches que celles implémentées dans les protocoles de signalisation normalisés (figure 21.25).

© Dunod – La photocopie non autorisée est un délit

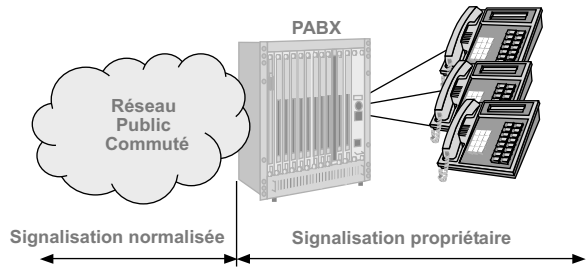


Figure 21.25 Le PABX et la signalisation.

La signalisation et le réseau de PABX

Deux approches de la mise en relation de PABX sont à considérer. Dans la première, il s'agit simplement d'acheminer des communications téléphoniques sur des liens privés sans apport de téléservice aux utilisateurs (interconnexion de PABX). Dans la seconde approche, il s'agit non seulement d'acheminer les communications téléphoniques mais aussi les services associés (réseau de PABX ou multisite).

➤ Interconnexion de PABX

Dans un réseau de PABX interconnectés, chaque PABX joue le rôle d'interface entre l'installation locale et le réseau privé d'une part et d'autre part entre l'installation locale et le réseau public. Lorsqu'un PABX est utilisé en tant que commutateur du réseau, il est dénommé PABX de transit, il achemine alors les communications téléphoniques et la signalisation associée (figure 21.26).

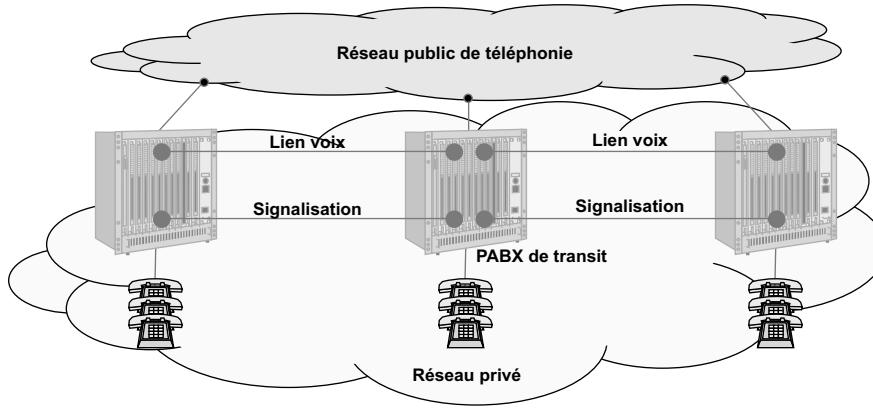


Figure 21.26 L'interconnexion de PABX.

Pour des liaisons analogiques (LIA), la signalisation peut être transportée sur les fils de voix (LIA 2 fils) ou sur des fils séparés des fils voix (LIA 4 fils). Pour les liaisons numériques (MIC) un intervalle de temps, généralement l'IT16, peut être dédié au transport de la signalisation mais celle-ci peut aussi être transportée par une liaison distincte. Chaque PABX de transit, interprétant la signalisation, peut éventuellement faire une conversion de celle-ci (arrivée sur un lien analogique et départ sur un lien numérique).

➤ Mise en réseau de PABX (multisite)

La réalisation d'un réseau multisite (ensemble du réseau vu comme un PABX virtuel) impose l'homogénéité de la signalisation sur l'ensemble du réseau. La figure 21.27 illustre le raccordement de trois PABX en réseau. Le lien d'interconnexion est un lien numérique structuré (MIC) avec ou sans IT16 selon les besoins de la signalisation du constructeur. Généralement, dans le cas d'une signalisation **CSS** (mode message), l'IT16 peut être banalisé, la signalisation prise de ligne, numérotation et autres événements étant transportés par le canal sémaphore affecté à un autre IT.

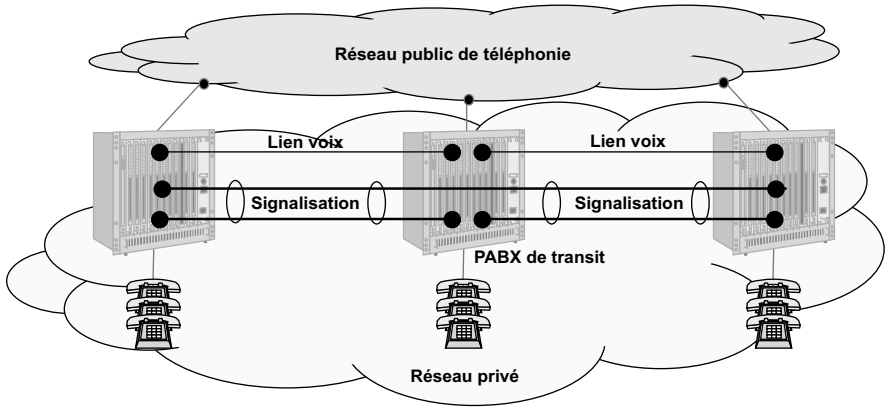


Figure 21.27 Le PABX en réseau et le transport de la signalisation propriétaire.

La différence essentielle entre une interconnexion simple de PABX et un réseau de PABX (réseau dit aussi multisite) réside dans le transport de la signalisation. Dans ce dernier cas, l'ensemble des PABX est vu comme un PABX virtuel et un lien de signalisation en point à point doit être établi entre chaque PABX (réseau sémaphore), ce lien peut être dédié ou n'être qu'un circuit virtuel d'une liaison X.25 entre les PABX. Le canal X.25 peut être séparé du lien voix (liaison LIA ou numérique) ou être transporté dans un IT d'une liaison numérique (MIC). L'utilisation de la signalisation SS7 simplifie le mode de diffusion de la signalisation, mais celle-ci devant être acheminée à travers le réseau nécessite qu'une fonction de commutation spécifique soit disponible dans les PABX (réseau de signalisation).

➤ Mise en réseau de PABX en milieu hétérogène

L'interconnexion de PABX hétérogènes se heurte à la non-homogénéité des protocoles de signalisation. La nécessité de disposer d'un protocole commun d'interconnexion a été résolue par le standard **DPNSS** (*Digital Private Network Signalling System*), très utilisé en Grande-Bretagne mais non conforme au modèle OSI. Les sociétés Alcatel et Siemens, rejoints par l'ensemble des grands constructeurs, ont fondé le forum **IPNS** (*ISDN PABX Networking Specification*) destiné à définir un protocole commun d'interconnexion conforme au modèle OSI. Les travaux ont abouti à la normalisation (ECMA - ETSI - ISO) du protocole **Q-SIG** (*Signalisation au point Q*).

Q-SIG définit un point d'interconnexion (point Q) entre des réseaux hétérogènes. Ce n'est pas un protocole de bout en bout (usager à usager), chaque réseau reste sous le contrôle de son protocole propriétaire (figure 21.28).

© Dunod – La photocopie non autorisée est un délit

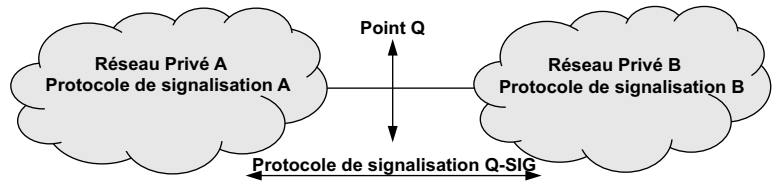


Figure 21.28 La position de la norme d'interconnexion Q-SIG.

Q-SIG, basé sur le protocole D (RNIS) dont il enrichit les messages, est orienté commutation de paquets en mode non connecté et connecté. Il ne définit que des services téléphoniques et non des fonctions de routage. Le transit (appel reçu par un PABX pour un usager raccordé à un autre PABX) est géré par le PABX sollicité en transit et non par le protocole d'interconnexion.

La figure 21.29 compare les différentes fonctionnalités disponibles selon le protocole de signalisation utilisé.

Services	LIA	Transgroupe[a]	Q-SIG	Propriétaire
Facilités en émission				
Accès sélectif au réseau	•		•	•
Substitution				•
Num abrégée sur l'ensemble du réseau				•
Facilité en réception				
Acheminement par opératrice	•	•	•	•
SDA Euro-Numéris	•	•	•	•
SDA Transgroupe	•	•	•	•
Renvois à distance			•	•
Renvois en cascade	•	•	•	•
Filtrage				•
Interception d'appels				•
Protection contre l'interception				•
Outrepassement				•
Facilités en communication				
Va-et-Vient	•	•	•	•
Reprise d'appel	•	•	•	•
Conférence à trois	•	•	•	•
Transfert poste libre ou occupé	•	•	•	•
Transfert avec annonce	•	•	•	•
Parcage avec reprise du correspondant				•
Rappel automatique sur poste occupé			•	•
Rappel automatique sur poste libre			•	•
Rappel automatique sur faisceau occupé			•	•
Identification d'appels malveillants				•
Facilités propres au poste opérateur				
Intervention prioritaire			•	•
Outrepassement des renvois			•	•
Outrepassement du non-dérangement			•	•
Affichage de l'état des terminaux (supervision)			•	•

Figure 21.29 La comparaison des services disponibles selon la signalisation utilisée.

Services	LIA	Transgroupe[a]	Q-SIG	Propriétaire
Facilités des postes numériques				
Affichage date et heure				•
Identification correspondant intérieur		•	•	•
Dépôt de message (aviser)				•
Rappel du dernier appelant			•	•
Renvoi sur sonnerie (dévier)			•	•
Facilités système				
Changement de catégorie programmée				•
Faisceau de lignes extérieures	•		•	•
Débordement automatique	•		•	•
Renvoi général	•	•	•	•
Taxation au fil de l'eau			•	•
Taxation extérieure				•
Prépaiement				•
Dialogue avec l'autocommutateur				
Gestion de la numérotation abrégée				•
Gestion de la catégorie des postes				•
Gestion de la taxation				•
Annuaire				•

a. La signalisation Transgroupe est la signalisation utilisée par France Telecom pour son offre de réseaux privés virtuels de téléphonie (Colisée Numéris).

Figure 21.29 La comparaison des services disponibles selon la signalisation utilisée. (suite)

21.4 PRINCIPES DES RÉSEAUX VOIX/DONNÉES

21.4.1 Généralités

Le budget téléphonie représente plus de 80 % des dépenses de télécommunication (voix, données) des entreprises. Très tôt, il est apparu qu'à partir d'un certain seuil de communication entre les divers établissements d'une entreprise, il devenait très avantageux de réaliser un réseau privé pour assurer le transport conjoint de la voix et de la donnée (partage de bande passante). L'échec de l'intégration des services de transport de données dans le PABX a conduit d'abord à la réalisation de réseaux voix/données à l'aide de multiplexeurs (figure 21.30).

21.4.2 Les réseaux de multiplexeurs

Dans les réseaux de multiplexeurs temporels (TDM), les intervalles de temps sont affectés à un canal voix ou données. De ce fait, lorsqu'une communication n'est pas établie, la bande qui lui est allouée est perdue. Dans la trame multiplexée représentée figure 21.31, les canaux 3 à 5, n'ayant aucune donnée à transmettre, sont inutilisés, la bande passante est perdue.

L'avantage des multiplexeurs temporels réside essentiellement dans la simplicité des algorithmes de gestion, ce qui autorise des temps de traitement courts et donc de faibles délais de transit, dans le réseau. Cependant, le TDM n'est pas une technique adaptée aux transferts de données sporadiques comme en provoque l'interconnexion des réseaux locaux.

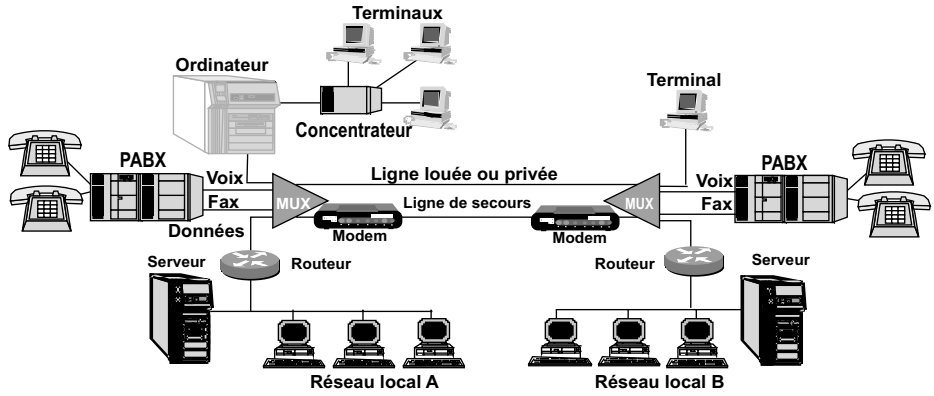


Figure 21.30 Principe des réseaux voix/données.

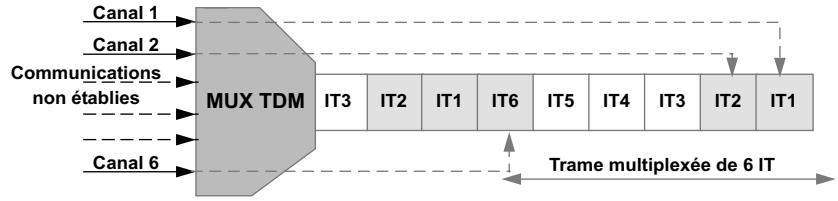


Figure 21.31 Principe de l'allocation statique des canaux dans un MUX TDM.

21.4.3 La voix paquétisée

Généralités

Plusieurs raisons conduisent à transmettre la voix sur des systèmes à commutation de paquets :

- la téléphonie traditionnelle est orientée connexion, deux canaux de 64 kbit/s sont ouverts en permanence entre les deux interlocuteurs, même pendant les périodes de silence ;
- le caractère *half duplex* d'une conversation et les temps de silence font que 60 % de la bande allouée à une communication téléphonique n'est pas utilisée ;
- la commutation de paquets permet de mutualiser les ressources (multiplexage statistique) ;
- l'utilisation d'une même infrastructure pour la donnée et la voix est génératrice d'économie, notamment dans la mise en œuvre des réseaux.

Transporter la voix sur un réseau en mode paquet nécessite de modéliser le flux voix comme un flux de données en transformant le flux d'information continu (échantillons de voix) en un flux périodique (paquets). Si on peut garantir, aux paquets, un transfert respectant les contraintes temporelles du transfert isochrone, il est alors possible d'utiliser un réseau à commutation de paquets pour transmettre la voix. Le multiplexage par étiquette, utilisé par la commutation de paquets, garantit une utilisation optimale de la bande (figure 21.32), une administration unifiée du réseau, une réduction des coûts (la voix étant transportée selon la tarification de la donnée, généralement forfaitaire) et, si l'entreprise ou l'opérateur disposait d'un réseau voix et d'un réseau données séparés, la suppression des coûts de l'infrastructure téléphonique.

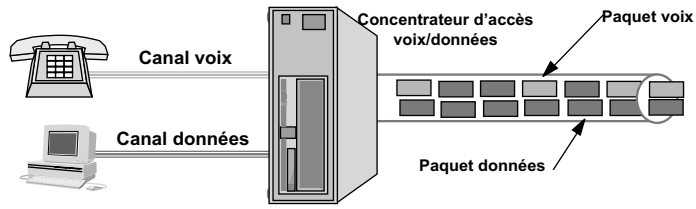


Figure 21.32 La paquétisation de la voix et réseau à commutation de paquets.

Pour garantir le transport de la voix, les systèmes d'interconnexion de réseaux voix/données doivent assurer :

– un débit minimal garanti, les flux voix ne devant jamais occuper plus de 50 % de la bande passante du support ;
– un transfert dans un délai aussi réduit que possible par prioritisation des flux voix (< 150 ms, avec une tolérance jusqu'à 200 ms) ;
– la maîtrise de la gigue dans le réseau (< 40 ms, avec une tolérance jusqu'à 70 ms) et sa correction dans la passerelle destination ;
– la reprise sur erreur n'ayant aucun sens pour les flux temps réel et, malgré une faible sensibilité de la voix aux erreurs, un transfert correct de la voix nécessite un taux de perte inférieur à 1 % (paquets erronés, mais aussi paquets retardés), avec une valeur limite de 3 % ;
– enfin, pour garantir une utilisation optimale de la bande passante, un système de détection des silences doit être implémenté (**DSI**, *Digital Speech Interpolation*).

Les techniques mises en œuvre dans les réseaux voix/données

➤ Compression de la voix

Afin d'optimiser l'utilisation de la bande passante, les techniques de compression de voix sont implémentées dans tous les systèmes voix/données. Ces techniques apportent une réduction importante de la bande utilisée en contrepartie d'un temps de traitement non négligeable.

La voix analogique est numérisée et codée par le PABX (**MIC** ou **PCM** *Pulse Code Modulation*, norme G.711 à 64 kbit/s), l'équipement d'interconnexion effectue ensuite la compression (figure 21.33). Il ne s'agit pas réellement de compression des données voix, mais d'un codage spécifique réducteur de bande (chapitre 1).

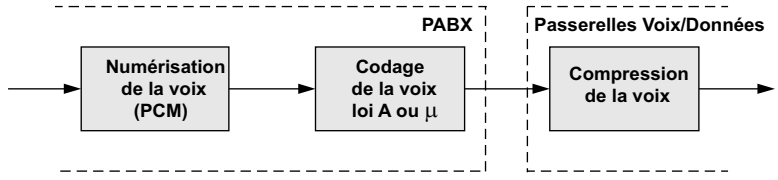


Figure 21.33 Principe de la compression de voix.

La méthode la plus simple, et donc la plus économique est l'**ADPCM** (*Adaptive Differential Pulse Code Modulation,* norme G.726). L'ADPCM réalise un codage différentiel par comparaison de la valeur de chaque échantillon à la valeur de l'échantillon précédent. Le sens de la variation est

© Dunod – La photocopie non autorisée est un délit

codé sur un bit, l'amplitude sur 1, 2 ou 3 bits, ce qui correspond respectivement à des débits de 16, 24 ou 32 kbit/s. Indépendamment de la réduction de bande, l'ADPCM est plus résistant aux erreurs que le codage MIC. Cependant, cette technique est aujourd'hui obsolète.

Des techniques plus élaborées s'appuient sur les caractéristiques du spectre de fréquence de la parole. Ces systèmes analysent (2,5 à 30 ms, selon le système) la voix et réalisent une prédiction linéaire du signal de voix à partir des quatre derniers échantillons (vecteur). Ils comparent le vecteur obtenu à une table de vecteurs préétablie, seul l'index d'entrée dans la table et une information d'amplitude sont envoyés au récepteur. Ce dernier reconstitue le signal d'origine à partir du vecteur et d'une série de filtres modélisant le conduit vocal de l'interlocuteur. Les codeurs **CELP** (*Code Excited Linear Predictive*) sont particulièrement performants. Ils n'introduisent qu'un faible retard dû à l'acquisition des données et à la prédiction (prétraitement de la trame suivante ou *Look ahead*). Plusieurs variantes existent. La figure 21.34 présente les différents systèmes et leurs caractéristiques. La qualité de restitution est exprimée en **MOS** (*Mean Opinion Score*). Cette notation réalisée par un groupe de personne sur l'écoute de plusieurs échantillons de voix est toute subjective.

Codec	Appellation	Débit (kbit/s)	Délai (ms)	MOS	Calcul (MIPS)	Trame (octets)	Commentaire
G.711	PCM	64	0,125	4,2	0,34	1	Compression logarithmique. Téléphonie et H.320.
G.721	ADPCM	32	0,125	4,4			Échantillon codé sur 4 bits
G.722	ADPCM	48, 56, 64	< 3				Spectre sonore de 50-7 000 Hz. Utilisation visioconférence (H.320).
G.722-1	ADPCM	16, 24, 32					Version 16 kbit/s supportée par Windows Messenger.
G.723	ACELP	5,3 et 6,4	90	3,9	16	20	
G.723-1	ACELP, MP-MLQ		37,5	3,9	16	24	H.323, H.324M (UMTS-99).
G.726	ADPCM	16, 24, 32, 40	< 3	4,5 à 2.0	14		Décomposition du spectre en sous-bande. Remplace G.721.
G.727	ADPCM	16, 24, 32, 40		3,9	33		Complète G.726. Changement du nombre de bits (débit) en cours de conversation.
G.728	LD-CELP	16	2,5	3,9			Trame courte de 2,5 ms.
G.729	CS-ACELP	8	15	3,92	20	10	Concurrent de G.723.1, recommandé pour voix sur Frame Relay et H.323.
G.729 a	CS-ACELP	8	15	3,7	10,4	10	G.729 + récupération des silences.

Le retard indiqué comprend le temps de codage et de décodage
MP-MLQ *Multiple Pulse Maximum Likelihood Quantizer*
LD-CELP *Low Delay CELP*
CS-ACELP *Conjugate Structure Algebric* CELP

Figure 21.34 La synthèse des systèmes de compression de voix.

Les normes G.72x ne traitent pas les silences (sauf G.729b). Durant les silences un signal réduit est transmis. Les normes G.729a et G.723.1 (ACLEP) sont les plus utilisées d'une part, pour la qualité du son restitué (figure 21.34) et, d'autre part pour la faible puissance de calcul nécessaire exprimée en MIPS (Million d'instructions par seconde). D'autres techniques autorisent des réductions de bande plus importantes. Toutefois, au-dessous de 8 kbit/s la qualité de restitution est généralement insuffisante.

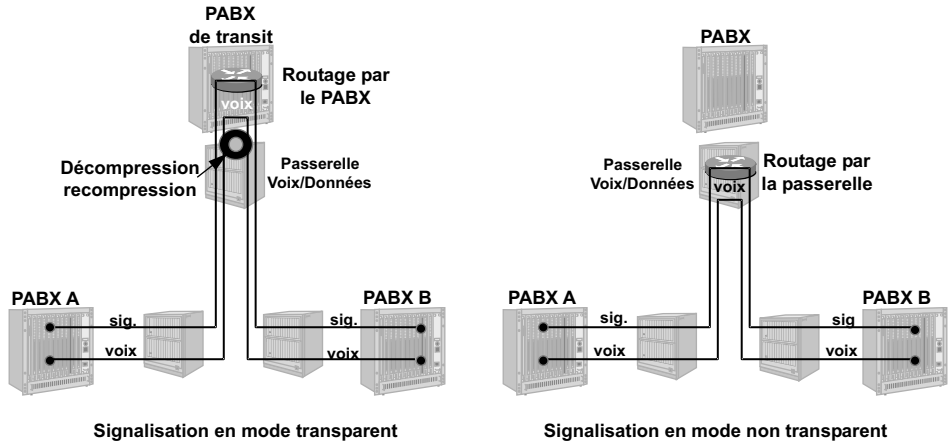


Figure 21.35 La communication entre les PABX A et B.

Dans un réseau voix/données deux modes d'établissement des communications sont envisageables. Le premier, le plus simple, consiste à transporter dans le réseau la signalisation de manière transparente. Les informations de signalisation ne sont alors pas interprétées par les équipements réseau (passerelles voix/données...) et sont acheminées comme des données ordinaires. Le routage des communications est alors réalisé par les PABX dits PABX de transit. Cette opération conduit à une décompression et à une recompression de la voix. Indépendamment des délais introduits, ce mode d'établissement des communications (figure 21.35) altère fortement la qualité de la voix et limite le nombre de bonds dans le réseau (opérations de compression et de décompression).

Dans le deuxième mode, dit non transparent, l'acheminement de la communication est réalisé par les équipements réseau qui interprètent la signalisation et assurent alors le routage de la communication. Le signal de voix n'a pas à être décompressé et recompressé. L'élongation du réseau n'est alors limitée que par les temps de transfert et de traitement.

➤ Limitation et correction de la gigue

Le temps total de transfert ou temps de bouche à oreille intervient dans l'interactivité de la communication téléphonique, alors que la variation de ce temps ou gigue est un processus réducteur de la qualité auditive de la communication. La gigue dans un réseau voix/données a deux origines. La première est liée aux délais variables de traitement des données par chaque élément du réseau, elle dépend de la charge de celui-ci et du dimensionnement du réseau (files d'attente). La seconde est liée directement à la nature des flux. Compte tenu de la spécificité des différents flux, dans les équipements voix/données, les flux voix et données sont séparés et mis en attente de traitement dans des files d'attente différentes. Le traitement de la voix bénéficie d'une priorité absolue, tant qu'un paquet de voix est présent, la file d'attente données est bloquée. Ce n'est qu'en l'absence de

© Dunod – La photocopie non autorisée est un délit

voix, ou entre deux paquets voix que les paquets de données sont traités et émis. La figure 21.36 illustre ce mécanisme. Les paquets de voix sont émis avec une période de récurrence constante (flux isochrone), cependant l'insertion d'un paquet de données engendre un retard dans l'émission du paquet voix suivant. Ce retard dépend de l'instant d'arrivée du paquet voix et de sa taille.

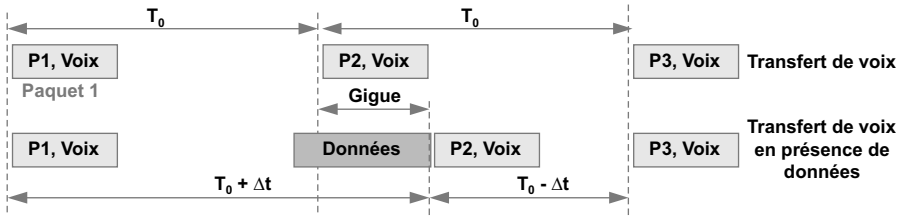


Figure 21.36 Introduction d'une gigue par l'émission d'un paquet de données.

Pour limiter la gigue, les paquets de données devront être aussi petits que possible (fragmentation des paquets de données en présence de paquets de voix). Chaque nœud intermédiaire franchi introduit, en présence de données, une variation du délai de transit. La gigue totale résulte de la somme des variations de délai introduites par chacun des nœuds. En sortie du réseau, la passerelle voix/données doit insérer un buffer « élastique » pour corriger cette gigue (figure 21.37). Si le buffer de gigue résout le problème de variation des délais, il allonge le temps de transfert de bout en bout.

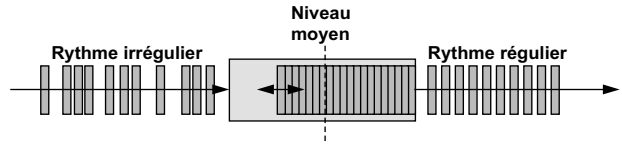


Figure 21.37 Principe de la correction de gigue par buffer « élastique ».

Si le protocole de transport transporte une information de séquencement, tout paquet retardé dans le réseau et arrivant hors séquence mais dans le délai de rétention du correcteur de gigue peut être inséré au bon endroit. Cette technique utilisée au-dessus des réseaux en mode datagramme (voix sur IP, protocole RTP) permet de rétablir, dans certaines limites, l'ordonnancement des paquets voix.

➤ Traitement des télécopies

La voix, même dégradée en qualité, est reconnaissable, il n'en est pas de même des données de télécopie (Fax G3). Les distorsions introduites par les codeurs bas débits interdisent la « reconstitution » d'un signal analogique correct. La solution généralement adoptée consiste à reconnaître les modulations, détecter la porteuse (exemple pour le V.29 porteuse à 2 100 Hz), la démoduler et transmettre, en utilisant un protocole de transport standard ou spécifique (**IFP**, *Internet Facsimile Protocol*, pour les réseaux VoIP), les données numériques issues du Fax comme une donnée ordinaire. Le système récepteur opérera à l'inverse en remodulant avant de remettre le signal au PABX destinataire.

➤ Traitement de l'écho

Le poste de l'usager est raccordé par deux fils, la liaison distante comporte généralement quatre fils (paire émission et paire réception). Un transformateur différentiel assure le passage de deux à quatre fils. Si l'adaptation d'impédance est mal réalisée, une partie de l'énergie est réfléchie : c'est l'écho. Les différents types d'écho sont représentés figure 21.38.

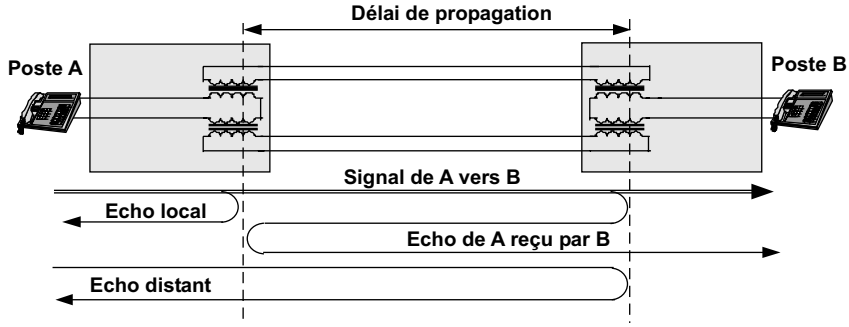


Figure 21.38 L'écho dans une liaison téléphonique.

L'écho local est peu gênant. Mais, à partir d'un certain délai de transmission, fonction de la distance séparant les deux PABX, l'écho distant peut devenir gênant. Supérieur à 45 ms, il constitue un véritable trouble de la conversation[7].

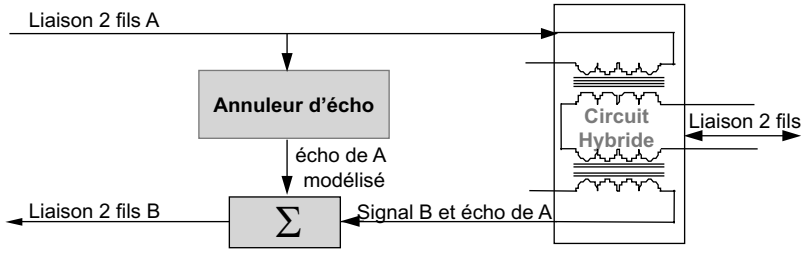


Figure 21.39 Principe de l'annulation d'écho.

S'il ne peut être évité, il convient de l'éliminer, les annulateurs d'écho effectuent cette fonction. Les annulateurs d'écho[8] construisent un modèle mathématique de la voix sur une voie, et réinjectent ce signal en opposition sur l'autre voie. Le principe des annulateurs d'écho est illustré figure 21.39. L'installation doit être symétrique (deux annuleurs d'écho par liaison).

L'écho perçu par le destinataire n'est gênant que s'il atteint un certain niveau vis-à-vis du signal utile. La recommandation G.131 indique les valeurs minimales de l'atténuation du signal d'écho (**TELR**, *Talker Echo Loudness Rating*) acceptables en fonction du délai moyen de transit dans le réseau. Cependant, compte tenu des délais importants introduits par les systèmes de voix paquétisée, la plupart des systèmes implémentent un annuleur d'écho.

7. L'IUT fixe à 24 ms le temps de propagation dans un réseau, au-delà, l'emploi d'annulateur d'écho est obligatoire.

8. Précédemment les réseaux utilisaient des suppresseurs d'écho, ces systèmes plus simples interdisaient la transmission *full duplex*. Lors de telles transmissions, il fallait inhiber la suppression d'écho par l'émission préalable d'un signal de commande à 2 100 Hz.

© Dunod – La photocopie non autorisée est un délit

➤ Traitement des silences

Lors d'une conversation seule une personne parle, son ou ses interlocuteurs écoutent et sont donc silencieux. Durant ces silences, le seul signal présent correspond aux bruits d'ambiance. Le signal de parole pouvant être modélisé (niveaux de puissance, spectre de fréquence), il est alors possible de détecter les silences et de ne rien transmettre durant ces instants. Cependant, l'absence de bruit chez le correspondant distant peut lui faire croire que son interlocuteur a raccroché. De même, en l'absence de réception d'information, le système local peut supposer un incident de ligne. Aussi, pour éviter ceci et recréer l'ambiance d'une communication téléphonique traditionnelle, des paquets spécifiques (paquets de silence) peuvent alors être émis pour signaler au système destinataire le silence. Celui-ci génère alors un bruit de fond. La bande passante récupérée peut ainsi atteindre 60 % de la bande nominale.

La figure 21.40 illustre un système de traitement des silences. Après l'étape de numérisation classique (G.711), la voix est analysée pour calculer le signal d'annulation d'écho (G.165/G.168). Afin de récupérer de la bande passante, le système de traitement des silences ou **VAD** (*Voice Activity Detection*) détecte les silences, la voix est ensuite compressée. Enfin, l'ensemble des informations est mis en paquets (paquets de voix ou paquets de silence). Les paquets de silence ne transportent aucune donnée, ils ne sont utilisés que pour signaler une absence de paquets voix, et non une perte, et ainsi, permettre au destinataire de générer un bruit aléatoire de fond.

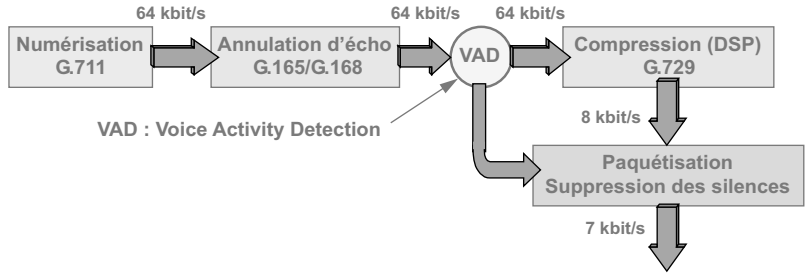


Figure 21.40 Exemple de système de traitement des silences.

Dans l'exemple de la figure 21.40, le débit minimal d'environ 7 kbit/s correspond au débit moyen de ligne après les diverses encapsulations du signal. Lors du dimensionnement d'un système voix/données, il ne faut pas tenir compte de cette récupération de bande pour définir les canaux voix, ils doivent l'être au maximum de la bande requise, soit dans notre exemple sur un réseau voix sur IP, et après les diverses encapsulations, 17,8 kbit/s (encapsulation RTP/UDP/IP/PPP).

➤ Contrôle d'erreur

Dans un système voix en mode paquet, chaque paquet transporte l'équivalent de plusieurs échantillons de voix, la perte d'un paquet correspond donc à la perte de plusieurs échantillons. Compte tenu des délais, la reprise sur erreur n'est pas envisageable. Il est alors possible de dupliquer le paquet précédent ou même de reconstruire, *via* des algorithmes prédictifs, les échantillons du paquet manquant. D'autres techniques peuvent être utilisées, comme la redondance (envoi de deux fois le même paquet) et l'entrelacement. Ces techniques allongent les délais et consomment de la bande passante.

Si le taux de pertes devient important, la reconstitution du flux voix n'est pas possible (> 3%). La qualité de service est l'un des éléments essentiel d'un réseau voix/données, aussi la voix sur

IP met en œuvre un protocole particulier **RTCP** (*Real-Time Transport Protocol*) pour informer les systèmes d'extrémité de la gigue, du taux moyen de perte de paquets...

Les modes de relation téléphonique dans les réseaux en mode paquet

Trois modes de mise en relation téléphonique peuvent être distingués (figure 21.41). Un réseau voix/données peut mixer ces différentes configurations :

– le mode « postes de service » met en relation directe deux ou plusieurs postes téléphoniques analogiques isolés utilisant la signalisation RON/TRON. L'interface **FXS** (*Foreing eXchange Station*) émule vis-à-vis du poste téléphonique un PABX ;
– le mode « postes déportés » permet de relier un ou plusieurs postes analogiques distants (signalisation RON/TRON) à travers une interface **FXO** (*Foreing eXchange Office*) et FXS à un PABX distant. Les postes distants ont accès aux postes de l'installation locale, et réciproquement. Ils ont aussi accès, *via* le PABX, au réseau téléphonique public. L'interface FXO émule vis-à-vis du PABX un ou plusieurs postes téléphoniques ;
– le mode « interconnexion de PBX » vise à la réalisation de réseaux privés de téléphonie, il utilise des interfaces de type LIA ou E1. Outre la voix, ce système assure le transfert de la signalisation téléphonique (RON/TRON, Q.931, MF Socotel, Colisée, QSig...).

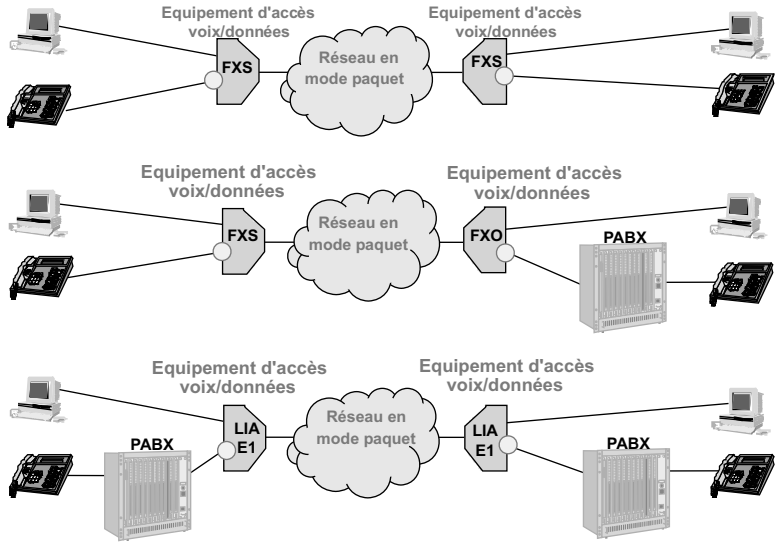


Figure 21.41 Le mode de mise en relation à travers un réseau en mode paquet.

21.5 LA VOIX SUR ATM

Initialement prévu pour assurer l'évolution du réseau RNIS vers le large bande, ATM assure de manière native le transport de la voix au-dessus de l'AAL1 (service **CBR**, *Constant Bit Rate*). Pour optimiser l'utilisation de la bande passante, l'ATM Forum a spécifié deux modes d'utilisation de l'ATM pour réaliser des réseaux voix/données (figure 21.42), le mode CES et le mode VTA.

© Dunod – La photocopie non autorisée est un délit

Le mode **CES** (*Circuit Emulation Structured*) permet l'interconnexion de PABX *via* un réseau ATM. La signalisation, transportée en mode transparent, est interprétée par les PABX qui effectuent le routage des communications, ces PABX sont dits : PABX de transit. Assis sur l'AAL1, le CES procède par réservation de bande, il n'exploite pas les possibilités d'ATM, et ne permet pas une gestion dynamique de la bande passante. Le CES est comparable au multiplexage temporel.

Le PABX est relié au commutateur *via* une interface E1 en mode structuré (G.703/G.704, lien de *n* fois 64 kbit/s). Dans le réseau, le service est du type circuit virtuel permanent (PVC, *Permanent Virtual Circuit*). Chaque liaison ne nécessite qu'un PVC pour la voix (multiplexage des communications sur le PVC) et un PVC entre chaque PABX raccordé pour la signalisation (maillage complet). Entre le PABX et le commutateur d'accès, la signalisation du PABX peut être transportée dans l'IT16 de l'interface E1 (E1 structuré) ou utiliser un canal dédié (généralement du type X.25 ou simple lien HDLC).

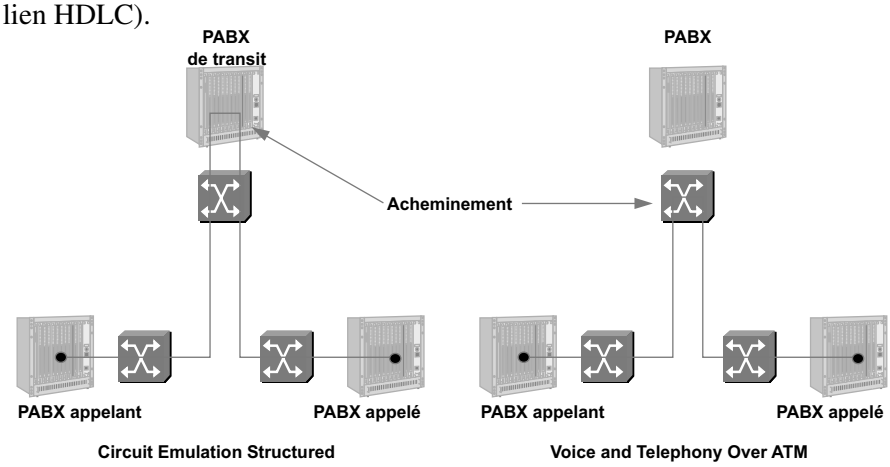


Figure 21.42 La voix dans les réseaux ATM.

Dans le mode **VTOA** (*Voice and Telephony Over ATM*), la signalisation est transportée en mode non transparent. VTOA ne privilégie pas une AAL particulière, seul un service de type VBR-rt (*Variable Bit Rate real time*) est requis. Le lien entre le commutateur de rattachement et le PABX est du type E1 structuré, la signalisation du type canal sémaphore (signalisation dite **CCS**, *Common Channel Signaling*) utilise l'IT16 ou un lien dédié (PVC). Les liaisons voix peuvent utiliser des liens de type **PVC** ou **SVC** (*Switched Virtual Circuit*). La signalisation peut être du type SS7, Q.931, QSIG, DPNSS... Elle est directement interprétée par les commutateurs qui effectuent le routage des communications, un seul lien de signalisation est alors nécessaire.

La figure 21.43 compare succinctement les deux solutions de la voix sur ATM.

Critères	CES	VTOA
Type de service	CBR	VBR-rt
Optimisation de la bande	Transport de nature TDM	Allocation dynamique de la bande
Signalisation	En mode transparent	Interprétation de la signalisation
Routage des communications	PABX de transit	Commutateurs du réseau
Types de liens	PVC uniquement	PVC et SVC

Figure 21.43 La comparaison de VTOA et du CES.

21.6 LA VOIX SUR LE FRAME RELAY

Face aux lenteurs de la normalisation d'ATM et à une relative complexité de l'administration d'un réseau ATM, les réseaux privés Frame Relay se sont rapidement imposés comme l'évolution naturelle des réseaux X.25. Le besoin de rentabiliser les liens a rapidement conduit certains constructeurs à implémenter dans les FRAD (*Frame Relay Access Device*) des fonctionnalités de transfert de voix sur le Frame Relay (**VFRAD**, *Voice FRAD*). La figure 21.44 illustre un réseau voix sur Frame Relay. Le réseau Frame Relay peut être de type privé ou public. Face à ces développements et bien que le Frame Relay ne soit pas prévu pour le transfert des flux isochrones, le Frame Relay Forum a défini le transport de la voix sur Frame Relay dans sa recommandation FRF11 et le transfert de données en présence de voix (trames de données de longueur fixe) dans la FRF12 (segmentation). Ces recommandations définissent les services voix, télécopie, modem analogique, données et le multiplexage de ces différents flux.

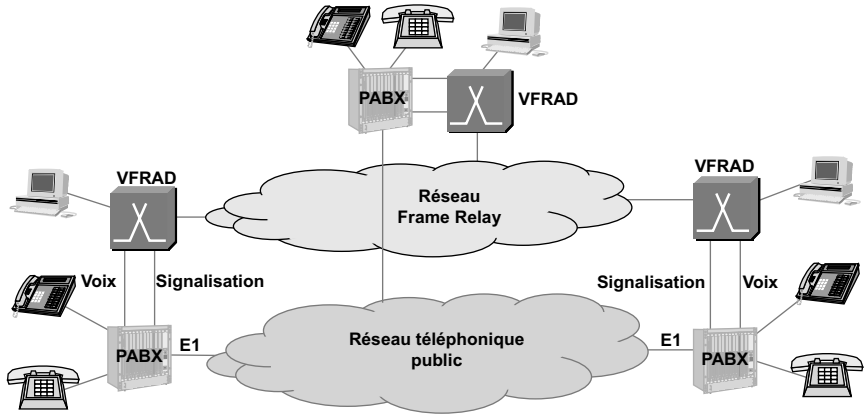


Figure 21.44 L'architecture générale d'un réseau voix/données Frame Relay.

- La recommandation FRF11 (**VoFR**, *Voice over Frame Relay*) spécifie : le multiplexage de canaux voix et données sur le même DLCI (*Data Link Circuit Identifier*). Cette possibilité ne sera utilisée que sur un réseau public tarifé au DLCI. Sur un réseau privé, pour améliorer la qualité de service, on séparera les flux ;
- le multiplexage de plusieurs canaux voix sur le même DLCI (jusqu'à 255) ;
- le regroupement de plusieurs canaux voix dans une seule trame (concaténation) ;
- le support la voix compressée sous différents algorithmes (G.711 ; G.726 à 40, 32 et 16 kbit/s ; G.727, G.728 et G.729) ;
- la signalisation ;
- la gestion des priorités ;
- l'utilisation de connexion Frame Relay à faible débit (classe 2) ou à débit élevé (classe 1). Les algorithmes de compression associés diffèrent selon la classe du réseau.

Pour permettre le multiplexage de plusieurs canaux voix (communications) et de la donnée sur un même DLCI, la FRF11 définit une encapsulation supplémentaire (sous-trame ou *sub-frame*) représentée figure 21.45.

© Dunod – La photocopie non autorisée est un délit

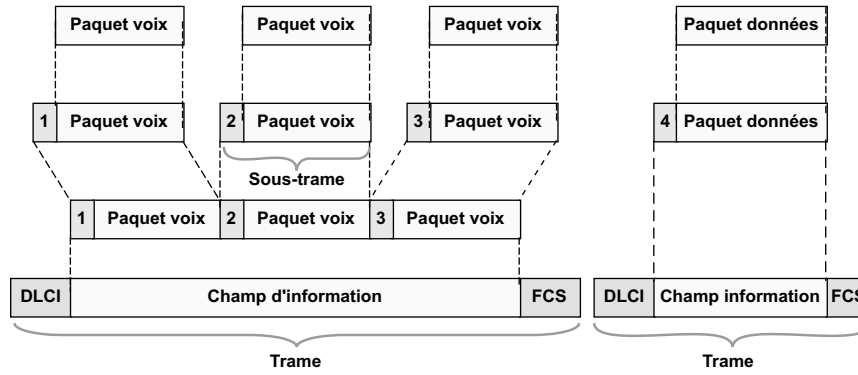


Figure 21.45 Le multiplexage des canaux dans une même trame Frame Relay.

La figure 21.46 présente le format de l'en-tête des sous-trames. L'en-tête a un format variable selon que la sous-trame est seule ou la dernière d'une trame (bit LI = 0).

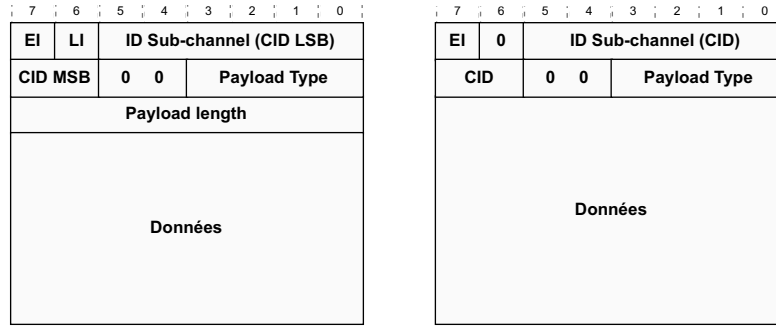


Figure 21.46 La VoFr, en-tête des sous-trames.

Le bit **EI** (*Extended Indicator*) précise la longueur du champ **CID** (*Channel IDentification*), à 0 les canaux sont identifiés sur 6 bits (64 canaux dans un même DLCI) ou 8 bits (255 canaux). Le champ **LI** (*Length Indicator*) indique si le champ Longueur des données (*Payload length*) est présent ou pas. Il est à 0 si la sous-trame est la seule transportée ou est la dernière de la trame. Il est à 1 dans toutes les autres sous-trames. Le champ *Playload type* indique le type de données transportées (voix, données, fax, bits de signalisation CAS). Le bit EI à 0 indique que la charge utile est de la voix codée en EADPCM (G.727) pour les réseaux de classe 1 ou de la voix CS-ACLEP (G.729) pour les réseaux de classe 2. Dans ce dernier cas l'octet *Payload type* n'est pas présent.

La recommandation FRF11 autorise aussi le regroupement ou *Packing factor* de plusieurs paquets voix d'une même communication dans une même sous-trame. Cette pratique améliore le rendement du protocole (réduction de l'*overhead*) mais allonge les délais et rend le transfert plus sensible aux erreurs

Le Frame Relay est une excellente solution au transport de la voix et des données sur des réseaux privés ou publics à faible ou moyen débit. Cependant, l'apparition de la voix sur IP a réduit le Frame Relay à n'être plus que la couche liaison d'un réseau IP transportant la voix sur IP.

21.7 LA VOIX ET TÉLÉPHONIE SUR IP

21.7.1 Généralités

Deux approches de la voix sur IP doivent être distinguées (figure 21.47). La première, à l'instar d'ATM et du Frame Relay, consiste à transporter la voix, issue des systèmes traditionnels (PABX), sur un réseau IP, nous l'appellerons voix sur IP (**VoIP**, *Voice over IP*). La seconde utilise le protocole IP de bout en bout, les téléphones (*IP phone*) sont directement connectés à un LAN IP, c'est la téléphonie sur IP (**ToIP**, *Telephony over IP*).

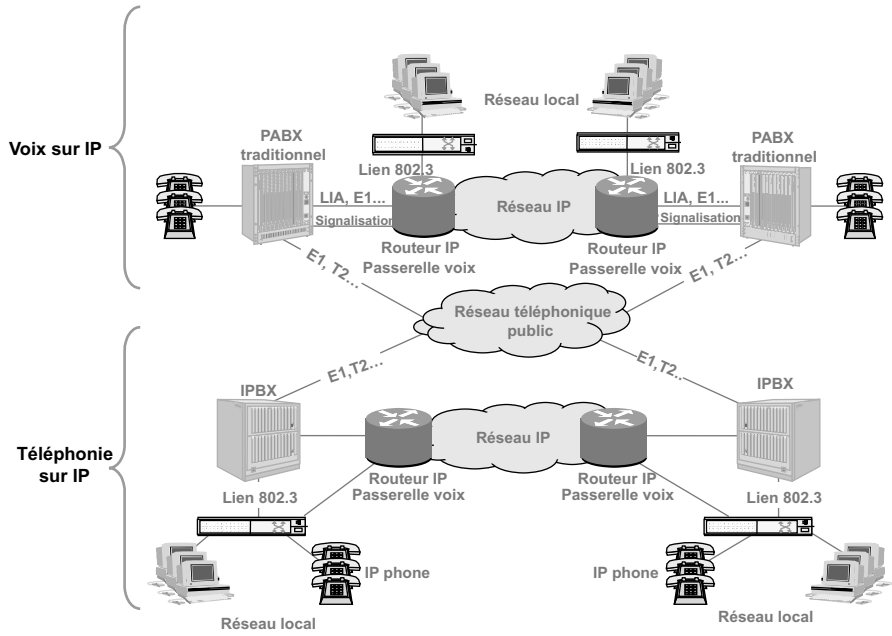


Figure 21.47 La voix et la téléphonie sur IP.

Outre la rationalisation des coûts, la téléphonie sur IP ouvre aux utilisateurs l'accès à de nouveaux services comme la messagerie unifiée, la convergence des annuaires, des services de types multimédia et de *streaming*...

S'appuyant sur une technologie en mode non connecté, la téléphonie sur IP nécessite, pour le transport de données temps réel[9], l'utilisation de protocoles complémentaires afin d'assurer la resynchronisation des paquets, de garantir la priorité des flux multimédia et la gestion de la congestion du réseau. Ces protocoles sont essentiellement :

– **RTP** (*Real Time Protocol*, RFC 1889 et RFC 1890) qui assure l'horodatage (correction de gigue) et le contrôle de séquencement des paquets ;
– **RTCP** (*Real Time Transport Protocol*) qui en particulier, informe les systèmes communicants, sur la qualité de service globale du ou des réseaux traversés ;

9. Il faudrait dire de données isochrones, cependant nous nous conformerons à l'usage et notamment aux RFC qui emploient le terme de temps réel pour ce type de données.

© Dunod – La photocopie non autorisée est un délit

– **RSVP** (*Resource reSerVation Protocol* de l'IETF, Q.397 de l'UIT) qui autorise, pour les flux multimédia, une réservation de ressources réseau de bout en bout. Ce protocole permet la cohabitation de flux multimédia et de flux sporadiques non prioritaires ;
– **MPPP** (*Multilink PPP*, extension de la RFC 1717) qui assure la segmentation des paquets de données longs (*Jumbogram*) en petits paquets et autorise le multiplexage de ces paquets avec des paquets temps réel (*Multilink fragmentation and interleaving*).

Rappelons que la téléphonie doit assurer le transport de deux flux d'information, la voix et la signalisation, l'ensemble s'intégrant, à l'origine, dans un modèle architectural décrit par l'UIT-T et repris par le RFC 2543 : le modèle H.323. Ce modèle permet l'établissement de communications entre terminaux IP/IP (*IP phone*) et des terminaux IP/Traditionnel. H.323 détermine les protocoles de signalisation interne au réseau et assure la conversion de signalisation vers les réseaux publics. Cette architecture est aujourd'hui concurrencée et/ou complétée par deux autres modèles : **SIP** *(Session Initiation Protocol*) d'origine IETF et **MGCP** (*Media Gateway Control Protocol*). D'autres solutions proches ont été proposées. Ces différentes propositions ont conduit à l'élaboration d'un standard commun MEGACO (*MEdia GAteway COntrol protocol*, RFC 3015) pour l'IETF et H.248 pour l'UIT.

21.7.2 TCP/IP et le transport de la voix

Pour des raisons d'efficacité le protocole **UDP** (*User Datagram Protocol*) s'impose pour le transfert des flux multimédia :

– pas d'ouverture, ni de fermeture de session (gain en performance) ;
– pas d'acquittement, ni de reprise sur erreur (sans objet pour un transfert de voix) ;
– pas de contrôle de flux et de congestion (incompatible avec la notion de flux isochrone) ;
– faible temps de latence (contrainte temporelle due à l'interactivité de la voix).

Deux protocoles complémentaires ont été adjoints à UDP, le premier **RTP** (*Real Time Protocol*) a essentiellement pour objet de fournir les informations nécessaires à la correction de gigue et au respect du séquencement. Le second, intégré dans RTP, **RTCP** (*Real Time Control Protocol*) fournit périodiquement des informations sur la qualité de service dans le réseau. La figure 21.48 illustre les différents flux protocolaires.

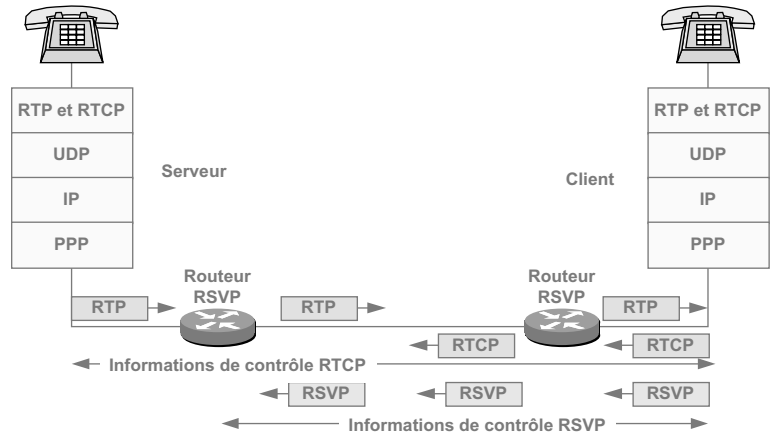


Figure 21.48 Le contrôle de session par RTP et RTCP.

Le protocole RTP

Dans une session multimédia, chaque flux est transporté par une session RTP (ports pairs) distincte. De même, à chaque session RTP est associé un flux de contrôle RTCP (ports impairs immédiatement supérieurs). Une session RTP est une association de plusieurs communicants, au moins 2, elle est identifiée par le couple port/adresse. L'en-tête RTC contient les informations d'identification, de séquencement, de type de charge utile et d'horodatage (figure 21.49).

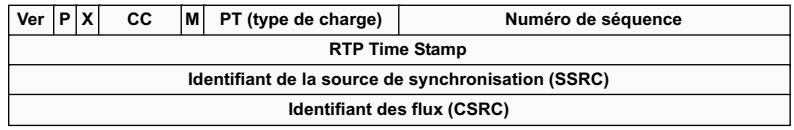


Figure 21.49 L'en-tête RTP.

Sur 2 bits, le champ **Ver** indique la version de RTP (actuellement 2). Le bit **P** (*Padding*) indique s'il y a (1) ou non (0) des octets de bourrage. Le nombre d'octets de bourrage est précisé dans la charge utile. Le champ **X** à 1 indique qu'il y a des extensions d'en-tête. Les 4 bits suivants (**CC**, *CSRC - Contributing SouRCe- Count*) indiquent le nombre d'identificateurs de contributeurs CSCR qui suivent l'en-tête. La signification du bit **M** (*Marker*) dépend du profil de l'application. Par exemple, M=1 dans chaque paquet de parole suivant une période de silence (H.225.0). Le champ **PT** (*Payload Type*) indique le type de charge utile (audio, vidéo...) et le format de codage. La figure 21.50 fournit quelques exemples de valeurs de PT utilisées par H.323 et **SIP** (*Session Initiation Protocol*).

Application	Valeur de PT	Type de codec
Audio	0	PCM, loi m
	4	PCM, loi A
	8	G.723
	9	G.722
	15	G.728
	18	G.729
Vidéo	31	H.261
	34	H.263

Figure 21.50 Les exemples de valeurs du champ PT.

Le numéro de séquence est incrémenté de 1 à chaque paquet. Le champ *Time Stamp* indique sur 32 bits l'instant d'échantillonnage du premier octet du paquet RTP. Le numéro de séquence et le marqueur temporel sont initialisés à des valeurs aléatoires à chaque début de session. Ces informations permettent la récupération de gigue (marqueur temporel), l'insertion dans la file d'attente au bon endroit d'un paquet arrivant hors séquence et la détection de perte de paquets (numéro de séquence). Tout paquet arrivant après le délai de rétention du buffer de gigue ne peut être inséré correctement dans la file, il sera considéré comme un paquet perdu. Le champ *SSRC* (*Synchronisation Source Report Count*), unique au sein d'une session RTP, identifie la source sur laquelle les paquets de données sont synchronisés (marqueur temporel). Le champ **CSRC** (*Contributing Source*) est utilisé quand plusieurs sources fournissent des informations et que le paquet contient des informations reconstituées à partir de ces différentes sources (non utilisé dans H.323 et SIP).

© Dunod – La photocopie non autorisée est un délit

Le protocole RTCP

Le protocole RTCP est essentiellement utilisé pour fournir aux systèmes d'extrémité des informations sur la qualité de service dans le réseau. Il comporte 5 types de messages :

- les rapports d'émetteur (message **SR**, *Sender Report*) utilisés pour fournir des statistiques des participants actifs en émission, ils contiennent des informations sur les flux émis mais aussi sur les flux reçus (figure 21.51) ;
- les rapports de récepteur (message **RR**, *Receiver Report*) qui transmettent les statistiques des récepteurs passifs (en écoute, sans émission de données) ;
- les paquets de description de source (**SDES**, *Source DEScription*) qui fournissent différents paramètres comme le nom canonique de l'émetteur (**CNAME***, Canonical NAME*), le nom au format libre (**NAME**), l'adresse électronique (**EMAIL**), le numéro de téléphone et la localisation de la source.
- les paquets de terminaison de session (**BYE**) ;
- et enfin, les paquets **APP** (Application) dont le format et le contenu dépendent du type d'application.

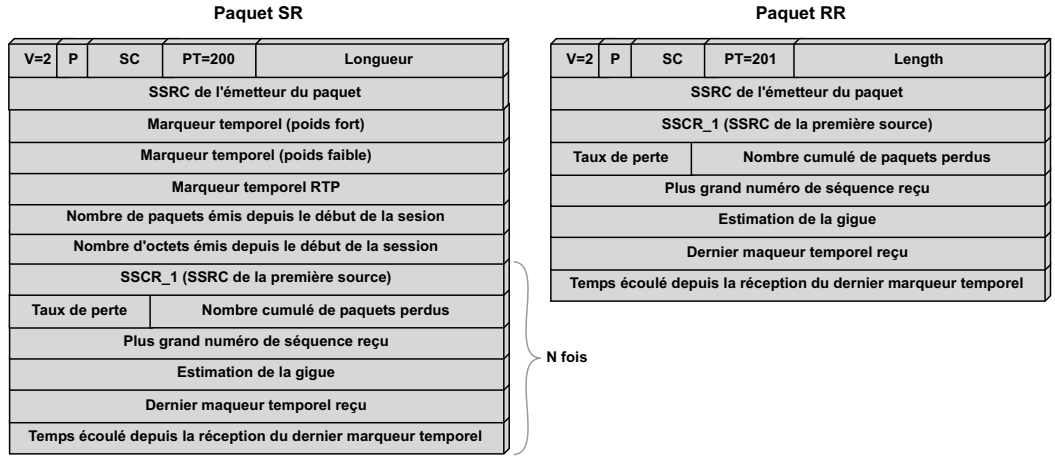


Figure 21.51 Les rapports d'émetteur et de récepteur.

L'encapsulation des données

L'encapsulation IP/UDP/RTP ajoute 40 octets au paquet de données (IP : 20, UDP : 8, RTP : 12), auxquels il faut ajouter l'en-tête de niveau 2. La figure 21.52 indique la bande passante, arrondie au kbit/s le plus proche, requise en fonction du type de protocole de niveau 2.

Le rapport charge utile/données de service est tel qu'un mécanisme de compression d'en-tête (**CRTP**, *Compressed Real Time Transport Protocol*, RFC 1144), basé sur la redondance des informations d'en-tête permettant de réduire d'un facteur d'environ 10 (en-tête de 2 à 4 octets) la taille des données de service (figure 21.53) est apparu indispensable. Par exemple, la compression CRPT associée à la récupération des silences réduit le débit du G.723.1 de 17 à 6 kbit/s (niveau 3). La compression CRTP compresse les données lien par lien, ce qui signifie d'une part, que tous les équipements intermédiaires doivent supporter la compression CRTP et d'autre part, que ce traitement induit un délai supplémentaire d'autant plus important que le nombre de bonds est grand.

Algorithme	Débit Codec (kbit/s)	Charge utile/Nb paquets seconde	Niveau 3	Niveau 2			
			IP/UDP/RTP	Ethernet	PPP	Frame Relay	ATM
Octets overhead			40	26	6	6	5
G.711	64	160/50	80	90	82	82	88
G.711	64	240/33	74	81	76	76	84
G.723.1	6,3	24/33	17	24	18	18	28
G.729	8	20/50	24	34	26	26	42

Figure 21.52 La bande utile après encapsulation.

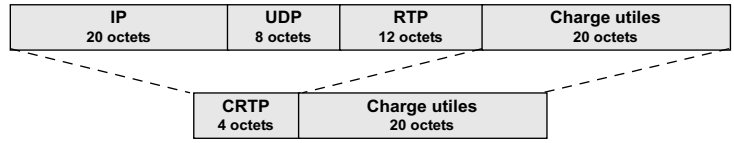


Figure 21.53 La compression d'en-tête CRTP.

Pour limiter la gigue, le protocole **MLPPP** (*MultiLink PPP*, RFC 1990) fragmente les paquets longs. Les petits paquets, notamment ceux de voix, sont encapsulés normalement et entrelacés (multiplexés) avec le flux fragmenté (figure 21.54).

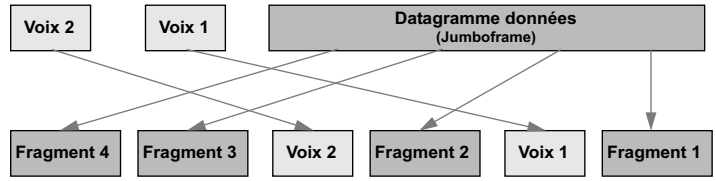


Figure 21.54 L'entrelacement des paquets voix et données (MLPPP).

21.7.3 Les terminaux

Généralités

On distingue deux types de terminaux téléphoniques IP :

– Les « *hardphones* » (*IPPhone* ou *EtherPhone*) correspondent dans l'environnement VoIP au téléphone traditionnel, ils peuvent être dotés d'un mini-écran donnant accès à différents services et en particulier à la messagerie.
– Les « *softphones* » sont constitués d'un ensemble de logiciels émulant, sur un PC traditionnel équipé d'un microphone et d'un écouteur, un terminal téléphonique.

L'accès au service téléphonique s'effectue par une procédure d'authentification, l'utilisateur dispose alors, sur n'importe quel poste téléphonique de l'entreprise, des services téléphoniques qui lui ont été attribués. En particulier, il peut consulter sa messagerie vocale ou texte, les messages textes pouvant être convertis en messages voix par un logiciel dit « *text-to-speech* », son agenda et accéder à tous les services de l'intranet de l'entreprise.

© Dunod – La photocopie non autorisée est un délit

L'alimentation électrique

➤ Généralités

L'alimentation électrique des terminaux IP est l'un des points sensibles du système. Dans les systèmes de téléphonie traditionnels, les terminaux téléphoniques sont télé-alimentés par le PABX secouru par un ensemble de batteries offrant une autonomie généralement supérieure à 24 heures. L'alimentation électrique d'un système de téléphonie sur IP doit donc offrir la même garantie de continuité de service. Or, il ne suffit plus de secourir seulement des terminaux dont la consommation est relativement faible mais aussi les différents éléments actifs de l'ensemble du réseau (*hubs*, commutateurs, service d'annuaire...), ce qui représente un bilan électrique important. Tout projet de téléphonie sur IP devra obligatoirement prendre en considération ce point délicat.

À l'origine, les téléphones IP étaient alimentés directement par le réseau électrique traditionnel. Cette approche constituait un point de vulnérabilité du système : raccordement électrique, transformateur... aussi très vite des techniques de télé-alimentation des postes IP, *via* le câblage réseau (catégorie 5 et au-delà), ont été développées. Aujourd'hui ces techniques font l'objet d'une recommandation de l'IEEE pour les câblages Ethernet 10/100 Mbit/s (**PoE**, *Power over Ethernet* ou IEEE 802.3af). Au-delà de la téléphonie sur IP, la recommandation IEEE 802.3af permet ainsi la télé-alimentation des points d'accès *Wireless* (réseau sans fil).

➤ La télé-alimentation (IEEE 802.3af)

La technologie PoE fournit aux équipements terminaux une puissance électrique maximale de 15 W sous une tension de 48 V continu (CC). Deux modes d'injection sont décrits, l'énergie peut être fournie directement par l'élément actif (commutateur ou *hub*), ce mode est dit *End-Span*) ou par un équipement supplémentaire intermédiaire (mode *Mid-Span*). Cette dernière technique dite par panneaux de brassage utilise un équipement spécifique d'aspect similaire à un commutateur, elle nécessite un double brassage (figure 21.55).

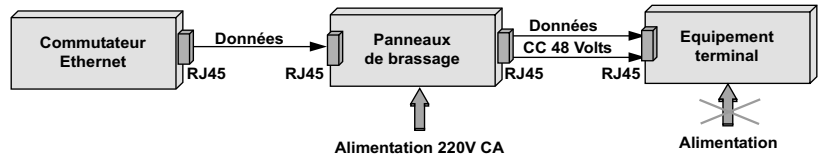


Figure 21.55 L'injection par panneaux de brassage (Mid-Span).

Afin de ne pas endommager l'équipement terminal, le système d'injection (**PSE**, *Power Sourcing Equipment*) doit s'assurer que l'équipement terminal est compatible 802.3af. Les PSE implémentent un système de détection. Ce dernier vérifie que l'équipement terminal peut admettre la télé-alimentation et détermine quelles sont les paires utilisées pour fournir l'énergie électrique.

La télé-alimentation peut être fournie par les paires non utilisées pour la transmission des données (*Spare Pairs*, paires 1 et 4 disponibles) ou sur les paires de données (*Signal Pair*, paires 2 et 3). Ces deux modes sont représentées en figure 21.56.

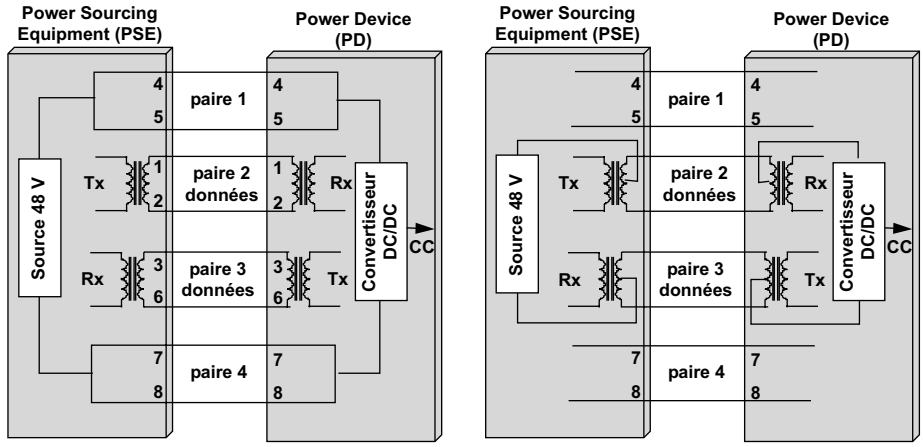


Figure 21.56 Les deux modes de télé-alimentation.

21.7.4 Les architectures et protocoles de signalisation

Généralités

Une architecture voix sur IP, outre les téléphones IP, est organisée autour d'une passerelle voix/vidéo (*Voice/Video Gateway*) et d'un contrôleur de communication (*Call manager*). La passerelle (figure 21.57) réalise l'interconnexion de l'installation voix locale vers les réseaux traditionnels : réseau en mode paquet (WAN IP) et les réseaux en mode circuit (RTC et RNIS).

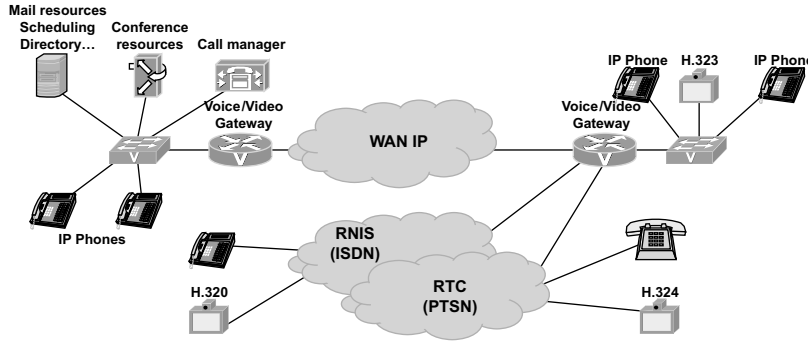


Figure 21.57 L'architecture ToIP de principe.

Elle assure essentiellement les conversions nécessaires de format des flux voix/vidéo et la translation des protocoles de signalisation. Concrètement une passerelle voix peut être un PABX traditionnel auquel on a ajouté une interface IP (VoIP) ou un routeur équipé de cartes voix (ToIP). Le contrôleur de communication réalise le contrôle des appels, la mise en correspondance d'un numéro de téléphone et d'une adresse IP, le routage des appels distants vers la passerelle. Un troisième élément, optionnel, gère l'établissement, le mixage et la diffusion des conférences (*Conference resources*). Ces différentes fonctionnalités peuvent être localisées dans une même entité (IPBX) ou réparties sur plusieurs éléments.

© Dunod – La photocopie non autorisée est un délit

L'architecture H.323 de l'UIT-T

La recommandation H.323 définit un modèle architectural pour assurer le transport de la voix sur un réseau sans qualité de service. L'architecture H.323 comprend diverses fonctionnalités (ou éléments) représentées figure 21.58.

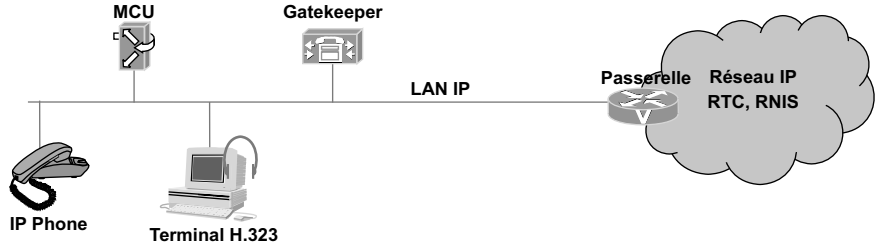


Figure 21.58 L'architecture matérielle d'une zone H.323.

Les terminaux H.323 sont raccordés directement au LAN IP. Ils ont la capacité d'établir des communications voix, vidéo et/ou données en temps réel avec tout terminal de la zone H.323 ou non en mode point à point, multipoint ou diffusion. L'appel est réalisé selon le protocole Q.931 (protocole D du RNIS). Les protocoles mis en œuvre par un terminal H.323 sont :

– H.225 ou **RAS** (*Registration Admission Status*), ce protocole gère l'enregistrement du poste terminal auprès d'une passerelle (*Registration*), réalise une demande de ressource auprès du *gatekeeper* (*Admission* et *Status*). Il est également chargé de la signalisation et de l'établissement d'un appel (sous-ensemble du protocole Q.931 du RNIS) ;
– H.245, ce protocole permet aux terminaux d'échanger leurs capacités audio/vidéo (codecs supportés, nombre de canaux possibles, modes de conférence acceptés...) et de négocier les canaux logiques de dialogue ;
– T.120, ce protocole optionnel gère l'échange de données entre terminaux H.323.

La passerelle H.323 ou *Voice/Video Gateway* assure l'interface avec une entité H.323 et une entité non H.323 comme les réseaux RNIS (H.320) ou ATM (H.321), la conversion de signalisation H.225/Q.931, l'adaptation des supports et des débits. Chaque passerelle H.323 connaît les numéros E.164 (numéros de téléphone) qui lui sont rattachés, elle dispose en mémoire d'une table de correspondance qui associe à un numéro E.164 une adresse IP, un email ou un alias (figure 21.59). Si le réseau est important, la maintenance des tables peut devenir vite impossible. Ce problème trouve sa solution par l'emploi d'un *gatekeeper*[10] qui va centraliser les tables de conversion d'adresses. Chaque *gateway* vient s'enregistrer sur son g*atekeeper* et lui déclare toutes ses adresses E.164. Lorsqu'une passerelle doit établir un appel, elle s'adresse au *gatekeeper* qui lui fournit l'adresse IP de la passerelle destination.

Le portier H.323 ou *gatekepeer*, système optionnel de gestion des communications établies par les entités H.323 fournit les services :

– enregistrement (*Registration*), liste des utilisateurs joignables sur un terminal donné, translation d'adresses (alias, e-mail, E.164...),

10. Littéralement : garde-barrière ; certains utilisent le terme de portier, ce qui est réaliste en terme de fonctionnalités. La plupart des ouvrages en langue française utilise le terme anglo-saxon, nous nous conformerons à cette habitude.

– admission des appels : contrôle des droits des utilisateurs (rejet éventuel d'appel) et gestion de la bande passante,
– translation d'adresses (alias, e-mail, E.164...),
– gestion de la passerelle H.323 (management de la zone),
– journalisation des appels, taxation.

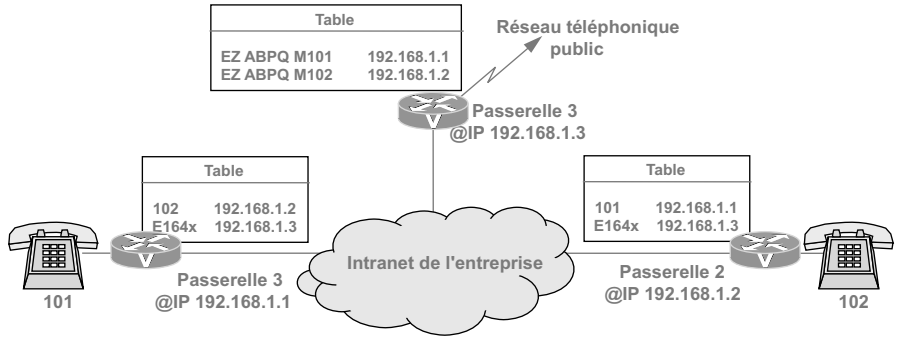


Figure 21.59 La résolution d'adresses par les passerelles.

Enfin, le **MCU** (*Multipoint Control Unit*) équipement optionnel gère l'établissement, le mixage et la diffusion des conférences (contrôle des liaisons multipoints en *multicast*).

La figure 21.60 décrit la pile protocolaire H.323. La voix est transportée en mode datagramme sur UDP tandis que la signalisation est transportée en mode connecté sur TCP (encapsulation **TPKP**, *Transport PacKeT*, RFC 1006). Les spécifications H.323 correspondent aux niveaux session et supérieurs du modèle de référence, cette approche assure l'interopérabilité des systèmes quel que soit le réseau de transport utilisé.

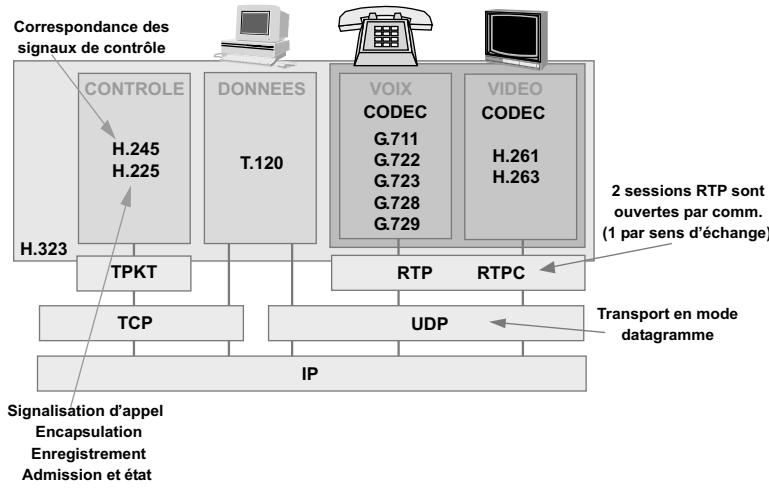


Figure 21.60 La pile protocolaire H323.

© Dunod – La photocopie non autorisée est un délit

La figure 21.61 illustre les relations protocolaires entre un terminal H.323 et un équipement non H.323, dans ce cas de figure la liaison entre le PABX et la passerelle voix est généralement réalisée par des cartes voix présentant une interface de type MIC, E1... Le terminal téléphonique, non H.323, établit un appel en direction du PC multimédia, le routeur (*Gateway* H.323) interprète la numérotation et initialise un appel Q.931 vers l'agent H.323 distant. L'agent H.323 réalise la correspondance entre une adresse E.164 (Q.931) et une adresse IP, il établit un canal de communication entre le demandé et le demandeur.

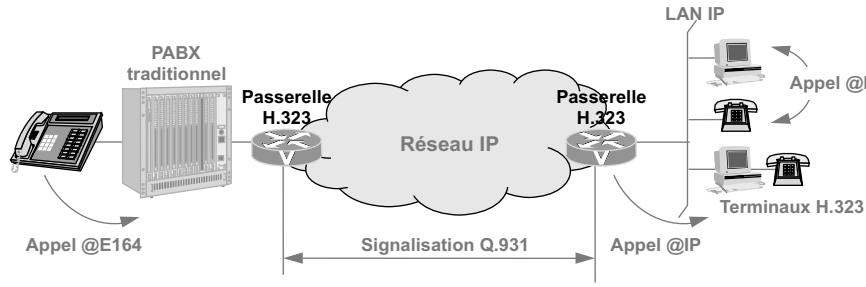


Figure 21.61 La mise en relation selon H.323.

L'établissement d'une communication H.323 diffère selon que le système utilise ou non un *gatekeeper*. En mode direct (sans *gatekeeper*), le terminal qui établit un appel E.164 assure lui-même la traduction d'adresse, la liaison est établie directement par un échange de messages H.225 et H.245 (*Setup*...). En mode *gatekeeper*, le terminal appelant interroge, au préalable (message **RAS**, *Registration, Admission and Status*), le *gatekeeper*[11], pour traduire l'adresse et obtenir l'autorisation d'appeler son correspondant (vérification de la bande passante avant d'accepter un nouveau flux). De même, le correspondant n'accepte l'appel qu'après autorisation de son *gatekeeper*. Le message d'*Admission Request* comporte en particulier l'identifiant de l'appelant, identifiant alloué lors de la phase d'enregistrement par le *gatekeeper*, une référence d'appel, le type d'appel, le type de terminal souhaité, l'identifiant de l'appelé (E.164, alias e-mail...), une estimation de la bande passante nécessaire... En réponse, si l'appel est accepté, le *gatekeeper* fournit l'adresse de transport et le port à utiliser pour joindre le destinataire, la bande passante allouée pour cet appel... La figure 21.62 illustre l'échange de messages H.323.v1.

La mise en relation des correspondants est initialisée par le message *Setup* (H.225, contenant des éléments d'information hérités de Q.931). En particulier le message *Setup* comporte les informations indiquant le type d'appel (vidéo ou voix), l'identifiant appelé appelant, référence d'appel... Ce message adressé au correspondant distant (@IP connue ou en mode *gatekeeper* fournie par ce dernier) au port 1720. Le message *Call Proceding*, acquitte le message *Setup* et indique que l'appel est en cours de traitement. Après autorisation du *gatekeeper*, l'appelant est informé que le terminal appelé sonne (message *Alerting*). Enfin, lorsque l'appelant décroche son combiné, le message *Connect* est envoyé. Ce dernier message fournit à l'appelant l'adresse et le port à utiliser pour la connexion de signalisation (H.245).

11. Un terminal mobile peut obtenir l'adresse IP d'un gatekeeper par un message *multicast* (*Gatekeeper request*) à l'adresse 224.0.1.41:1718 (UDP). Tout terminal H.323 arrivant sur un réseau H.323 doit s'enregistrer auprès d'un *gatekeeper*.

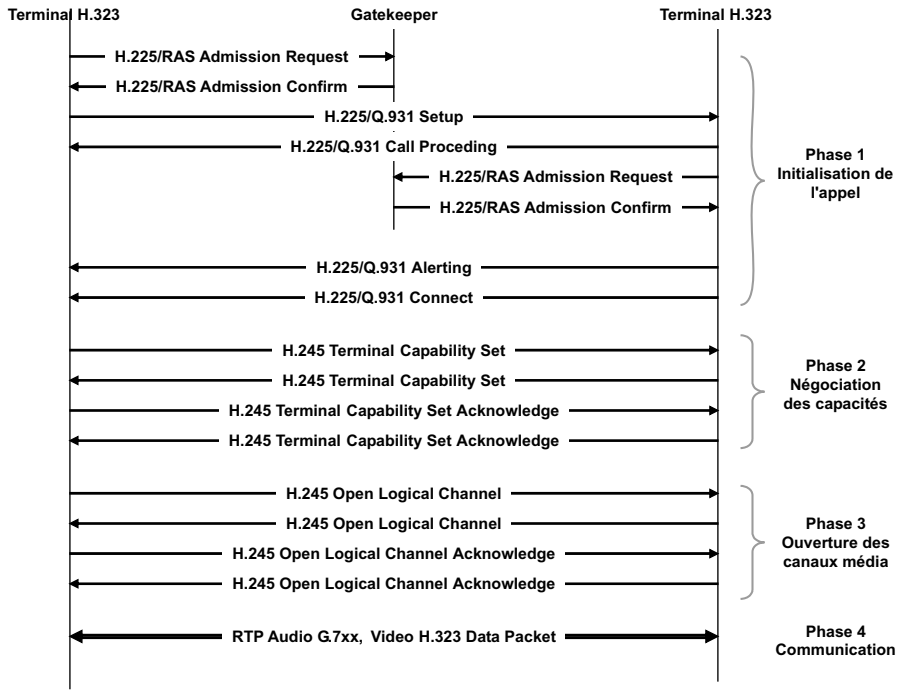


Figure 21.62 L'établissement d'appel sous H.323.v1.

Les deux terminaux entrent alors dans une phase de « négociation » des codecs à utiliser (message *Terminal Capability Set*). Chacun fournit à l'autre une liste ordonnée des codecs dont il dispose (*Capability Descriptors*). Par exemple, si la liste contient : G.723 OU G.729 ET H.261, cela signifie que la source est capable d'utiliser les codecs voix G.723 ou G.729 et d'accepter simultanément une liaison voix et une liaison vidéo codée H.261. Si le terminal peut accepter plusieurs connexions simultanées, il l'indique dans une structure dite *Simultaneous Capabilities*, la liste H.261 ET H.261 ET H.261 indique que le système est capable d'accepter trois connexions simultanées en H.261. L'autre extrémité, en fonction de ses propres capacités, sélectionne le ou les codecs qu'elle utilisera et en informe son correspondant (*Terminal Capability ACK*). L'échange peut ne pas être symétrique, la liaison peut utiliser le codec G.711 dans un sens et G.729 dans l'autre ! Les canaux logiques d'échange d'information dits canaux média peuvent alors être ouverts et la communication débuter.

La libération d'appel suit aussi un scénario symétrique (figure 21.63). Le terminal qui raccroche en premier envoi un message H.245 *Close Logical Channel* (1 message par canal ouvert), ce message est acquitté par le correspondant distant (*Close Logical Channel ACK*). Les deux entités ferment leurs canaux logiques média et signalisation (canal H.245). Lorsque tous les canaux sont fermés, chaque entité confirme la fin de session (*Release Complete*). Enfin, les ressources allouées sont libérées.

Compte tenu de la complexité des échanges, l'établissement d'une communication H.323 peut prendre plusieurs secondes. En introduisant une nouvelle procédure dite *Early* H.245, l'UIT a

© Dunod – La photocopie non autorisée est un délit

allégé ce protocole. Celle-ci permet au message *Setup* de fournir, à l'appelé, l'adresse de transport (@IP:Port) du canal de signalisation et d'établir ainsi immédiatement le canal H.245. Le canal de signalisation ainsi établi permet d'anticiper la négociation des capacités. H.323.v2 a introduit une nouvelle procédure d'établissement de communication dite *Fast Connect.*

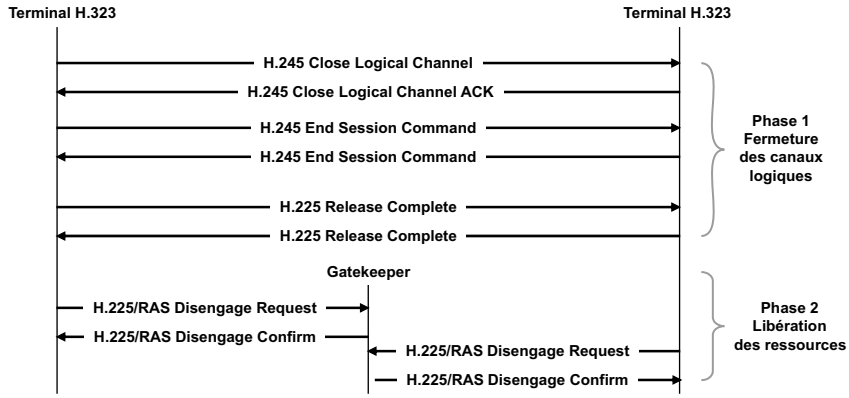


Figure 21.63 La libération d'un appel sous H.323.

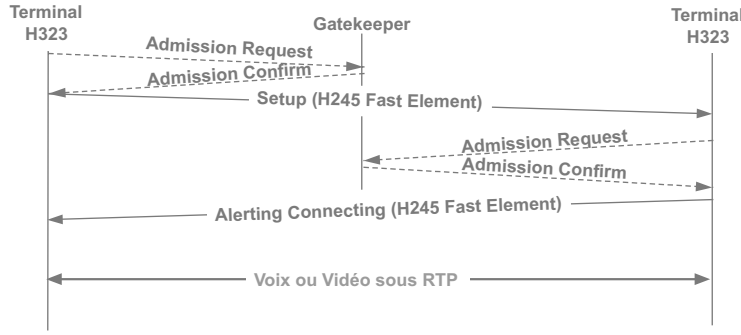


Figure 21.64 L'établissement d'un appel sous H.323v2.

Le message *Fast Connect* modifie les messages de connexion (*Setup*) en y insérant directement ses différentes capacités et en autorisant une ouverture directe des canaux logiques. Le destinataire compare les capacités proposées à ses propres capacités et renvoi un message Q.931 *Connect* définissant les capacités qui seront utilisées durant la connexion, le canal de retour est alors ouvert. La figure 21.65 indique les principales évolutions apportées par les différentes versions d'H.323. Bien que la version courante soit la 5, la plupart des constructeurs n'implémentent que la v2.

Version	Date	Principaux apports
1	Juin 1996	Version de base pour l'établissement et la libération d'appel.
2	Février 1998	Procédure d'établissement d'appel « *Fast Connect* ». Sécurisation des conférences : authentification, intégrité, non-répudiation, confidentialité. Transfert et redirection des appels.
3	Septembre 1999	Restriction de présentation d'identité du correspondant. Mise en attente et indication de mise en attente des appels...
4	Novembre 2000	Possibilité de transmettre les tonalités DTMF avant l'établissement complet de la communication. Possibilité d'utilisation simultanée de la procédure *Early* H.245 et *Fast Connect*. Identification de nom, rappel sur occupation, présentation d'appel sur poste occupé.
5	Juillet 2003	Corrections de quelques problèmes mineurs. Possibilité d'utiliser **SCTP** (*Stream Control Transmission Protocol*) au lieu de TCP pour le transport de la signalisation.

Figure 21.65 Les principales évolutions de H.323.

Le protocole SIP de l'IETF (RFC 3261[12])

Actuellement la plupart des solutions développées utilisent la signalisation H.323 (v1, v2 ou v3) d'origine UIT-T. Développé au sein du groupe de travail **MMUSIC** (*Multiparty Multimedia SessIon Control*) de l'IETF, le protocole **SIP** (*Session Initiation Protocol*), beaucoup plus simple que H.323 pourrait, à terme, remplacer H.323. Inspirés par le protocole HTTP, les messages SIP sont au format texte, ce qui confère au protocole une grande évolutivité. L'architecture est du type client/serveur, un échange forme une transaction, il est composé d'une requête émise par le client et d'une réponse fournie par un serveur. La figure 21.66 illustre l'architecture SIP.

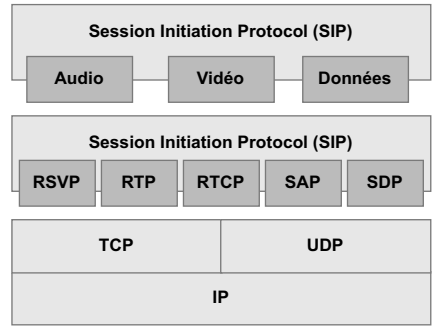


Figure 21.66 L'architecture protocolaire SIP.

À l'instar d'H.323, SIP s'appuie sur les protocoles temps réel (RTP et RTCP), il peut éventuellement utiliser RSVP pour obtenir une certaine qualité de service sur le réseau. Le protocole **SAP**

12. La RFC 3261 remplace la RFC 2543 d'origine, les mécanismes des deux RFC ne sont pas compatibles, sauf l'appel et la libération d'appel.

© Dunod – La photocopie non autorisée est un délit

(Session Announcement Protocol) informe de l'ouverture d'une session multimédia en mode *multicast* ou non et le protocole **SDP** (*Session Description Protocol*) fournit la description des sessions multimédia.

Basé sur le modèle client serveur, SIP distingue deux types d'agent : les clients et les serveurs. Les clients ou **UAC** (*User Agent Client*) sont les équipements à l'origine des appels SIP (téléphone IP) ou des passerelles voix. Les passerelles voix SIP ont les mêmes fonctionnalités que les passerelles H.323.

Les agents serveurs (**UAS**, *User Agent Server*) sont des équipements classiques (Serveur NT...) qui regroupent les services offerts par SIP. Ce sont :

- les serveurs d'enregistrement utilisés pour la localisation des utilisateurs (*Registar*). Les serveurs d'enregistrement contiennent toutes les caractéristiques des agents SIP autres que les passerelles ;
- les serveurs de délégation (*Proxy server*) qui gèrent les clients SIP, reçoivent et transmettent les requêtes au serveur suivant (*Next-hop server*). Le SIP *Proxy* a un rôle similaire au *gatekeeper* d'H.323 (*Call manager* ou contrôleur de communication). Un SIP *Proxy* peut interroger un SIP *Registar* ou un DNS pour acquérir les informations d'acheminement de la signalisation et des communications ;
- les serveurs de redirection (*Redirect server*) qui, sur requête, transmettent l'adresse du *next-hop server* à l'agent client.

Les messages SIP sont de deux types, les requêtes et les réponses. Les primitives de requêtes sont :

- REGISTER, message émis par un agent pour informer un serveur SIP *Registar* de sa localisation. Le client fournit une adresse du type Nom@Domaine ;
- INVITE, message d'ouverture de session, émis par un UAC (*User Agent Client*). Ce message peut être transmis directement à l'agent appelé ou à un serveur *Proxy* pour acheminement ;
- BYE, émis par tout agent client pour mettre fin à une session en cours ;
- CANCEL, annulant une session, ne peut être utilisé que pendant la phase d'ouverture ;
- ACK, qui acquitte un message INVITE et établit la session d'échange ;
- OPTIONS, message d'obtention des capacités (caractéristiques) d'un terminal, similaire à H.245.

Les messages de réponse sont aussi au nombre de six, ce sont :

- INFORMATIONAL, simple message de service ;
- SUCCESSFULL, message indiquant que l'action a été menée à bien (succès)...
- REDIRECTION, message indiquant qu'une autre action doit être conduite pour valider la requête,
- CLIENT FAILURE, message signalant une erreur de syntaxe, la requête ne peut être traitée,
- SERVER FAILURE, message signalant une erreur sur un agent serveur,
- GLOBAL FAILURE, erreur générale, la requête ne peut être traitée par aucun serveur.

Les messages de réponse comportent un code d'état, dont les principaux sont listés dans la figure 21.67.

Type de messages	Code d'état	Appellation	Commentaires éventuels
INFORMATIONAL La requête a été reçue et est en cours de traitement.	100 180 182	*Trying* Ringing Queued	Appel pris en compte Retour de sonnerie Mise en attente
SUCCESSFULL La demande a été reçue et acceptée.	200	OK	Signale que l'appelé a décroché
REDIRECTION Une autre action doit être entreprise pour valider cette requête.	301 302 305 380	*Moved permanently* Moved temporarily Use proxy server	Rediriger l'appel vers cette nouvelle position Rediriger temporairement vers cette adresse Transiter par ce proxy Réservé
CLIENT FAILURE La requête contient une erreur et/ou ne peut être traitée.	400 401 420 483 485	*Bad request* Unauthorised Bad extension Loop Detected Address incomplete	Émis quand un serveur reçoit une requête pour lui-même
SERVER FAILURE La requête, bien que correcte, ne peut être traitée par le serveur.	500 501 502 504	*Internal Server Error* Not Implemented Bad Gateway Gateway timeout	Erreur interne du serveur Non implémenté
GLOBAL FAILURE Cette requête ne peut être traitée par aucun serveur.	600 603 606	*Busy* Decline Not acceptable	Occupé Émis quand l'appelé ne désire pas établir de communication

Figure 21.67 Les codes d'état des messages de réponse SIP.

La figure 21.68 illustre un appel SIP vers un utilisateur qui s'est déplacé. Le client appelant envoie une requête INVITE au serveur proxy auquel il est relié. Ce message contient l'adresse connue du destinataire. Le *proxy server* interroge le *location server* (DNS, LDAP ou autre) qui lui fournit la nouvelle adresse, le *proxy* redirige la requête vers la nouvelle adresse de l'appelé (INVITE). Le poste appelé sonne et le poste appelant reçoit un message de retour de sonnerie (SIP 180). L'appelé décroche signifiant ainsi son acceptation de la communication, le système émet alors un message SIP 200 (OK). L'appelant acquitte le message d'acceptation. Le message BYE acquitté met fin à la communication.

Sans *Server Proxy*, l'appelant se serait adressé à un *redirect server*, celui-ci consulte le *location server* et envoie à l'appelant la nouvelle adresse dans un message **SIP 302** (*Moved temporarily*) ou **SIP 301** (*Moved permanently*). L'appelant émet alors une requête INVITE directement à l'appelé.

Malgré sa simplicité, SIP a du mal à s'imposer devant H.323 plus mature et issu du monde de la téléphonie. La seule supériorité fonctionnelle reconnue, à ce jour à SIP, est l'implémentation de la messagerie instantanée, non prévue par H.323.

Le protocole MGCP/MEGACO-H.248

H.323 et SIP considèrent que chaque élément du réseau, y compris les terminaux, dispose d'une certaine capacité de calcul (intelligence répartie), le protocole **MGCP** (*Media Gateway Control*

© Dunod – La photocopie non autorisée est un délit

Protocol) procède d'une autre approche. Il considère les terminaux comme inintelligent et centralise l'intelligence dans le réseau (protocole à stimulus). Cette seconde approche autorise l'intégration de clients légers et autorise une grande évolutivité des systèmes.

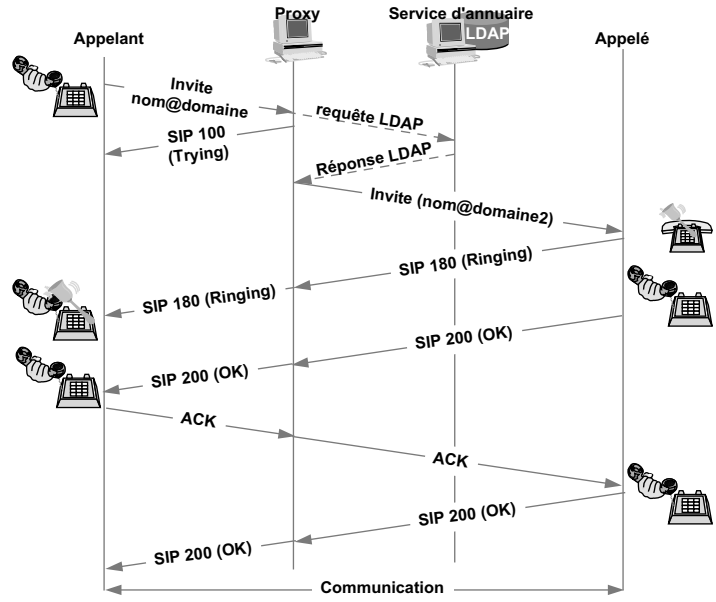


Figure 21.68 L'ouverture d'une communication en mode proxy.

Contrairement aux protocoles à état (H.323, SIP), dans un protocole à stimulus, l'action à entreprendre, en fonction d'un état, n'est pas prédéfinie mais décidée par l'organe de contrôle. Par exemple, dans un terminal téléphonique traditionnel (simple téléphone résidentiel par exemple), le décrochage du combiné est détecté par le commutateur de rattachement et c'est ce dernier qui décide de générer la tonalité d'invitation à numéroter ou d'envoyer un message du style : « vous avez *x* messages dans votre boîte vocale ». De ce fait, MGCP n'est pas en concurrence avec SIP et H.323, il les complète. SIP et H.323 sont des protocoles de cœur de réseau et de périphérie alors que MGCP n'est qu'un protocole de périphérie dont la souplesse permet l'intégration de nombreux périphériques différents (poste téléphonique analogique, modem, passerelle d'interconnexion...) dans un réseau IP.

MGCP définit plusieurs entités. La passerelle de signalisation (**SG**, *Signalling Gateway*) assure la mise en relation de la signalisation du réseau téléphonique traditionnel, généralement SS7, avec la signalisation utilisée dans le réseau en mode paquet. La passerelle média (**MG**, *Media Gateway*) réalise la paquétisation des signaux voix. Enfin, le contrôleur de passerelle média (**MGC**, *Media Gateway Controller* ou **CA**, *Call Agent*), cœur du système, pilote les différentes passerelles. La figure 21.69 illustre l'interconnexion entre un réseau de type RNIS et un réseau IP.

La notion de passerelle voix (**MG**, *Media Gateway*) est très large. Elle recouvre aussi bien la passerelle entre un réseau téléphonique traditionnel (*Trunking gateway*) capable de gérer des milliers de communication, au téléphone IP terminal, en passant par la passerelle résidentielle permettant de connecter un ou plusieurs téléphones analogiques, un modem ADSL offrant ainsi des services d'accès à Internet (figure 21.70).

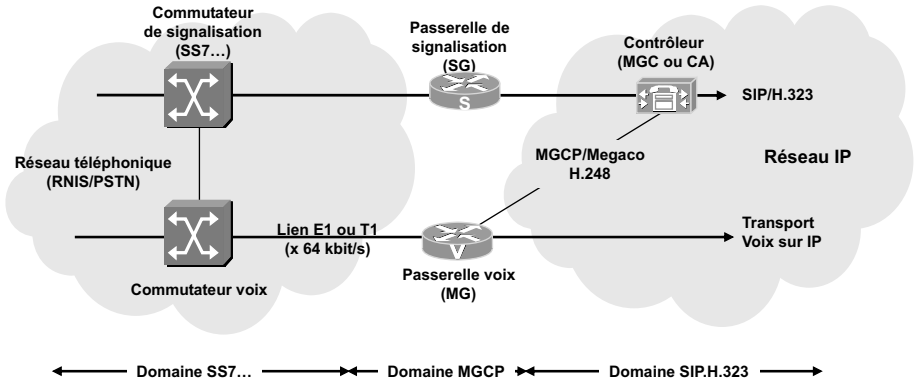


Figure 21.69 L'interconnexion RNIS et la voix sur IP.

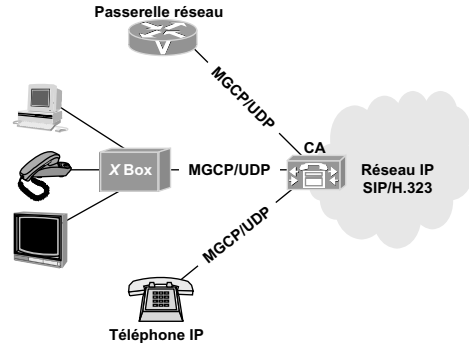


Figure 21.70 Les différentes passerelles MGCP.

Alors que SIP et H.323 utilisent TCP pour le transport de la signalisation, MGCP s'adressant à des terminaux légers se contente d'UDP. Cependant la non-fiabilité d'UDP a conduit à définir un nouveau protocole de transport SCTP (*Stream Control Transmission Protocol*). SCTP garantit une délivrance sans erreur et en séquence. Bien qu'étudié pour le transport de la signalisation téléphonique IP, SCTP peut aussi bien transporter tout autre flux de données et par conséquent pourrait, à terme, remplacer TCP !

21.8 CONCLUSION

La convergence voix/données a donné naissance à une nouvelle génération de réseau dans laquelle la notion de qualité de service devient prépondérante. L'évolution de la téléphonie pour son intégration au réseau données est en plein développement ; déjà plus de 60 % des communications internationales sont établies en voix sur IP. Si la téléphonie sur IP a fait naître l'espoir d'interopérabilité des systèmes, le développement de signalisations propriétaires sur IP, l'opposition H.323 et SIP font reculer cet espoir.

Cependant, le choix se fera autour de H.323 ou de SIP. H.323 bénéficie de son antériorité et d'un fonctionnement assuré, SIP a l'avantage de la simplicité et de l'évolutivité mais il doit encore faire ses preuves.

© Dunod – La photocopie non autorisée est un délit

EXERCICES

Exercice 21.1 Utilisation de l'abaque d'Erlang

Un système à refus dispose de M circuits. Quel est le trafic à soumettre pour un taux de perte 1 %, 10 %, 50 %, lorsque M est respectivement égal à 5, 10 ou 15 ? Déterminez pour chaque valeur, le trafic soumis, écoulé et perdu. (Utilisez l'abaque en annexe.)

Exercice 21.2 Trafic sur un faisceau

Deux systèmes de commutation sont reliés par deux faisceaux de 10 lignes chacun. En supposant un taux de perte de 5 %, complétez la figure 21.71 en indiquant :

1. Quel est le trafic soumis, le trafic réellement écoulé par chaque faisceau ainsi que le rendement par ligne (η) ?
2. Quel est le trafic total soumis par les deux faisceaux ?
3. On regroupe les deux faisceaux en un seul de 20 circuits, en supposant le même taux de perte, quels sont le nouveau trafic soumis, écoulé et le rendement par ligne ?

Faisceaux	Trafic soumis	Trafic écoulé	η par ligne
1 seul de 10 lignes			
2 de 10 lignes			
1 seul de 20 lignes			

Figure 21.71 Calcul du rendement d'un faisceau.

Exercice 21.3 Raccordement d'un PABX

Une entreprise a un parc de téléphones en service de 120 postes dont 100 seulement ont accès à l'extérieur. Sachant qu'un utilisateur normal a un trafic téléphonique de 0,12 E se répartissant comme suit :

- 0,04 E en trafic sortant,
- 0,04 E en trafic entrant,
- 0,04 E en trafic interne à l'entreprise.

Définissez :

1. la capacité de commutation totale, en erlang, du PABX ;
2. le faisceau SPA (appel sortant) sachant que, lorsque le faisceau est occupé, les appelants ont la tonalité d'occupation (le taux d'échec ne doit pas dépasser 10 %) ;
3. le faisceau SPB (appel entrant) sachant que lorsque le poste appelé est occupé, l'appelant entend une musique d'attente (le taux d'échec ne doit pas dépasser 2 %).

Exercice 21.4 Trafic d'un centre d'appel

Un centre d'appel prévoit que, pour une prochaine émission de télévision, il devra accueillir quelque 720 000 appels en 2 heures. Sachant que l'automate de traitement acquiert les données relatives à l'appel en 25 secondes et que le commutateur d'accès met 5 secondes pour prendre en compte une communication, déterminez le nombre de lignes nécessaires et le trafic à écouler en erlang.

Exercice 21.5 Réseau voix/données

Une passerelle voix/données utilise le protocole Frame Relay (FRF11 et FRF12) sur le lien WAN. Sachant que :

- la voix est compressée selon l'algorithme ADPCM à 16 kbit/s,
- le débit du lien WAN est de 64 kbit/s,
- les paquets de voix sont émis avec une périodicité de 20 ms,
- l'encapsulation utilisée FRF11 et FRF12

Déterminez :

1. le nombre de liens voix utilisables sur cette liaison,
2. le débit maximal restant disponible pour les données,
3. la taille maximale des paquets de données en présence de la voix,
4. la gigue maximale introduite par l'insertion d'un paquet de données.

Exercice 21.6 Dimensionnement d'un réseau Frame Relay/voix/données

Un réseau Frame Relay utilise des liens loués à 128 kbit/s. Chaque lien supporte deux canaux voix (ADPCM, 16 kbit/s, fréquence des trames 50 Hz), la signalisation (9,6 kbit/s) et un lien données. Chaque flux utilisera un DLCI différent. Définissez la valeur du CIR et de l'EIR de chacun des DLCI.

Exercice 21.7 Comparaison H.323 et SIP

Complétez la figure 21.72.

Critères	H.323	SIP
Normalisation		
Transport de la signalisation		
Transport des flux multimédia		
Établissement de canaux logiques		
Signalisation *multicast*		
Prioritisation des appels		
Codage des primitives		
Évolutivité		
Détection des boucles		
Gestion des conférences		

Figure 21.72 Comparaison H.323 et SIP.

© Dunod – La photocopie non autorisée est un délit

Partie **V**

Administration et ingénierie

22 Administration des réseaux – Principes généraux 709
22.1 Généralités 709
22.2 L'administration vue par l'ISO 710
22.3 L'administration dans l'environnement TCP/IP 714
22.4 SNMP et ISO 719
22.5 Les plates-formes d'administration 719
22.6 Conclusion 720
EXERCICES 721

23 La sécurité des systèmes d'information 723
23.1 Généralités 723
23.2 La sûreté de fonctionnement 723
23.3 La sécurité 730
23.4 Le commerce électronique 749
23.5 Conclusion 750
EXERCICES 751

24 Notions d'ingénierie des réseaux 755
24.1 Généralités 755
24.2 Les services et la tarification 756
24.3 Les éléments d'architecture réseaux 756
24.4 Le dimensionnement et l'évaluation des performances 760
24.5 Conclusion 768
EXERCICES 769

Chapitre **22**

Administration des réseaux Principes généraux

22.1 GÉNÉRALITÉS

22.1.1 Définition

La stratégie générale d'une entreprise résulte de nombreux facteurs tant internes qu'externes. Mais, indépendamment de la compétence de ses décideurs, la pertinence du système d'information et les moyens d'y accéder sont parmi les éléments majeurs du système décisionnaire.

Dans ces conditions, le système de communication, dont la matérialisation est le réseau de télécommunication de l'entreprise, devient un enjeu stratégique. L'ensemble des moyens mis en œuvre, pour garantir l'efficacité du système et sa disponibilité, pour assurer la surveillance des coûts et la planification des évolutions, constitue l'administration de réseau (*Network Management*).

22.1.2 Principe général

L'administration d'un réseau suppose l'existence d'un système d'information décrivant le réseau de l'entreprise et recensant toutes les données et événements relatifs à chaque constituant du réseau administré (figure 22.1).

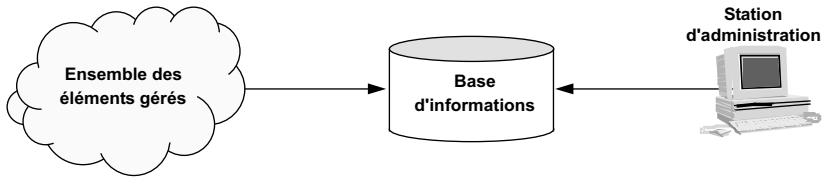


Figure 22.1 Principe général d'un système d'administration réseau.

Le traitement des informations collectées appartient à la sphère de compétence de l'administrateur. L'expérience et l'intuition, qualités essentielles de ce dernier, ne sont pas modélisables, cependant, aujourd'hui, les moteurs d'inférence (intelligence artificielle) constituent une aide non négligeable au diagnostic, à la simulation et à la planification des opérations correctives ou évolutives.

22.1.3 Structure d'un système d'administration

Un réseau comporte un grand nombre de composants (objets) que le système d'administration surveille. Dans chaque objet, un programme en tâche de fond (*Daemon*) transmet régulièrement, ou sur sollicitation, les informations relatives à son état (figure 22.2).

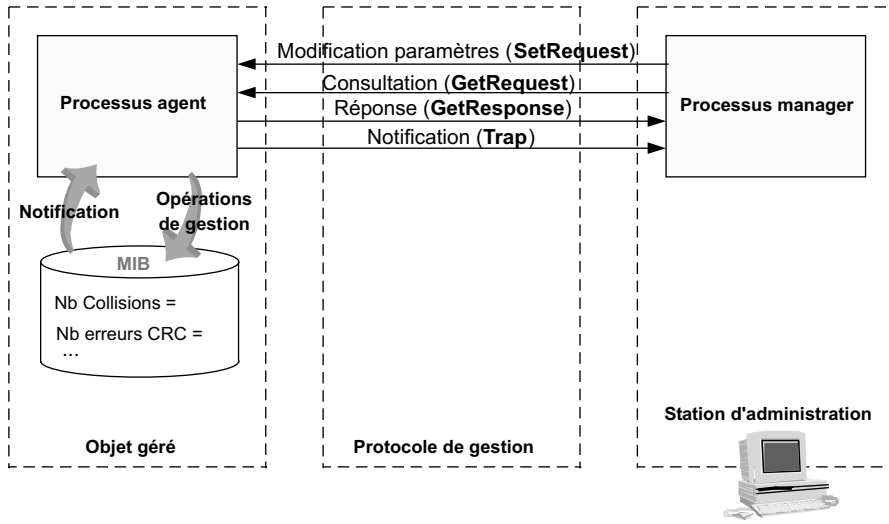


Figure 22.2 La structure fonctionnelle d'un système d'administration.

Les échanges s'effectuent à deux niveaux : entre le composant administré (*Processus agent*) et sa base d'information (**MIB,** *Management Information Base*) d'une part, et d'autre part, entre le composant et le programme d'administration (*Processus manager*).

22.2 L'ADMINISTRATION VUE PAR L'ISO

22.2.1 Généralités

L'ISO ne spécifie aucun système d'administration de réseau, elle définit un cadre architectural général (ISO 7498-4, *OSI Management Framework*) et un aperçu général des opérations de gestion des systèmes (ISO 10040, *OSI System Management*). Ces documents de base décrivent trois modèles :

- un modèle organisationnel ou architectural (**MSA**, *Managed System and Agents*) qui organise la gestion OSI et définit la notion de systèmes gérés et gérants (**DMAP**, *Distributed Management Application Processus*) ;
- le modèle informationnel (**MIB**, *Management Information Base*) qui constitue la base de données des informations de gestion. La MIB énumère les objets gérés et les informations s'y rapportant (attributs) ;
- le modèle fonctionnel (**SMFA**, *Specific Management Function Area*) qui répartit les fonctions d'administration en cinq domaines (aires) fonctionnels (figure 22.3).

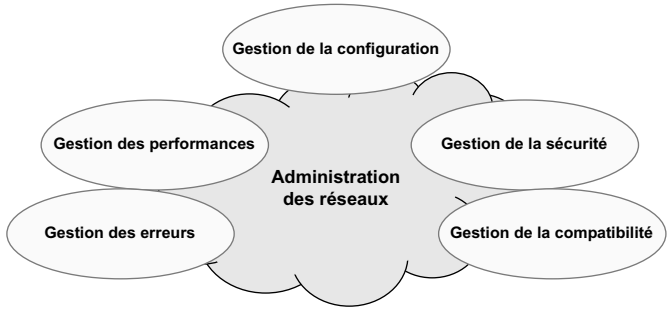


Figure 22.3 Les aires fonctionnelles de la gestion ISO.

22.2.2 Les différents modèles

Le modèle architectural

Le modèle architectural définit trois types d'activité : la gestion du système (*System Management*), la gestion de couche (*Layer management*) et les opérations de couche (*Layer Operation*).

La gestion du système (**SMAE**, *System Management Application Entity*) met en relation deux processus : un **processus gérant** et un **processus agent**. L'agent gère localement un ensemble de ressources locales (équipements, protocoles...) sous le contrôle de l'agent gérant (figure 22.4).

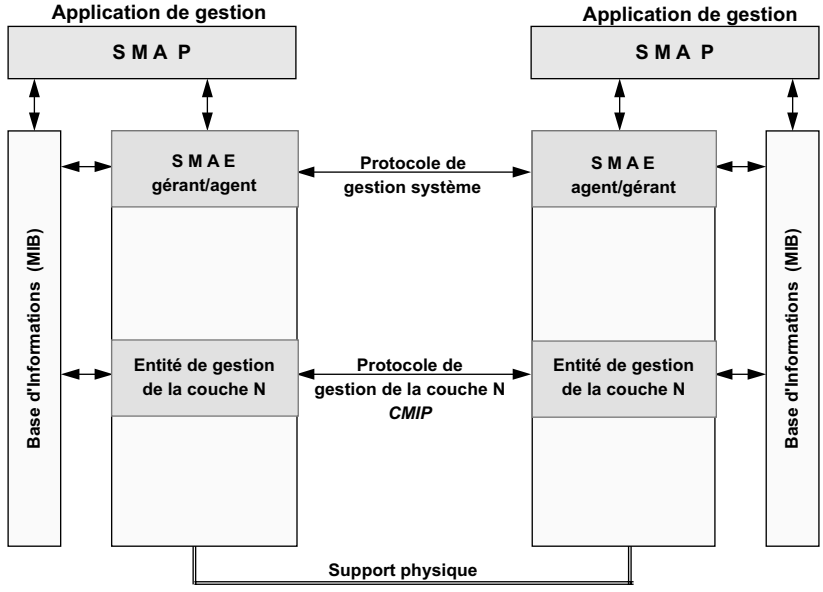


Figure 22.4 Le modèle architectural de l'ISO.

La gestion système repose sur des échanges verticaux entre couches (**CMIS,** *Common Management Information Service*). CMIS (ISO 9595) définit les primitives d'accès aux informations. Ces primitives assurent le transfert d'information vers les applications de gestion (**SMAP**, *System Management Application Process*) non spécifiées par l'ISO.

© Dunod – La photocopie non autorisée est un délit

La gestion de couche, ou protocole de gestion de couche, fournit les moyens de transfert des informations de gestion entre les sites administrés, c'est un dialogue horizontal (**CMIP**, *Common Management Information Protocol*, ISO 9596). Les opérations de couche (*N*), ou protocole de couche (*N*), supervisent une connexion de niveau *N*. Ces opérations utilisent les protocoles OSI classiques pour le transfert d'information.

CMIP utilise les primitives de service suivantes (**CMISE**, *Common Management Information Service Element*) :

- **Get**, cet élément de service est utilisé par le gérant pour lire la valeur d'un attribut ;
- **Set** fixe la valeur d'un attribut ;
- **Event** permet à un agent de signaler un événement ;
- **Create** génère un nouvel objet ;
- **Delete** permet à l'agent de supprimer un objet.

Le modèle informationnel

Le standard OSI décrit une méthode de définition des données d'administration qui modélise la représentation des informations et qui fournit un ensemble de directives pour garantir la cohérence de la base (**SMI**, *Structure of Management Information*).

La représentation des éléments gérés (objets gérés) est orientée objet, les classes et occurrences d'objets sont représentées selon un arbre. Les classes sont rattachées à un arbre dit d'héritage (*Inheritance tree*), les occurrences d'objets à un arbre dit de contenance (*Containment tree*). Un objet est décrit par sa classe d'appartenance, son nom, ses attributs et les types d'opération qu'il supporte.

L'ensemble des objets gérés constitue la MIB (ISO 10165). La MIB contient toutes les informations administratives sur les objets gérés (ponts, routeurs, cartes...). La norme ne spécifie aucune organisation particulière des données. Celles-ci peuvent y être organisées selon une structure en ligne, une base de données... Seul, le *processus agent* a accès à la MIB. Le *processus manager* accède aux données *via* le *processus agent*.

Le modèle fonctionnel

Ce modèle, plus concret que les précédents, définit des domaines fonctionnels d'administration et leurs relations. Cinq domaines ou fonctions (aires fonctionnelles) y sont décrits (**SMFA**, *Specific Management Function Area*).

➤ Gestion des anomalies

La gestion des anomalies (*Fault management*) est une fonction dominante. En effet, l'objectif essentiel d'une administration de réseaux est l'optimisation des ressources et des moyens. Il importe donc d'être en mesure de diagnostiquer rapidement toute défaillance du système, que celle-ci soit d'origine externe (ex. : coupure d'un lien public) ou interne au système (ex. : panne d'un routeur). La gestion des anomalies comporte notamment :

- la surveillance des alarmes (filtre, report...),
- le traitement de celles-ci,
- la localisation et le diagnostic des incidents,
- la mémorisation des anomalies (journalisation),
- la définition des opérations curatives...

➤ Gestion de la comptabilité

La gestion des éléments comptables (*Accounting management*) permet d'évaluer les coûts et de les imputer aux utilisateurs selon l'usage réel des moyens. Ces informations autorisent la répartition des coûts selon les centres de frais de l'entreprise (comptabilité analytique). La comptabilité comporte les tâches suivantes :

– définition des centres de coût,
– mesure des dépenses de structure (coûts fixes) et répartition,
– mesure des consommations par service,
– imputation des coûts.

➤ Gestion de la configuration et des noms

La gestion de la configuration (*Configuration management*) consiste à maintenir un inventaire précis des ressources matérielles (type, équipement...) et logicielles (version, fonctions...) et d'en préciser la localisation géographique. La gestion de la configuration associe, à chaque objet géré (chaque objet de l'inventaire), un nom qui l'identifie de manière unique.

➤ Gestion des performances

La gestion des performances (*Performance management*) met en œuvre les moyens qui permettent d'évaluer le comportement des objets gérés. L'évaluation des performances nécessite la collecte d'information statistique afin de déterminer, en permanence, si le réseau est apte à satisfaire les besoins de communication des utilisateurs. La mesure de la dégradation des performances permet d'anticiper les défaillances et de programmer les évolutions du système. La gestion des performances comprend notamment :

– la collecte d'information (mesure du trafic, temps de réponse, taux d'erreur...),
– le stockage (archivage...),
– l'interprétation des mesures (calcul de charge du système...).

La gestion des performances nécessite de disposer d'outil de modélisation et de simulation pour évaluer l'impact, sur l'ensemble du système, de la modification de l'un de ses paramètres.

➤ Gestion de la sécurité

Afin d'assurer l'intégrité des informations traitées et des objets administrés, la gestion de la sécurité (*Security management*) couvre tous les domaines de la sécurité. L'ISO a défini cinq services de sécurité :

– les contrôles d'accès au réseau,
– la confidentialité qui consiste à s'assurer que les données ne sont communiquées qu'aux personnes, ou processus autorisés,
– l'intégrité qui s'assure que les données n'ont pas été accidentellement ou volontairement modifiées ou détruites,
– l'authentification qui garantit que l'entité participant à la communication est bien celle déclarée,
– le non-désaveu, mécanisme qui interdit, à une entité participant à la communication, de nier d'avoir participé à celle-ci.

© Dunod – La photocopie non autorisée est un délit

Pour cela l'ISO utilise les mécanismes d'encryptage, l'authentification des extrémités (source et destinataire) et le contrôle des accès aux données (voir chapitre 23).

22.3 L'ADMINISTRATION DANS L'ENVIRONNEMENT TCP/IP

22.3.1 Principes généraux

Standard de fait dans l'administration des réseaux TCP/IP, le protocole **SNMP** (*Simple Network Management Protocol*) est proche des concepts ISO. Cependant, non orienté objet, SNMP confond la notion d'attribut et d'objet. Issu du protocole de gestion des passerelles IP (**SGMP**, *Simple Gateway Monitoring Protocol* – RFC 1028), SNMP est décrit dans la RFC 1157. Ce document est complété par de nombreuses RFC dont :

– RFC 1155 qui spécifie comment les objets gérés sont représentés dans les bases d'informations (**SMI**, *Structure of Management Information*). SMI utilise la notation ASN1 (*Abstract Syntax Notation 1*) ;

– les RFC 1156 et 1213 qui définissent les MIB (MIB I et MIB II). Les MIB décrivent les objets gérés (attributs ISO). Une MIB particulière (**RMON MIB**, *Remote Monitor Network MIB*) est spécifiée pour les réseaux locaux (Ethernet et Token Ring), les objets RMON sont implémentés dans des sondes d'analyse et de surveillance. Cependant en environnement commuté, les sondes RMON n'ont accès qu'aux segments sur lesquels elles sont installées. Pour assurer un accès aux différents éléments des réseaux commutés, une sonde spécifique a été définie (RFC 2613, **SMON**, *Switched RMON*).

SNMP spécifie les échanges entre la station d'administration et l'agent. S'appuyant sur UDP (*User Datagram Protocol*), SNMP est en mode non connecté. De ce fait, les alarmes (*Trap*) ne sont pas confirmées. Le choix d'UDP procure une plus grande résistance aux défaillances des réseaux, offre de meilleures performances et permet une implémentation simple, l'entité n'ayant pas à gérer de connexion. La figure 22.5 illustre les échanges SNMP.

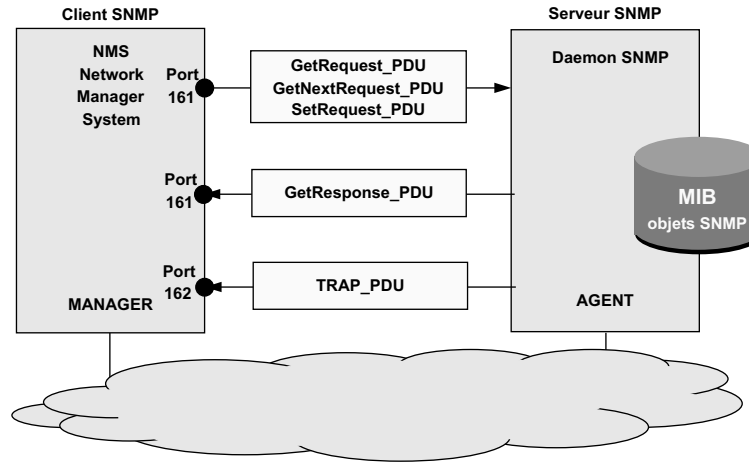


Figure 22.5 Les divers échanges SNMP.

Les messages SNMP permettent de lire la valeur (exemple : compteur de collisions) d'un objet administré (attribut d'ISO) (***GetRequest*** et ***GetNextRequest***), de modifier la valeur d'un objet (***SetRequest***). L'agent administré répond à ces sollicitations par le message ***GetResponse***. Le message ***Trap*** est émis sur l'initiative de l'agent qui notifie ainsi, à l'administrateur, qu'une condition d'alarme a été détectée.

22.3.2 Les MIB

La description des objets

Les MIB décrivent les objets gérés, en définissent le nommage, et en précisent le type, le format et les actions. Les différentes valeurs des objets ne sont pas contenues dans la MIB, mais dans des registres externes que l'agent vient consulter à la demande du manager. La RFC 1213 (MIB II) formalise une structure de définition des objets.

Ainsi, l'objet ***SysUpTime*** qui mesure le temps, en centième de seconde, depuis que l'agent a été réinitialisé, est de type *TimeTicks* (type de variable défini dans la SMI, *TimeTicks* mesure le temps en centièmes de seconde) et est accessible uniquement en lecture (*Read_only*). Cet objet obligatoire (*Mandatory*) est le troisième objet décrit dans la MIB *system*. Sa description est donnée figure 22.6.

```
OBJECT_TYPE MACRO ::=
BEGIN
 TYPE NOTATION ::=
              "SYNTAX" type (TYPE ObjectSyntax)
              "ACCESS" Access
              "STATUS" Status
 VALUE NOTATION ::= value (VALUE ObjectName)
 DESCRIPTION value (description DisplayString) | empty
 Access ::= "read_only" | "write_only" | "not_accessible"
 Status ::= "madatory" | "optional" | "obsolete" | "deprecated"
 DisplayString ::= OCTET STRING SIZE (0..255)
END
```

Description formelle d'un objet

```
SysUpTime OBJECT_TYPE
   Syntax TimeTicks
   Access read_only
   Status mandatory
   Description "The Time (in hundreths of a
   second) since the network management
   portion of a system was last reinitialized"
::= {system 3}
```

Exemple : description de l'objet SysUpTime

Figure 22.6 La description d'objet selon la MIB II.

Le nommage des objets

Les objets (variables) gérés par les MIB sont désignés selon une hiérarchie définie par l'ISO selon un arbre dit **arbre de nommage**. Dans l'arbre de la figure 22.7, chaque organisation de normalisation possède une entrée au premier niveau. Les différentes branches permettent de nommer un objet de manière unique. Les MIB standard établies par l'IETF appartiennent à la branche « Internet » et sont classées dans la sous-branche mgmt(2). Ainsi, l'objet *SysUpTime* de la figure 22.7 est désigné par : *iso.org.dod.internet.mgmt.mib-2.system.sysuptime*

Le même objet peut être décrit par le chemin qui de la racine (Root) mène à l'objet, soit la suite de nombre : **1.3.6.1.2.1.1.3** ou encore plus simplement **mib-2(1.3)**.

La suite d'entiers qui désigne de manière non ambiguë un objet SNMP est l'**OID** de l'objet (*Object IDentifier*).

© Dunod – La photocopie non autorisée est un délit

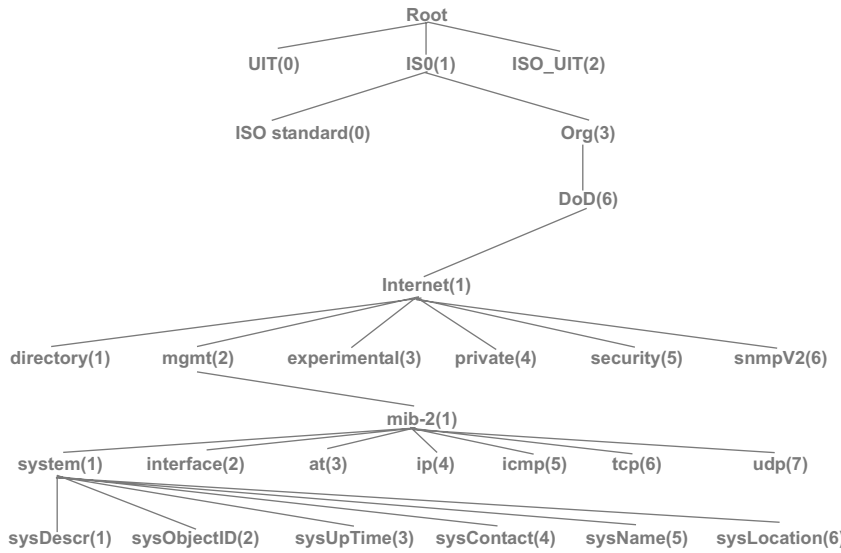


Figure 22.7 L'arbre de nommage des objets SNMP.

Les MIB privées

La MIB I contient 114 objets, la MIB II en définit 170. Malgré l'extension de la RMON MIB, les constructeurs ont constitué des MIB privées. Celles-ci sont développées dans la branche ***private***. Par exemple, la MIB IBM contient quelque 600 objets. La figure 22.8 fournit un exemple d'utilisation de la branche *private*. L'accès aux variables des MIB privées est assuré par un agent spécifique qui effectue les conversions nécessaires : le ***proxy-agent***.

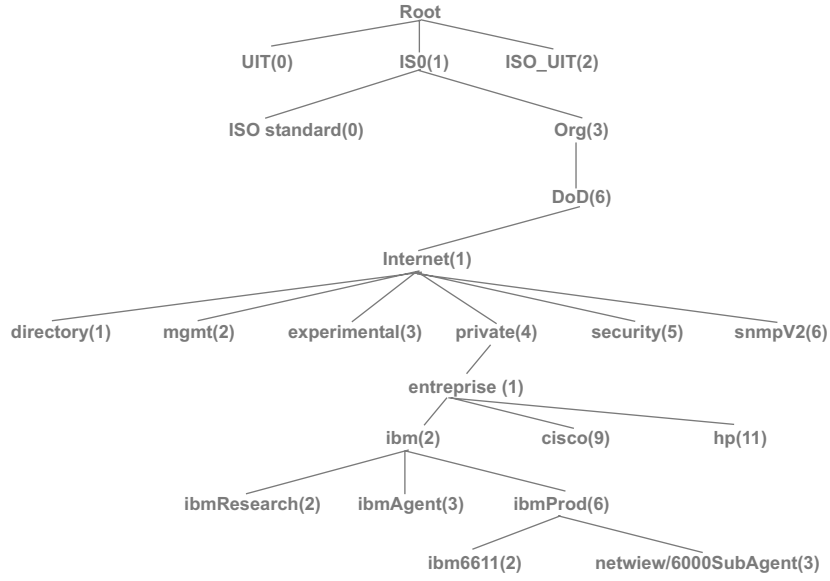


Figure 22.8 L'extrait de la branche private de la MIB IBM.

Le *proxy-agent* permet ainsi le dialogue entre deux systèmes d'administration différents. Le principe du *proxy-agent* est illustré par la figure 22.9. Celui-ci peut être localisé dans le serveur pour l'utilisation d'une MIB privée, ou dans le manager si l'agent serveur n'est pas conforme au standard (conversion de protocole).

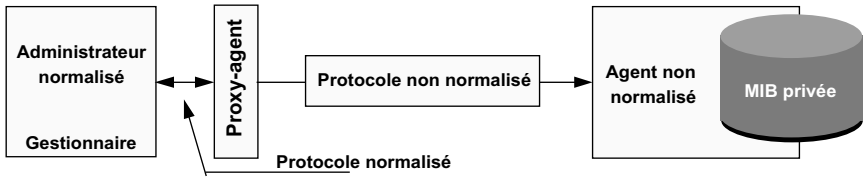


Figure 22.9 Principe d'un proxy-agent (mandataire).

La représentation codée des objets

Les requêtes SNMP identifient l'objet sollicité. Le codage de l'OID (*Objet IDentifier*) suit les règles de codage des données définies par ASN1 : **BER** (*Basic Encoding Rules*) qui code le type, la longueur du champ et la valeur. Les deux premiers bits d'identification d'un objet permettent d'indiquer la nature de l'étiquette (00 universal, 01 application, 10 context, 11 private). Le troisième bit distingue un type primitif (0) d'un type construit (1). Les cinq suivants définissent la variable. SNMP n'utilise qu'un sous-ensemble de désignation des types (figure 22.10).

ID	Types primitifs	Signification
2	INTEGER	Entier de taille arbitraire, utilisable pour définir des types énumérés
4	OCTET STRING	Liste d'octets (valeur 0 à 255)
5	NULL (NIL)	Objet sans type, peut être utilisé pour finir une liste
6	OBJECT IDENTIFIER	Identifie l'objet dans l'arbre de nommage
16	SEQUENCE	Autorise la construction de types complexes (similaire au record du Pascal)

Figure 22.10 Les types « UNIVERSAL » d'ASN1 utilisés par SNMP.

Le codage des deux premiers entiers de l'OID suit des règles particulières. Compte tenu que le premier entier ne peut prendre que les valeurs 1 à 3 et que le second est toujours inférieur à 40, les deux premiers entiers sont codés sur un seul octet : (A $\times$ 40 + B) où A représente le premier octet et B le second. Ainsi, l'objet **SysUpTime** (1.3.6.1.2.1.1.3), précédemment défini, est codé (figure 22.11) :

Type	Longueur	Valeurs
OBJECT IDENTIFIER	6	(1 $\times$ 40 + 3), 6, 1, 2, 1,1, 3
0x06	0x7	0x2B 0x06 0x01 0x02 0x01 0x01 0x03

Figure 22.11 La codification de l'objet SysUpTime.

22.3.3 Le protocole SNMP

Les protocoles SNMPv1 et v2 utilisent le même format de message (figure 22.12). Le champ *version number* vaut 0 (SNMPv1) ou 1 (SNMPv2). Le champ *community string* correspond à un mot

© Dunod – La photocopie non autorisée est un délit

de passe. Transmis en clair sur le réseau, il définit les droits d'un utilisateur sur une branche de la MIB (*MIB views*), ce n'est nullement un élément de sécurité.

Les primitives ***GetRequest***, ***GetResponse***, ***GetNextRequest*** et ***SetRequest*** utilisent la même structure de données.

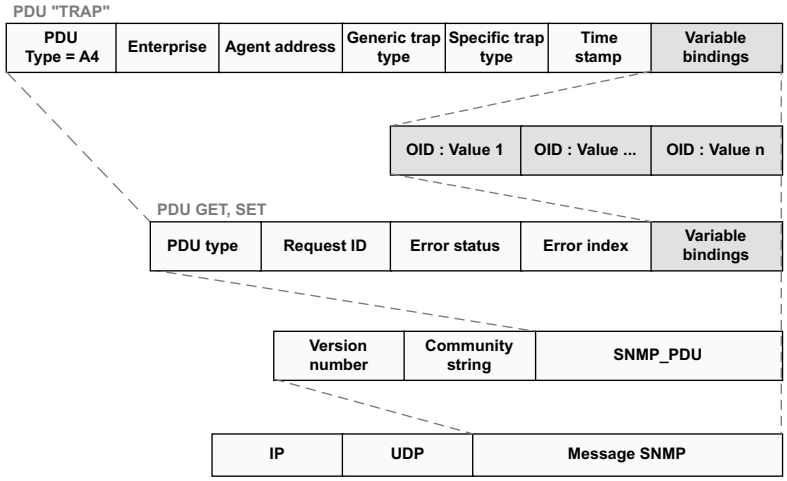


Figure 22.12 Le format des messages SNMP.

Les primitives ***Get***, ***GetNextRequest***, ***GetResponse*** et ***GetBulk*** (SNMPv2) permettent, à l'initiative de la station d'administration, de lire les valeurs des objets de la MIB. La primitive ***GetNext Request*** permet de récupérer les valeurs des objets qui se suivent dans l'ordre lexicographique de l'arbre de nommage. Cette primitive permet de faire des appels récursifs. Cette primitive génère un trafic important, la version 2 a introduit la primitive ***GetBulk*** qui limite le nombre de variables retournées (*Max-repetition*). La primitive ***Set*** permet de fixer une valeur à un objet. Ces primitives sont acquittées par la primitive ***GetResponse***. Sur condition d'alerte, les primitives de type *Event* (***Trap*** et ***Trap-SNMPv2***) sont émises, elles ne sont pas acquittées.

Les apports de SNMPv2 sont essentiellement :

- Un nouveau modèle administratif, l'entité SNMPv2 peut à la fois être *manager* et agent.
- L'introduction de la notion de dialogue de *manager* à *manager* (primitive *Inform*).
- L'amélioration de la modélisation des objets, mais celle-ci reste proche de celle de la v1.
- La définition d'une nouvelle primitive (*GetBulk*).
- L'amélioration des messages de type *Trap (snmpv2_trap).*
- L'introduction de mécanismes de sécurité qui garantissent l'authentification par message digest (MD5), la confidentialité des messages SNMP par cryptographie (DES) et un mécanisme d'antirejeu par synchronisation des horloges, enfin, le support multiprotocole (UDP, OSI...).

La version 3 transpose le modèle client/serveur de la v1 et v2 en un modèle *peer-to-peer*. La différenciation agent/manager est remplacée par celle plus générale d'entité SNMP (*SNMP Entity*). Malgré les apports des versions 2 et 3, notamment en matière de sécurité, la version 1 reste la plus utilisée.

22.4 SNMP ET ISO

Indépendamment de l'aspect orientation objet précédemment abordé, SNMP et ISO diffèrent essentiellement par la méthode de collecte des informations. SNMP travaille dans le mode sollicitation (*polling*) et ne peut interroger qu'un objet SNMP à la fois. Cette contrainte rend le protocole bavard. SNMP est peu adapté à la gestion de vastes réseaux. SNMP v2 pallie ce défaut en implémentant une nouvelle fonction : *Bulk data transfert*, qui autorise l'interrogation et la réponse de plusieurs objets. L'utilisation de *proxy-agents* permet de limiter le dialogue sur le WAN, le dialogue est SNMP entre le *proxy-agent* et l'organe administré, le *proxy-agent* ne transmettant au manager que les alertes.

Outre le faible nombre d'objets gérés, le reproche le plus courant fait à SNMP MIB1 est le manque de sécurité (une table de routage peut circuler en clair sur le réseau). Ces deux aspects sont corrigés par la MIB II, malheureusement moins implémentée.

Le protocole CMIS/CMIP d'ISO est plus adapté aux grands réseaux. Cependant il est très gourmand en ressources et les systèmes administrés n'implémentent que des agents SNMP. Dans ces conditions, un protocole intermédiaire, simplification du protocole CMIP, **CMOT** (*CMIP Over TCP/IP*) a été défini pour utiliser les agents SNMP des réseaux TCP/IP dans les environnements de gestion OSI. À cet effet, une couche spécifique de présentation (**LPP**, *Lightweight Presentation Protocol*) a été définie au-dessus d'UDP, elle sert d'interface entre le monde TCP/IP et le monde OSI

22.5 LES PLATES-FORMES D'ADMINISTRATION

Les outils d'administration se répartissent en trois catégories :

- les systèmes de gestion des couches basses,
- les hyperviseurs donnant une vue d'ensemble du réseau,
- les systèmes d'exploitation avec administration partiellement intégrée.

22.5.1 Les outils d'administration des couches basses

Dans cette catégorie, on trouve les consoles d'administration de câblage et les analyseurs de protocoles. Les gestionnaires de câblage permettent de suivre les évolutions du câblage et le brassage de celui-ci. Compte tenu de la charge de travail imposée par l'acquisition préalable des données et la mise à jour des évolutions, ces outils ne sont justifiés que pour les réseaux importants en nombre de prises.

Les sondes sont des éléments insérés dans un réseau pour en surveiller le fonctionnement. Elles fournissent, en temps réel, toutes les informations utiles au gestionnaire pour connaître l'état actuel de son réseau (taux d'erreur, trafic...).

22.5.2 Les hyperviseurs

Les hyperviseurs sont de véritables plates-formes complètes d'administration de réseau. Ils permettent de superviser le réseau global de l'entreprise. Offrant les services d'une administration propriétaire (ex. : NetView d'IBM pour le réseau SNA) ou ouverte (ex. : OpenView d'HP pour les environnements Unix), les hyperviseurs offrent une vue d'ensemble du réseau (état des liens, des nœuds, d'un port d'un routeur, d'une carte...).

© Dunod – La photocopie non autorisée est un délit

22.5.3 Les systèmes intégrés au système d'exploitation

Les **NOS** (*Network Operating System*) comportent un ensemble d'outils non seulement pour la gestion des utilisateurs, des ressources et de la sécurité, mais aussi de supervision du fonctionnement général du réseau et tout particulièrement de la machine serveur (charge du CPU, *swapping*...).

22.6 CONCLUSION

Dans les réseaux de petites et moyennes importances, l'administration de réseau est souvent perçue comme une tâche superflue, chaque utilisateur pouvant être vu comme une « sonde ». L'ouverture des réseaux et leur nécessaire sécurisation ont fait prendre conscience des enjeux : le concept d'administration est aujourd'hui appréhendé dès la conception des réseaux. Cependant, bien que l'interface commune soit aujourd'hui du type navigateur web (**WBEM**, *Web-Based Enterprise Management*), les solutions propriétaires dominent le marché.

EXERCICES

Exercice 22.1 Analyse de trace SNMP

Un analyseur de protocole a relevé la trace suivante (figure 22.13), il s'agit d'une trame Ethernet, contenant une requête SNMP.

```
Captured at:  +00:03.004
Length: 100    Status: Ok
OFFST DATA                                                    ASCII
0000: 00 A0 24 BD 75 DB 08 00 02 05 2D FE 08 00 45 00  ..$.u.....-...E.
0010: 00 52 3C EF 00 00 1C 06 A4 FF 80 00 64 00 D0 80  .`<.........d...
0020: 08 29 0A CF 00 A1 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D4 00 00 30 28 02 01 00 04 06 70 75 62   .r...0c.....pub
0040: 6C 69 63 A0 1B 02 04 03 05 52 AE 02 01 00 02 01  lic.............
0050: 00 30 0D 30 0B 06 07 2B 06 01 02 01 01 03 05 00  .0.0...+........
0060: 9F 59 6E FC                                      .Yn.
```

Les règles de codage des SNMP_PDU sont données ci-dessous.

```
Message SNMP DEFINITION ::=
BEGIN
 MESSAGE_SEQUENCE ::= SEQUENCE
            { version        Integer        -- Version = 0  pour  MIB 1
              commity        Octet String   -- "Mot de passe" de longueur variable
              data           Any            -- Données du message
            }
 PDUs :: = CHOISE
            { gest_request          GetRequest_PDU,
              gest_next_request     GetNextRequest_PDU,
              get_response          GetResponse_PDU,
              set_request           SetResponse_PDU,
              trap                  Trap_PDU
            }
END

GetRequest_PDU ::= [0] Implicit Sequence
            { request_ID        Request_ID,    -- Identification du couple question/réponse
              error_status      ErrorStatus,   -- Toujours à 0
              error_index       Error_Index,   -- Toujours à 0
             variable_bindlist  VarBindList    -- Liste OID et valeurs dans PDUs réponse
            }
```

Figure 22.13 Le format général des messages SNMP et de la PDU GetRequest.

Décodez cette trame et analysez les champs de la SNMP_PDU transportée.

Exercice 22.2 SNMP et charge du réseau

Si la période de *polling* est fixée à 10 secondes, le débit du lien de 64 kbit/s et la taille moyenne d'un message SNMP de 100 octets, quelle est l'influence de la consultation de 100 objets SNMP à travers un lien WAN ?

Chapitre **23**

La sécurité des systèmes d'information

23.1 GÉNÉRALITÉS

L'ouverture des réseaux vers l'extérieur de l'entreprise et surtout la multiplication des moyens d'accès fragilisent le système d'information. Ce dernier devient alors la cible d'attaques qui visent non seulement à prendre connaissance ou à modifier l'information, mais aussi à paralyser le système. Les moyens mis en œuvre pour le protéger se regroupent sous le vocable de « sécurité des systèmes d'information ». Cependant, il convient de distinguer deux approches de la sécurité :

- la **sûreté de fonctionnement** (*safety*), qui concerne l'ensemble des mesures prises et des moyens utilisés pour se prémunir contre les dysfonctionnements du système ;
- la **sécurité** (*security*), proprement dite, qui regroupe tous les moyens et les mesures prises pour mettre le système d'information à l'abri de toute agression.

23.2 LA SÛRETÉ DE FONCTIONNEMENT

23.2.1 Principes généraux de la sûreté

L'indisponibilité d'un système peut résulter de la défaillance des équipements de traitement (panne), de la perte d'information par dysfonctionnement des mémoires de masse, d'un défaut des équipements réseau, d'une défaillance involontaire (panne) ou volontaire (grève) de la fourniture d'énergie mais aussi d'agressions physiques comme l'incendie et les inondations.

23.2.2 Les systèmes à tolérance de panne

La sécurisation de l'accès aux données

La sécurisation de l'accès aux données représente un enjeu capital pour la validité d'un système d'information. Aussi l'attachement direct (**DAS**, *Direct Attached System*) où chaque disque est physiquement relié à un serveur tend à être remplacé par des systèmes de stockage en réseau.

Deux systèmes s'opposent, le **NAS** (*Network Attached Storage*) et le **SAN** (*Stokage Area Network*). Le premier est un système de mutualisation des ressources disques sur un réseau local de type Ethernet, tandis que le second constitue à lui seul un réseau, généralement de type *fiber channel*, assurant la fiabilisation de l'accès aux données. Notons qu'un NAS peut être partie d'un SAN. Ces deux systèmes qui mettent en œuvre des moyens de sécurisation fondé sur la redondance sont dits à tolérance de panne (*fault tolerant*). La redondance peut être interne à l'équipement (alimentation...) ou externe. Les systèmes à redondance utilisent les techniques de ***mirroring*** et/ou de ***duplexing***.

Le *mirroring* est une technique dans laquelle le système de secours est maintenu en permanence dans le même état que le système actif (miroir). Le *duplexing* consiste à mettre en œuvre un équipement disponible qui prend automatiquement le relais du système défaillant.

Le *mirroring* disques consiste à écrire simultanément les données sur deux disques distincts. En cas de défaillance de l'un, l'autre continue d'assurer les services disques. La panne est transparente pour l'utilisateur. Après remplacement du disque défectueux, le système reconstruit automatiquement le disque miroir (figure 23.1). Évolution du *mirroring*, le *duplexing* consiste à relier chaque disque miroir à un contrôleur disque différent. Il répartit le trafic sur les canaux disques et, par conséquent, améliore les performances. Le *duplexing* protège à la fois contre les défaillances d'un disque et celles du contrôleur.

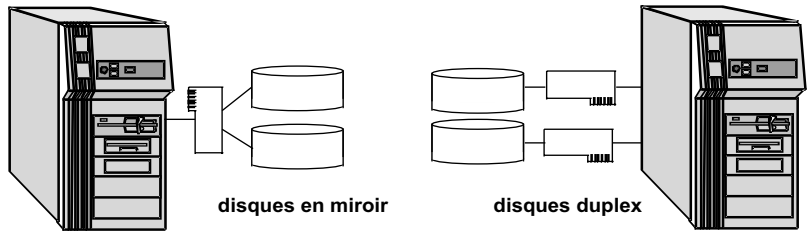


Figure 23.1 Le mirroring et de duplexing de disques.

Pour les mémoires de masse, les stratégies de tolérance de panne (**RAID**[1], *Redundant Array of Independant Disk*) sont classées en six niveaux. En pratique, seuls deux niveaux sont utilisés (niveau 1 et 5). La figure 23.2 présente une synthèse des systèmes RAID.

L'utilisation des systèmes de sécurité du type RAID ne dispense pas de réaliser des sauvegardes régulières, seule solution capable de protéger les données d'un effacement accidentel (erreur d'un utilisateur). Les sauvegardes peuvent être réalisées sur une autre machine du réseau dédiée à cet usage, sur des mémoires de masses distantes ou sur des bandes de sauvegardes conservées dans un autre local.

La mise en duplex d'équipement comme les serveurs représentent le niveau le plus élevé. Chaque serveur (figure 23.3) constitue un sous-système géré par le système d'exploitation. L'utilisateur est

1. Les différentes mises en oeuvres des systèmes RAID ne sont pas obligatoirement compatibles entre elles. Ces divergences d'implémentations peuvent poser de nombreux problèmes lors de la restauration totale d'un système sur celui d'un autre constructeur. Aussi, la **SNIA** (*Storage Networking Industry Association*), qui regroupe 29 sociétés, est en train d'élaborer un nouveau système appelé provisoirement **DDF** (*Common RAID Disk Data Format*), ce format devrait permettre une meilleure interopérabilité entre constructeurs.

Niveau	Description
RAID 0	Le RAID 0 est un système d'agrégats de bandes (*stripping*). Les données sont séparées en blocs répartis selon un ordre prédéterminé entre tous les disques de la grappe. En écrivant les différents blocs simultanément, RAID 0 améliore les performances, mais ce n'est pas un système à tolérance de panne (pas de redondance).
RAID 1	Système de disques miroirs, RAID 1 améliore les performances en lecture (lectures simultanées). Il n'a pas d'incidence sur les performances en écriture (écriture en parallèle).
RAID 2	Correspond à l'exploitation des disques par bandes (RAID 0), avec un code de correction d'erreur (ECC). Un ou plusieurs disques sont dédiés à la sauvegarde des ECC.
RAID 3	Reprend les principes du RAID 2 et ajoute un contrôle de parité.
RAID 4	Similaire au RAID 3 mais les codes de contrôle de parité sont stockés sur un disque particulier.
RAID 5	Semblable au RAID 4 mais les codes de contrôle de parités sont répartis sur tous les disques de la grappe. En cas de défaillance d'un disque, les données de celui-ci sont reconstituées. Il n'y a pas d'interruption de service. Lors du remplacement du disque défaillant, celui-ci est reconstruit automatiquement par le système.

Figure 23.2 La synthèse des systèmes RAID.

connecté à l'un des serveurs. Toutes les opérations effectuées sur l'un sont recopiées, *via* un canal à haut débit, sur l'autre. En cas de défaillance d'un serveur, la connexion de l'utilisateur est basculée sur l'autre. La panne est totalement transparente.

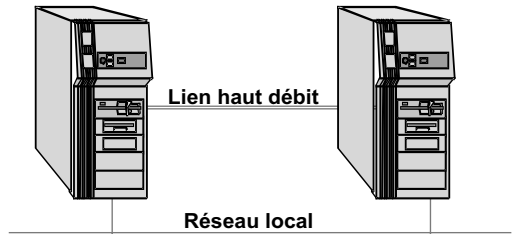


Figure 23.3 Le duplexing de serveurs.

La sécurisation de l'accès au réseau

La sécurité des moyens de transport est généralement réalisée par la redondance des liens obtenue par le maillage du réseau ou par le doublement des raccordements au réseau de l'opérateur. Dans ce dernier cas, il faut veiller à ce que le cheminement des liens, leur point de raccordement au réseau de l'opérateur et les pénétrations dans les locaux informatiques soient distincts. En fonctionnement normal le réseau peut utiliser les deux liens (équilibrage de charge), en cas de rupture d'un lien, le trafic sera intégralement écoulé sur le lien restant (fonctionnement dégradé).

Le protocole **VRRP**[2] (*Virtual Router Redundancy Protocol,* RFC 2338) résout ce problème en permettant à un ensemble de routeurs situés dans un même domaine de diffusion d'être vus par une seule et même adresse IP (@IP virtuelle) et une seule et même adresse MAC (@MAC virtuelle). Un seul routeur est actif à la fois (figure 23.4). Un domaine VRRP comprend :

– un ensemble de routeur identifiés par un même **VRID** (*Virtual Router ID*) ;

2. Pour plus de détail, voir chapitre 13, § 13.4.3.

© Dunod – La photocopie non autorisée est un délit

– un routeur maître, seul actif à un moment donné (*Master virtual router*) ;
– un routeur propriétaire de l'adresse IP du groupe VRRP, le « *Owner virtual router* », c'est sur cette adresse que sont réalisées les opérations de routage, alors que tous les autres routeurs du groupe restent identifiés par une adresse IP propre ;
– un ou plusieurs routeurs « *backup virtual router* » capable de prendre le relais du routeur primaire en cas de défaillance de celui-ci ou de la chute d'un lien de ce dernier.

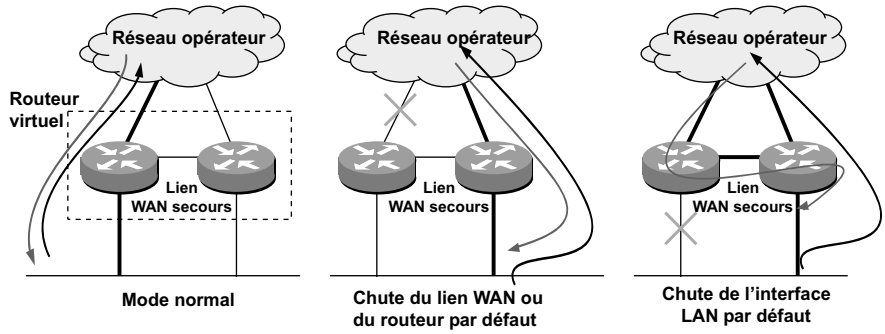


Figure 23.4 Principe du protocole VRRP.

Le protocole VRRP fonctionne en mode Actif/Passif, des implémentations propriétaires autorisent un mode Actif/Actif.

Compte tenu des coûts, de nombreuses petites entreprises préfèrent utiliser une connexion de secours établie à la demande. Dans ce cas, c'est le réseau téléphonique qui est utilisé comme lien de secours. Une communication est établie en agrégeant, selon le besoin, plusieurs canaux B (figure 23.5).

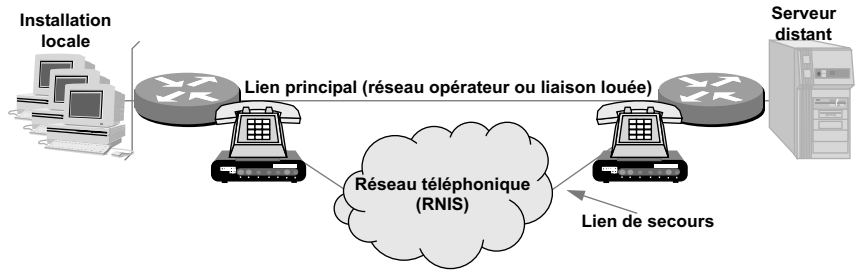


Figure 23.5 La duplication de la ligne de transmission.

23.2.3 La sûreté environnementale

L'indisponibilité des équipements peut résulter de leur défaillance interne mais aussi d'événements d'origine externe. Le réseau électrique est la principale source de perturbation (coupures, microcoupures, parasites, foudre...). Des équipements spécifiques peuvent prendre le relais en cas de

défaillance du réseau (onduleur *off-line*) ou constituer la source d'alimentation électrique permanente du système (onduleur *on-line*). Ces équipements fournissent, à partir de batteries, le courant électrique d'alimentation au système.

Les onduleurs de type *off-line* (figure 23.6) sont surtout destinés à alimenter des systèmes autonomes (protection d'un poste de travail...). En présence du courant secteur, le convertisseur chargeur de batteries maintient la charge de celles-ci. L'équipement est alimenté directement par le réseau électrique. En cas de coupure, le commutateur bascule en quelques millisecondes, et le système est alors alimenté par le convertisseur courant continu/courant alternatif.

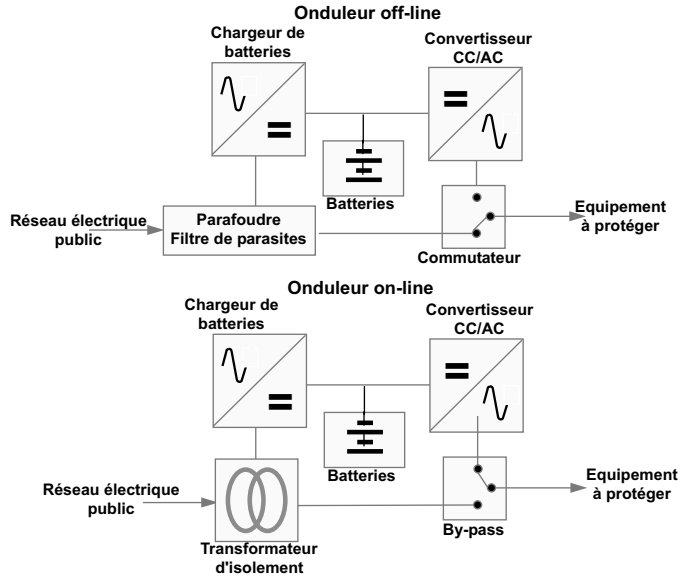


Figure 23.6 Principes des onduleurs.

Les onduleurs *on-line* alimentent en permanence le système externe. Le courant alternatif fourni est parfaitement stabilisé en amplitude et fréquence. Le système est protégé des micro-coupures. En cas de panne de l'onduleur ou d'une surcharge, un commutateur automatique (*by-pass*) bascule le système sur le réseau électrique. Ce mode de sécurisation conduit généralement à réaliser, dans l'entreprise, deux réseaux de distribution courant fort. Le premier relié directement au réseau public fournit l'énergie électrique à l'ensemble des moyens techniques de l'entreprise, le second est dédié aux moyens informatiques.

L'autonomie de tels systèmes est généralement fixée à 20 minutes Pour les systèmes devant assurer un fonctionnement permanent, en cas de défaillance du fournisseur d'énergie, un groupe électrogène se substitue au réseau d'énergie public. Avec l'apparition de la téléphonie sur IP, l'autonomie électrique d'un système d'information devient un point de plus en plus sensible.

La durée de fonctionnement d'un équipement est aussi en relation directe avec les contraintes thermiques qu'il subit, aussi, les locaux informatiques doivent-ils être climatisés (20 à 23 °C). La climatisation doit assurer une ventilation forcée des équipements avec un taux de poussière maximal (200 μg/m^3/24h), maintenir un degré hygrométrique (H) correct (40 % < H < 85 %). La salle doit être protégée contre les agressions extérieures comme les intrusions, mais aussi contre les éléments (inondation et incendie).

© Dunod – La photocopie non autorisée est un délit

En fonction des moyens mis en œuvre et de la fiabilité de chacun des éléments, on peut déterminer la probabilité pour que le système fonctionne correctement pendant un laps de temps donné (disponibilité).

23.2.4 Quantification

Définitions

La **fiabilité** d'un système est la probabilité pour que le système fonctionne correctement pendant une durée donnée dans des conditions définies. La **maintenabilité** d'un système est la probabilité de retour à un bon fonctionnement dans un temps donné. Les différentes pannes pouvant être catalectiques (l'élément fonctionne ou ne fonctionne pas), ou aléatoires (défaillance statistiquement indépendante d'une précédente, la panne d'un élément n'affecte pas les autres). Le comportement d'un système peut être décrit dans le temps comme une suite d'états de bon et de mauvais fonctionnement.

On appelle **MTTR**, (*Mean Time To Repair*, temps moyen de toute réparation), le temps nécessaire à la remise en état du système et **MTBF** (*Mean Time Between Failure,* temps moyen de bon fonctionnement) le temps moyen entre deux pannes successives.

La relation entre disponibilité et MTTR/MTBF

La disponibilité (*Avaibility*) est définie comme étant le rapport :

$$A = \frac{MTBF}{MTBF + MTTR}$$

et l'indisponibilité comme en étant le complément (le matériel est indisponible lorsqu'il n'est plus disponible) :

$$I = 1 - A = \frac{MTTR}{MTBF + MTTR} \quad \text{avec} \quad \frac{I}{A} = \frac{MTTR}{MTBF}$$

Pour rendre un système plus efficace, on peut jouer sur deux valeurs : augmenter la MTBF, les composants réseaux seront alors plus onéreux, ou diminuer les temps d'indisponibilité et c'est la maintenance qui devient plus coûteuse.

Les structures de fiabilité

Selon les relations existantes entre les différents composants du système (figure 23.7), la résistance à la défaillance sera plus ou moins grande. Généralement, on distingue quatre structures de base :

- la structure série sans redondance : dans un tel système lorsque l'un des composants tombe en panne, l'ensemble du système est indisponible ;
- la structure avec duplication de systèmes : dans une telle organisation, la panne d'un seul composant n'affecte pas le fonctionnement global du système ;
- la structure avec duplication de toutes les unités : ici la panne de plusieurs composants ne rend pas le système indisponible ;
- enfin, la structure avec duplication partielle : compte tenu des coûts engendrés par la duplication totale, seuls sont dupliqués dans ce cas les systèmes les plus sensibles.

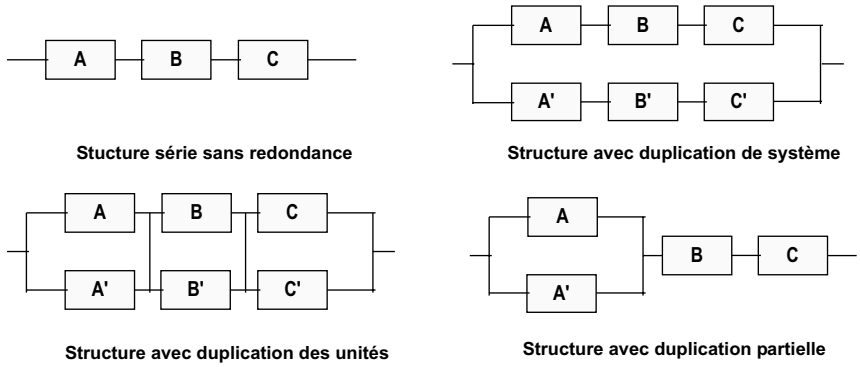


Figure 23.7 Les structures de fiabilité.

La mesure de la disponibilité globale d'un système dépend de sa structure. Deux structures élémentaires sont à la base de tout système : la structure série et la structure parallèle (figure 23.8).

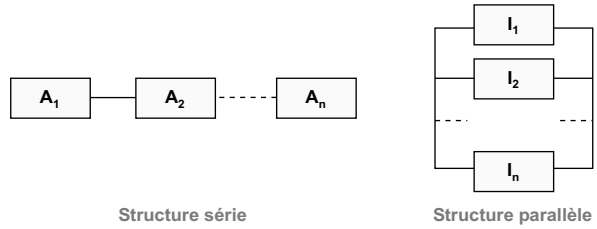


Figure 23.8 Les structures élémentaires.

➤ La structure série

La disponibilité résultante est plus petite que celle du composant le plus faible :

$$A_t = A_1 \cdot A_2 \cdot \ldots \cdot A_n$$

L'indisponibilité est alors :

$$I_t = 1 - A_t = 1 - [(1 - I_1) \times (1 - I_2) \ldots \times (1 - I_n)]$$

Si $A \approx 1$, c'est-à-dire que I est très petit on peut écrire :

$$I_t = \sum_{1}^{n} I_n$$

On montrerait aussi que :

$$MTBF_s = \frac{1}{\sum_{i=1}^{i=n} (1/MTBF_i)}$$

© Dunod – La photocopie non autorisée est un délit

➤ La structure parallèle

L'indisponibilité du système est plus petite que celle du composant qui a la plus faible indisponibilité :

$$I_t = I_1 \cdot I_2 \cdot \ldots \cdot I_n$$

La disponibilité est alors :

$$A_t = 1 - I_t = 1 - [(1 - A_1) \times (1 - A_2) \times \ldots \times (1 - A_n)]$$

De même, on montre que :

$$MTTR_p = \frac{1}{\sum_{i=1}^{i=n} (1/MTTR_i)}$$

23.3 LA SÉCURITÉ

23.3.1 Généralités

L'ouverture des réseaux de l'entreprise au monde extérieur, la décentralisation des traitements et des données ainsi que la multiplication des postes de travail accroissent les risques de dénaturation des systèmes et d'altérations des données. Les menaces peuvent se regrouper en cinq catégories, celles qui visent à :

- prendre connaissance des données sans y être habilité (**confidentialité**),
- altérer les données (**intégrité**),
- mystifier les correspondants par usurpation d'identité (**authentification**),
- nier l'existence d'une transaction (**désaveu** ou répudiation),
- paralyser les systèmes (**déni de service**).

Les mécanismes mis en œuvre pour garantir la confidentialité, l'intégrité, l'authentification, le non-désaveu et la disponibilité du système peuvent se répartir en deux techniques : celles qui tendent à protéger les données et celles qui tendent à protéger les systèmes.

23.3.2 La protection des données

D'une manière générale, la confidentialité est assurée par le chiffrement des messages, l'authentification des correspondants par un échange de mots de passe plus ou moins simple, enfin le non-désaveu est garanti par un système d'accusé de réception ou par l'intervention d'un tiers (le notaire) qui mémorise et authentifie les transactions (notarisation).

Notions de cryptographie

➤ Généralités

Le chiffrement est une technique destinée à rendre les données inintelligibles pour les tiers non autorisés. L'opération de brouillage du texte s'effectue à partir d'une clé (clé de chiffrement). La figure 23.9 illustre une chaîne de cryptage. Le message en clair est codé (chiffré)

à l'aide d'une clé de chiffrement ; seul, le cryptogramme (message chiffré) est transmis sur le réseau. Le destinataire du message effectue le décryptage à l'aide d'une clé de déchiffrement.

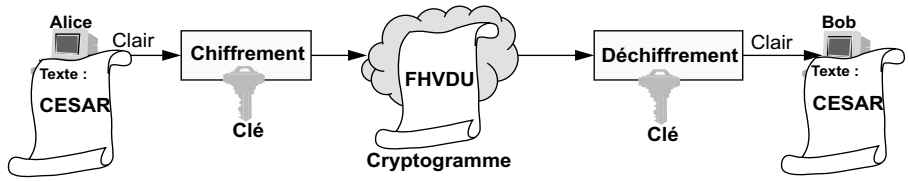


Figure 23.9 Principe de la cryptographie.

Les techniques de cryptographie sont utilisées pour :

– assurer la confidentialité des données (algorithme de chiffrement),
– garantir l'intégrité des données (algorithme de hachage),
– authentifier l'émetteur des données (algorithme de signature numérique).

➤ Les méthodes de chiffrement symétrique

Les systèmes à **clés symétriques** ou secrètes utilisent une clé de chiffrement et une clé de déchiffrement identiques, convenues par avance et conservées secrètes (algorithme à clé secrète). Ils ne permettent pas d'identifier l'interlocuteur distant. Les algorithmes utilisent deux techniques : la substitution et la transposition indépendamment l'une de l'autre ou successivement.

Le code de César, dit aussi code à translation, est le plus vieil algorithme de chiffrement symétrique à substitution connu. Son principe est extrêmement simple, il suffit de substituer à chaque lettre du clair, une lettre de l'alphabet obtenue par simple translation (clé secrète) dans l'alphabet. Par exemple, si la translation est de 3, la lettre A est remplacée par la lettre D, la lettre B par E... La figure 23.10 illustre l'application de ce codage au mot « CESAR », la clé étant fixée à 4. Le clair « CESAR » donne alors pour chiffre le message « FHVDU ».

	A	B	**C**	D	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	**R**	**S**	T	U	V	W	X	Y	Z
C			•	•	•	**F**																				
E					•	•	•	**H**																		
S																			•	•	•	**V**				
A	•	•	•	**D**																						
R																		•	•	•	**U**					

Figure 23.10 Le décalage de César.

Le principe des codes à permutation ou transposition consiste à modifier, selon une loi prédéfinie, l'ordre des caractères. Les méthodes de pliage constituent un exemple simple des codes à transposition. Ils consistent à écrire le message d'origine (clair) dans une matrice comportant autant de colonnes que la clé de caractères. Le cryptogramme est obtenu en écrivant, en ligne, le clair dans la matrice puis en lisant cette matrice en colonnes dans l'ordre défini

© Dunod – La photocopie non autorisée est un délit

par la clé. Soit, par exemple, le message « UNE PLANCHE A VOILE » et la clé de codage 4312 :

– La clé a une longueur de 4, on crée une matrice de quatre colonnes puis on inscrit le message horizontalement (sans les blancs). Enfin, on lit la matrice verticalement dans l'ordre de la clé (figure 23.11). On obtient le message :

PCVE ENAL ULHO NAEI

– À l'inverse, pour déchiffrer un message, il suffit de l'écrire verticalement dans l'ordre de la clé et de lire horizontalement.

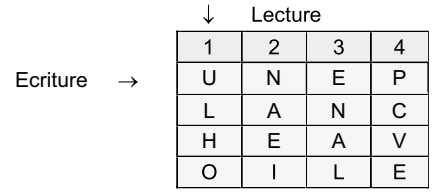


Figure 23.11 La matrice de chiffrement et de décryptage.

Le **DES** (*Data Encryption Standard*) d'origine IBM (Karl Meyer 1977) est l'algorithme à clé symétrique le plus connu. Il consiste en une suite de substitutions (DES-S) et de transpositions, ou permutations (DES-P), par bloc de 64 bits. La figure 23.12 illustre de manière simple le principe d'un tel code. Utilisant une clé de 56 bits (64 bits dont 8 de parité), le DES est aujourd'hui facilement « cassable », il est remplacé par le triple DES (3DES, application de trois DES successivement avec trois clés indépendantes).

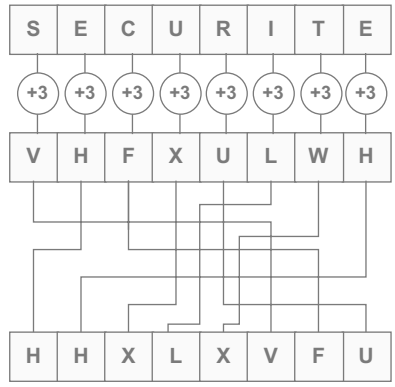


Figure 23.12 Principe du DES.

Les algorithmes de cryptographie à clé secrète demandent relativement peu de puissance, le temps de calcul est compatible avec un échange interactif de messages. Cependant, la découverte de la clé secrète donne accès à l'information. Dans de tels algorithmes, le secret (la clé) doit être transmis d'où les risques d'interception ou alors préalablement connu des deux correspondants et dans ce cas c'est un de trop !

➤ Les méthodes de chiffrement asymétrique

Évitant la diffusion de clés, les systèmes à **clés asymétriques** utilisent deux clés, l'une est connue de tous (**clé publique**), l'autre n'est connue que de l'un des correspondants (**clé secrète**). Le message chiffré avec l'une ne peut être déchiffré qu'avec l'autre. Les deux clés sont reliées mathématiquement entre elles, mais l'utilisation de grands nombres rend ce lien pratiquement impossible à retrouver. La figure 23.13 illustre ce mécanisme.



Figure 23.13 Principe de la cryptographie à clé publique.

Le système de cryptographie à clé asymétrique le plus répandu, le **RSA** du nom de ses inventeurs (*Rivest, Shamir et Adleman*) repose sur l'arithmétique des grands nombres. La fonction de chiffrement est de la forme :

$$\text{Crypte} = [\text{Clair}^{\text{clé C}} \text{ modulo } n]$$

où Crypte est le message codé,
Clair, le message à coder,
clé C, la clé de chiffrement,
n, un produit de nombres premiers.

La fonction de déchiffrement est identique :

$$\text{Clair} = [\text{Crypte}^{\text{clé D}} \text{ modulo } n]$$

La figure 23.14 illustre le chiffrement et déchiffrement pour un système dont les paramètres seraient C = 3, D = 7 et n = 33.

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	27	10 460 353 203	3
4	64	31	27 512 614 111	4
5	125	26	8 031 810 176	5

Figure 23.14 L'exemple de chiffrement et de déchiffrement à clé asymétrique.

Fondés sur la difficulté de factoriser des nombres premiers, les systèmes à clé publique permettent d'assurer la confidentialité des données mais, aussi d'authentifier l'émetteur d'un message.

➤ L'authentification de l'émetteur

Un message chiffré avec la clé publique n'est déchiffrable qu'à l'aide de la clé privée, cela assure la confidentialité mais ne permet pas d'authentifier l'auteur du message. L'authentification de l'émetteur peut être obtenue en chiffrant le message avec la clé secrète et en le déchiffrant avec la clé publique (figure 23.15).

© Dunod – La photocopie non autorisée est un délit



Figure 23.15 Principe de l'authentification de l'émetteur.

Si Alice, à l'aide de la clé publique de Bob, déchiffre le message, c'est que celui-ci a bien été codé à l'aide de la clé privée de Bob, donc Bob est bien l'émetteur du message. Ce procédé ne garantit pas la confidentialité des messages, tout possesseur de la clé publique peut déchiffrer le message, il ne garantit que l'origine (le détenteur de la clé privée), c'est un système de signature de messages.

➤ Le protocole d'échange de clés Diffie-Hellman

La cryptographie à clé publique nécessite une puissance de calcul importante. Le DES est entre 100 fois (implémentation logicielle) et 1 000 fois (implémentation *hardware*) plus rapide que le RSA. Le protocole d'échange de clés de Diffie-Hellman permet de construire une clé secrète (clé de session) sans que celle-ci circule sur le réseau. L'initiateur de l'échange transmet à son correspondant deux nombres grands et premiers (g, n). Les correspondants déterminent une clé privée, tenue secrète. Chacun, à partir de g, n et de sa clé secrète (nombres aléatoires A et B), génère une clé publique et la communique à l'autre. Puis, à partir de sa clé privée, de sa clé publique et de la clé publique de son correspondant, on calcule la clé de session (figure 23.16).

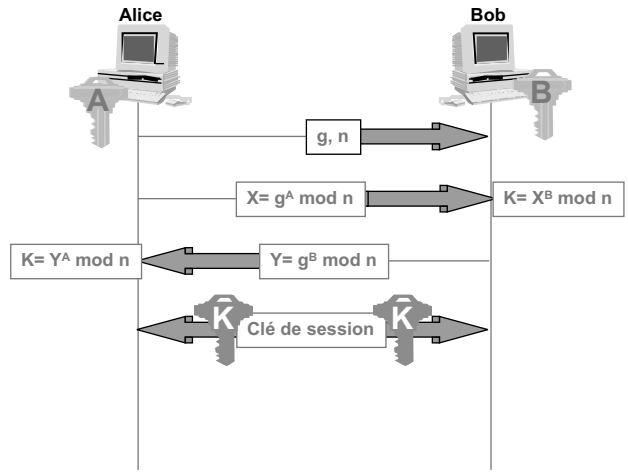


Figure 23.16 Principe de l'échange de Diffie-Hellman.

Le protocole de Diffie-Hellman permet de sécuriser l'échange de clé, cette technique est utilisée dans IPSec (*IP Secure*)

➤ Contrôle d'intégrité du message

Pour vérifier l'intégrité d'un message, on utilise une technique similaire à celle du CRC (*Cyclic Redundancy Check*). Une fonction dite de hachage (***hash***) est appliquée au contenu du message. Le

résultat obtenu ou ***digest*** (résumé, sceau...) est joint au message à transmettre, il est recalculé par le destinataire. Si le résultat du calcul local est identique au *digest* reçu, le message n'a pas été altéré (figure 23.17).

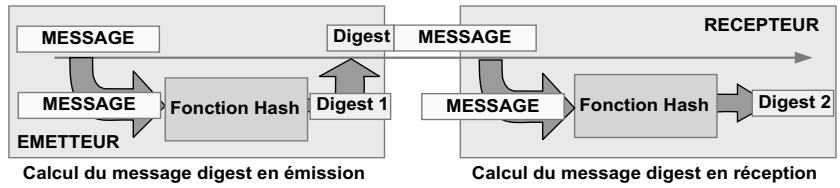


Figure 23.17 Principe de détermination du « digest ».

La fonction de hachage doit garantir qu'il est impossible à partir du *digest* de retrouver le message initial (non-retour arrière ou *one-way hash*) et qu'il doit être quasi impossible que deux messages différents donnent le même *digest* (résistance à la collision). Le *digest* a une longueur de 128 bits (MD2 à MD5, *Message Digest X*, défini par Ron Rivest et normalisé par la RFC 1321) ou de 160 bits (SHA-1, *Secure Hash Algorithm*).

➤ La signature numérique d'un message

En combinant un système de cryptographie et une fonction de hachage, on peut à la fois garantir l'intégrité du message et son authentification (**MAC**, *Message Authentification Code*). Selon que l'on utilise un système de cryptographie à clé secrète ou publique, on obtient une signature numérique dite symétrique ou asymétrique.

Dans le système à signature symétrique, l'émetteur calcule le digest sur la concaténation de la clé secrète et du message (figure 23.18). Le destinataire procède de même, si le digest trouvé est identique a celui qui a été reçu, c'est d'une part que le message n'a pas été altéré et d'autre part qu'il a bien été émis par l'autre possesseur de la clé partagée.

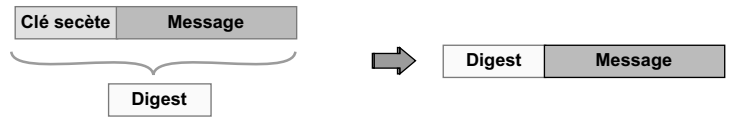


Figure 23.18 Le calcul d'une signature numérique symétrique.

Dans le système à signature asymétrique, le *digest* est calculé sur le message puis chiffré à l'aide de la clé privée de l'émetteur, le résultat est joint au message envoyé (figure 23.19). Le destinataire calcule le *digest* sur le message, déchiffre le *digest* reçu à l'aide de la clé publique de l'émetteur. Si les résultats sont identiques, le message n'a pas été altéré et l'émetteur est identifié, c'est le possesseur de la clé publique.

© Dunod – La photocopie non autorisée est un délit



Figure 23.19 Le calcul d'une signature numérique asymétrique.

Les systèmes à signature numérique permettent d'assurer l'authentification (qui est l'émetteur du message) et l'intégrité de celui-ci (le message n'a pas été modifié par un tiers). N'ayant besoin d'aucun secret partagé, l'authentification par signature numérique asymétrique est plus efficace. Cependant, elle nécessite une puissance de calcul supérieure et ralentit les échanges de messages. Le protocole IPSec utilise les deux systèmes, les correspondants s'authentifient d'abord par signature numérique asymétrique, puis les échanges suivants sont authentifiés par signature symétrique.

La sécurisation des échanges

➤ L'usurpation d'identité

L'un des problèmes de la cryptographie à clé publique est la possible intervention d'une tierce personne (figure 23.20). Lorsqu'Alice veut entrer en relation avec Bob en utilisant un système de cryptographie à clé publique, elle doit demander à Bob sa clé publique. Cet échange peut être intercepté par Charlie, un intrus malveillant, qui peut répondre en lieu et place de Bob avec sa propre clé publique. De cette manière, Charlie pourra se substituer à Bob lors des prochains échanges, Alice étant persuadée que les messages lui proviennent bien de Bob. La même opération est réalisée lorsqu'Alice envoie sa clé publique à Bob. Cette attaque est connue sous le nom de « *Man in the middle* ».

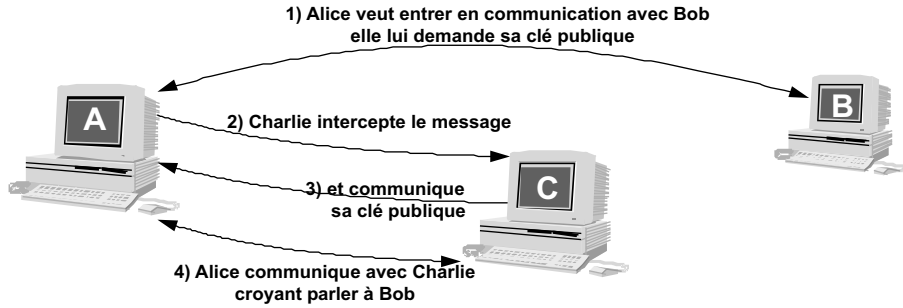


Figure 23.20 La substitution d'identité.

Afin d'éliminer la substitution d'identité, les clés publiques sont disponibles sur un serveur de clés publiques (annuaire) et donc accessibles à tous les utilisateurs, encore faut-il que soit confirmée la relation clé publique/possesseur. C'est l'intervention d'un tiers de confiance (**CA**, *Certificate Authority*) qui garantit la correspondance entre une clé publique et son propriétaire par la délivrance

d'un certificat. Le certificat contient l'identifiant d'un utilisateur et sa clé publique, le certificat est signé avec la clé privée de l'autorité d'authentification. L'autorité de certification peut être interne à l'entreprise (disponible sur l'intranet de l'entreprise) ou être un prestataire de service de certification.

➤ Exemple d'infrastructure de sécurité, la PKI

La **PKI** (*Public-Key Infrastructure*) est un ensemble de protocoles et de services associés qui assurent la gestion des clés publiques. Les différentes fonctions à assurer sont :

- La génération des clés : le système génère et gère deux types de clés, les clés de chiffrement et les clés de signature numérique des messages. La paire de clés publique/privée peut être générée par le CA (Autorité de certification) ou le client. Lorsqu'un client génère lui-même ses clés, il séquestre celle-ci chez le CA en vue d'obtenir la délivrance d'un certificat.
- L'archivage des clés et des certificats (séquestre) : l'agent de séquestre doit assurer le contrôle des accès aux clés privées.
- La délivrance des certificats et clés : celle-ci s'accompagne de la vérification de l'identité du demandeur.
- La gestion des listes de révocation (**CRL**, *Certificate Revocation List*), c'est-à-dire la liste des clés déclarées invalides avant leur date d'expiration.

La figure 23.21 illustre, dans un cas simple, celui où le client génère lui-même son couple de clés, le fonctionnement d'une infrastructure PKI. Bob formule une demande de certificat auprès d'une autorité de certification (CA). Celui-ci, après vérification de l'identité de Bob, lui délivre un certificat et le signe avec sa clé privée. Bob envoie son certificat à Alice et le signe avec sa clé privée. Alice apprend ainsi la clé publique de Bob (validée par la signature numérique du CA) et vérifie auprès du CA la validité du certificat (consultation de la liste des révocations, CRL). Elle vérifie ensuite que Bob est bien l'émetteur du message par lecture de la signature de Bob (utilisation de la clé publique de Bob).



Figure 23.21 Principe des échanges sous PKI.

La délivrance de certificats numériques est normalisée par l'UIT (X.509, actuellement version 3). Un certificat **X.509** identifie la norme (v3 actuellement), il comporte entre autres les informations suivantes :

- un numéro de série unique,
- un identifiant de l'algorithme de signature utilisé,
- le nom de l'émetteur,
- la période de validité,
- la clé publique du sujet,

© Dunod – La photocopie non autorisée est un délit

– l'identifiant de l'émetteur (CA),
– l'identifiant unique du sujet,
– un champ d'extension pouvant comporter du texte, une image...
– la signature de l'émetteur (CA),
– un second champ d'extension a été ajouté par la version 3, il permet notamment d'indiquer le nom et le prénom du titulaire, ses coordonnées...

Le protocole de sécurité de l'environnement IP (IPSec) utilise des certificats X.509 pour l'authentification et le chiffrement.

La sécurité et le protocole de transmission

➤ La sécurité et le protocole PPP (RFC 1334)

Rappelons que le protocole PPP (*Point to Point Protocol*) assure quatre fonctionnalités (figure 23.22), la négociation des paramètres de connexion, l'affectation d'adresse IP, la sécurisation des échanges par authentification des communicants et enfin le transfert de données.

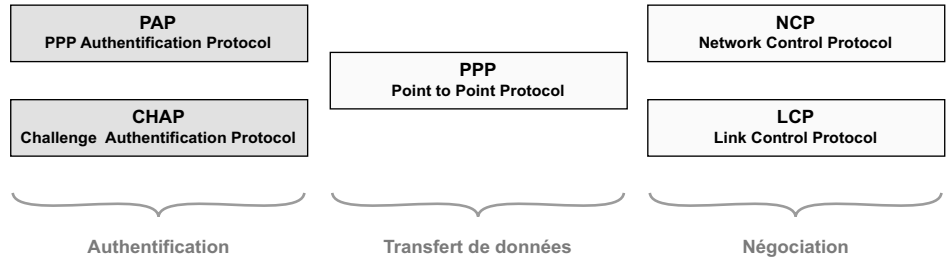


Figure 23.22 PPP et ses sous-protocoles.

Lorsque les paramètres liaison et réseau sont définis, si l'entité LCP a négocié une phase d'authentification, PPP procède à l'identification des entités communicantes.

PAP (*Password Authentification Protocol*) consiste en un simple échange de mots de passe en clair sur le réseau. Cette méthode est très vulnérable, les mots de passe peuvent être écoutés sur la liaison. Un intrus pourra ensuite usurper l'identité d'un des interlocuteurs.

CHAP (*Challenge Handshake Authentification Protocol*) repose sur l'échange de messages cryptés selon une clé secrète (algorithme à clés symétriques) qui ne circule pas sur le réseau. L'identificateur envoie un message en clair à l'interlocuteur distant (*Challenge*). Celui-ci crypte le message avec la clé secrète et le renvoie à l'identificateur (sceau). Si le message reçu est correctement crypté, l'identificateur en conclut que son interlocuteur est bien celui qu'il prétend être. La séquence exécutée dans les deux sens peut être répétée plusieurs fois au cours de la session (échange de sceaux).

➤ Sécurisation des échanges sur le Web

S-HTTP (Secure HTTP)

S-HTTP introduit la cryptographie au niveau HTTP dont elle constitue une extension. S-HTTP organise la session en trois étapes :

– l'authentification, par échange de mots de passe ;

– la négociation, phase où les interlocuteurs négocient le mode de cryptage à utiliser (DES, RSA...) ;
– la transaction, échange de messages cryptés selon le mode prédéfini.

La cryptographie est mise en œuvre par des scripts CGI ou par des « *daemon* » HTTP (*Plug in*).

SSL (Secure Sockets Layer)

Développé par Netscape Communication et intégré aux principaux navigateurs, **SSL** constitue une couche insérée entre la couche application et la couche TCP (figure 23.23). *Secure Sockets Layer* procède en quatre étapes :

– le client s'identifie auprès du serveur web ;
– le serveur web répond en communiquant sa clé publique ;
– le client génère alors une clé secrète, la chiffre à l'aide de la clé publique du serveur et la communique à ce dernier ;
– la clé ainsi attribuée est utilisée durant toute la session.

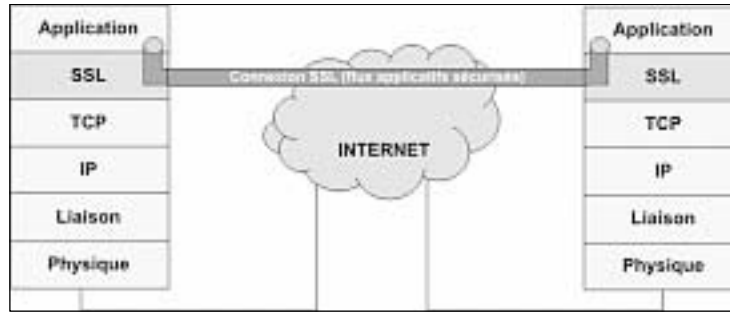


Figure 23.23 Principe de l'architecture de SSL.

SSL crée une connexion qui permet un échange sécurisé dans le réseau. Cependant, le système n'est pas infaillible. En effet, la clé secrète est générée à partir de l'horloge de la machine, ce qui permet de la trouver en quelques minutes.

➤ IP Security

Non limité aux échanges via un navigateur, l'*Internet Protocol Security Standard* fournit une sécurisation au niveau IP. Développé à l'origine le cadre d'IPv6 et adapté à IPv4, IPSec offre les services de contrôle d'accès, d'authentification, d'intégrité et de confidentialité des données, il met en œuvre un mécanisme d'anti-rejeu.

IPSec supporte de nombreux algorithmes de chiffrement (DES, triple DES, RC5, IDEA...), de hachage (MD5, SHA-1...) et d'authentification (signatures RSA ou DSS, clé secrète, clé publique). Dans ces conditions, l'utilisation d'IPSec est précédée d'une phase de négociation pour déterminer les mécanismes qui seront utilisés. L'ensemble des informations partagées entre les deux systèmes, pour établir une communication sécurisée, constitue une association de sécurité (**SA**, *Security Association*). Une association de sécurité est unidirectionnelle, un échange de données *full duplex* aboutit à la création de deux associations de sécurité.

© Dunod – La photocopie non autorisée est un délit

IPSec intègre deux modes de travail, le **mode transport** et le **mode tunnel** (figure 23.24). Le mode transport ne protège que le champ Données du datagramme IP. Le mode tunnel encapsule le datagramme IP d'origine, un nouvel en-tête IP est ainsi ajouté, les adresses IP source et destination initiales sont masquées.

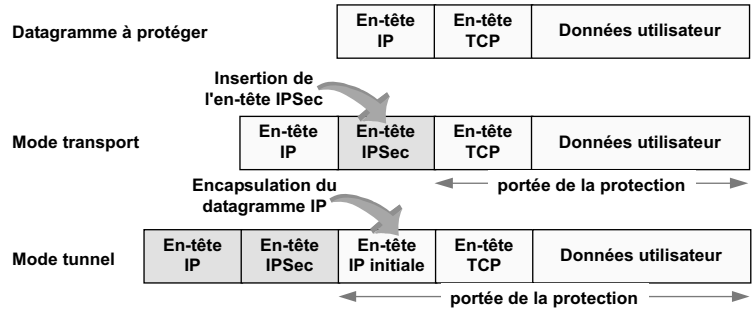


Figure 23.24 IPSec, mode transport et mode tunnel.

L'extension d'authentification (AH)

L'en-tête d'authentification (**AH**, *Authentification Header*) certifie, au destinataire du paquet IP, l'intégrité des données et l'identité de l'origine. Compte tenu de la modification par les éléments du réseau de certaines données d'en-tête IP (**TTL**, *Time To Live*...), le *digest* ne porte que sur les données non modifiées par le réseau. Lors du calcul, ces champs sont mis à 0. L'en-tête AH comporte l'identifiant de l'association de sécurité et, pour éviter le rejeu, un numéro de séquence unique. Les données de l'en-tête AH sont incluses dans le calcul.

L'extension de confidentialité-authentification (ESP)

L'en-tête de confidentialité (**ESP**, *Encapsulating Security Payload header*) garantit la confidentialité des datagrammes, l'intégrité des données et l'identité de la source, il se décompose en trois champs (figure 23.25) :

– à l'instar de l'en-tête AH, le sous-en-tête ESP comprend les données relatives à l'identification de l'association de sécurité et un numéro de séquence « anti-rejeu »,
– un *trailer* (en-queue) ESP précise la portée du chiffrement (mode transport ou mode tunnel),
– un *trailer* d'authentification ESP comporte les données d'authentification.

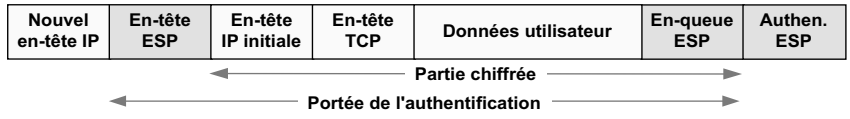


Figure 23.25 L'en-tête ESP en mode tunnel.

23.3.3 La protection du réseau

Les menaces

Les menaces contre les systèmes visent essentiellement à les rendre inaccessibles ou à en altérer profondément les performances. Par exemple, le protocole **ICMP** (*Internet Control Messages Protocol*) constitue l'une des failles (vulnérabilités) des environnements TCP/IP. En effet, il suffit, par exemple, d'adresser à un routeur d'interconnexion des paquets ICMP de signalisation de congestion pour que le routeur destinataire ralentisse ses émissions de messages vers le réseau extérieur. Cela peut faire supposer à un abonné que le réseau, auquel il a souscrit, n'est pas suffisamment dimensionné.

De même, les paquets ICMP sont utilisés par le protocole RIP (ICMP *redirect*) pour modifier les tables de routage. Il est alors possible de faire croire à un routeur qu'il n'existe plus aucune route pour aller vers tel ou tel site, ou même détourner le trafic vers un autre site. Ces attaques sont généralement difficiles à détecter.

Les attaques peuvent se classer en deux catégories : celles qui visent à prendre connaissance d'informations soit pour les exploiter soit pour les altérer et celles qui visent à paralyser voire détruire les systèmes. Les modes d'attaque sont nombreux, ils vont de la simple usurpation de mots de passe (*brute force attack*[3] ou *dictionary attack*[4]...) à l'introduction de code malicieux (virus) en passant par la mystification des systèmes (*IP Spoofing*[5]...).

La protection de l'intranet

➤ Protection du réseau local en interne

La sécurisation de la composante locale vise deux objectifs. Le premier tente de prévenir les connexions non autorisées par le contrôle d'adresses (association d'un port du commutateur ou du *hub* et d'une adresse MAC) et la désactivation des prises non utilisées. Le second assure un cloisonnement des trafics par la constitution de VLAN[6].

➤ Filtrage du trafic par le routeur d'accès

Le moyen le plus simple de protéger le réseau contre les intrusions peut être réalisé avec le routeur d'accès (figure 23.26).

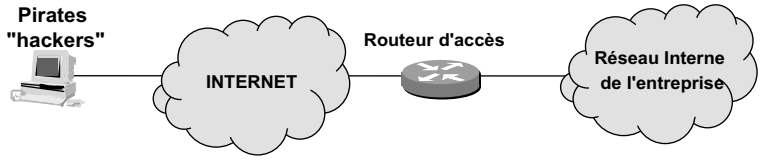


Figure 23.26 Le contrôle du trafic par le routeur d'accès.

3. Tentative de pénétrer un système en essayant toutes les combinaisons possibles de mots de passe.
4. Ces attaques visent à déchiffrer les mots de passe encryptés par comparaison avec un dictionnaire de mots de passe chiffrés.
5. IP *Spoofing* consiste à modifier les adresses IP pour intercepter un trafic.
6. Les VLAN ont été étudiés au chapitre 18.

© Dunod – La photocopie non autorisée est un délit

Le routeur peut assurer des fonctions simples de filtrage par analyse des adresses source et destination. Le routeur n'a de visibilité que sur les données protocolaires du niveau 3, c'est-à-dire les adresses et, dans le mode IP, le protocole transporté dans le datagramme. Ses possibilités de filtre sont donc réduites à ces deux éléments, la sécurité offerte est faible. Les règles de filtrage sont réunies dans des listes (**ACL**, *Access Control List*). La figure 23.27 donne un exemple de règles de filtrage, où « * » signifie toute valeur.

Action	Protocole	Source	Destination	Commentaire
Accept	*	194.23.10.0/24	194.23.11.0/24	Trafic sortant vers établissement de Paris
Accept	*	194.23.11.0/24	194.23.10.0/24	Trafic entrant de l'établissement de Paris
Rejet	*	*	*	

Figure 23.27 Exemple de règles de filtrage.

Le filtre de la figure 23.27 n'autorise le trafic qu'entre deux établissements de l'entreprise. L'établissement de filtres est délicat, il nécessite une analyse fine des trafics autorisés et des trafics interdits. Dans notre exemple simple, l'écriture de la ligne 3 en tête de liste interdirait tout trafic ! Lorsque les filtres sont décrits très finement, il n'est pas rare que certaines lignes soient en contradiction.

➤ La translation d'adresses (RFC 1631)

La translation d'adresses[7] est un moyen de contourner la pénurie d'adresses Internet, mais aussi de masquer, vis-à-vis de l'extérieur, le plan d'adressage de l'entreprise (*IP Masquerade*).

La traduction statique fait correspondre à une adresse interne du réseau une adresse externe, généralement publique. Ce mode de translation résout à la fois le problème de la pénurie d'adresse, du masquage du plan d'adressage local (mascarade) et sécurise le réseau en n'autorisant que certaines stations à accéder à l'Internet (figure 23.28).

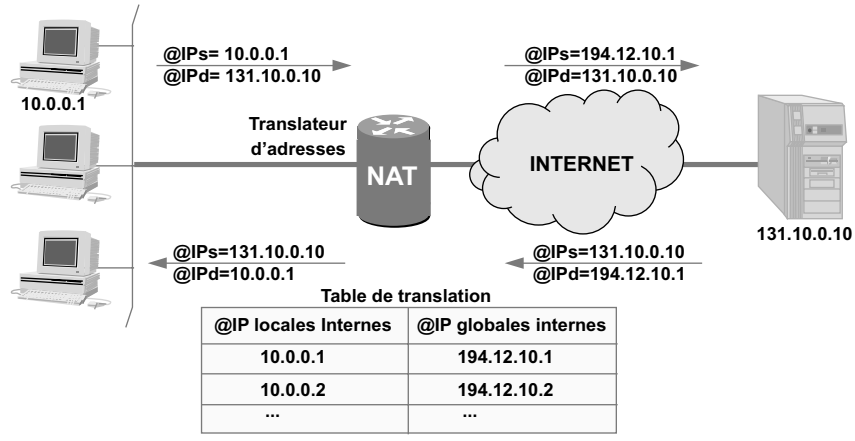


Figure 23.28 La traduction statique d'adresses.

7. La notion de translation d'adresses a été introduite au chapitre 10.

La translation statique limite le nombre de machines ayant accès à l'extérieur au nombre d'adresses publiques attribuées. La traduction dynamique s'affranchit de cette limite. Lorsqu'une machine veut atteindre une machine extérieure, le NAT (*Network Address Translation*) associe à l'adresse locale interne une adresse globale interne, ou adresse externe, choisie parmi un pool d'adresses mises à sa disposition. Le NAT introduit un protocole à état, indépendamment du fait qu'en cas de défaillance du NAT les relations sont perdues, l'état créé doit être détruit en fin de communication et l'adresse attribuée rendue disponible pour une autre connexion vers l'extérieur. Un temporisateur est donc associé à chaque connexion, il est réinitialisé à chaque message, la connexion est libérée sur *time out*.

Cependant, le nombre d'adresses publiques attribuées peut être insuffisant. Le **NAPT** (*Network Address and Port Translation*) permet à plusieurs machines de partager une même adresse externe par translation du numéro de port (figure 23.29). La fonction dite du **PAT** (*Port Address Translation*) autorise plusieurs milliers (65535) de connexion à se partager une même adresse IP externe dite aussi globale interne.

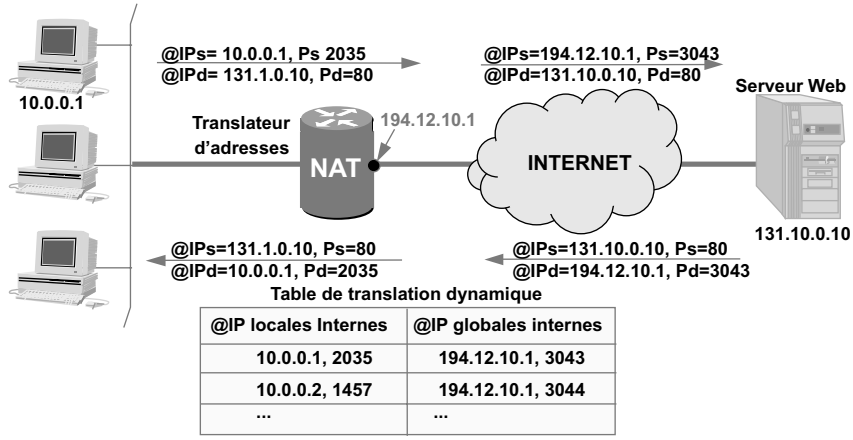


Table de translation dynamique

@IP locales Internes	@IP globales internes
10.0.0.1, 2035	194.12.10.1, 3043
10.0.0.2, 1457	194.12.10.1, 3044
...	...

Figure 23.29 Principe de la translation de port.

En translation dynamique, la correspondance @IP interne/@IP externe est initialisée par la machine interne. Un datagramme entrant, sans correspondance dans la table de translation, est rejeté. Pour donner accès aux machines extérieures, à certains services, on peut utiliser la technique dite du « *Port forwarding* ». Celle-ci permet un accès direct au service concerné et un accès indirect *via* les services d'un **DNS** (*Domain Name System*). La table de translation est pré-renseignée de l'adresse du ou des services ouverts (translation statique). La figure 23.30 illustre ce principe dans le cas où seul le DNS est visible de l'extérieur. Lors d'une requête entrante dont le port destination est le port 53 (DNS), le NAT « *forward* » la requête au DNS. Il extrait de la réponse du DNS l'adresse de la machine à atteindre (194.12.10.2 dans notre exemple) et initialise une entrée dans la table. Cette technique nécessite une adresse publique par machine visible de l'extérieur.

Si le NAT masque au monde extérieur le plan d'adressage de l'entreprise et protège les machines contre des attaques directes, il est consommateur de ressource et pénalise les performances du réseau. En effet, il nécessite le recalcul des *checksum* (IP et TCP). De plus, il est, en principe, incompatible avec IPSec, du moins en mode tunnel (encapsulation des champs Adresses).

© Dunod – La photocopie non autorisée est un délit

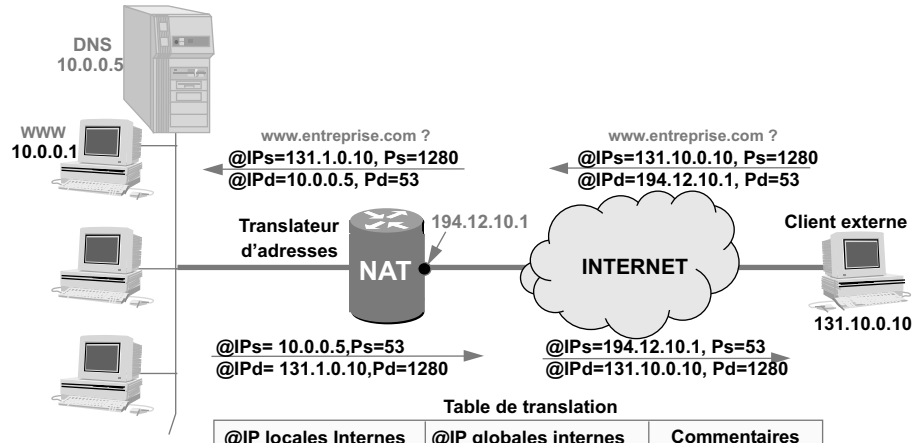


Table de translation

@IP locales Internes	@IP globales internes	Commentaires
10.0.0.5, 53	194.12.10.1, 53	Permanente, DNS
10.0.0.1, 80	194.12.10.2,80	
...	...	

Figure 23.30 La translation d'adresses et trafic entrant.

➤ Les pare-feu (*firewall*)

Le pare-feu (*firewall*) est un système aux fonctions de filtrage évoluées. Indépendamment des fonctions de routage et de translation d'adresses, chaque paquet reçu est examiné, une décision de rejet ou d'acceptation est prise en fonction de nombreux critères :

– l'adresse destination,
– l'adresse source,
– le protocole transporté (ICMP, UDP...),
– le port destination,
– le port source,
– la valeur de certains flags (ACK, SYN...)...

La décision est prise pour chaque datagramme, il n'y a pas de notion de contexte. Il existe deux types de pare-feu (figure 23.31).

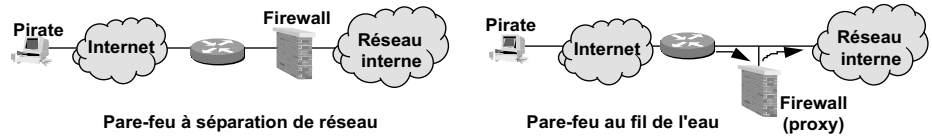


Figure 23.31 Les différents modes d'utilisation des pare-feu (firewall).

Le pare-feu à séparation des réseaux segmente le réseau en deux tronçons : le réseau interne et le réseau externe. Il contrôle le trafic et peut réaliser une translation d'adresses (NAT). Le pare-feu au fil de l'eau n'effectue aucune séparation physique des réseaux. Cependant, comme le pare-feu

à séparation des réseaux, il réalise l'isolation des trafics. Les postes ne communiquent qu'avec le pare-feu (passerelle par défaut) et le routeur ne voit que le pare-feu[8].

La figure 23.32 illustre les différentes architectures de sécurité envisageables, la mise à disposition d'un serveur public (service Web, messagerie...) est généralement réalisée par la constitution d'une zone de sécurité dite **DMZ** (*DeMilitarized Zone*). Différentes zones de sécurité peuvent être constituées, chacune accessible selon des critères spécifiques (filtres). L'utilisation de deux pare-feu permet de renforcer cette sécurité. Le premier masque le second aux pirates éventuels. En choisissant les deux pare-feu de marque différente, on améliore encore la sécurité, les vulnérabilités ou failles de l'un étant différentes de celles de l'autre. La zone démilitarisée accueillera les différents serveurs accessibles à la fois par le personnel de l'entreprise et par le monde extérieur. Pour différencier les services offerts et les règles de filtrage, il est possible de définir plusieurs DMZ, dans ce cas généralement l'une est accessible à tous (DMZ publique), et l'autre aux personnels de l'entreprise (DMZ privée).

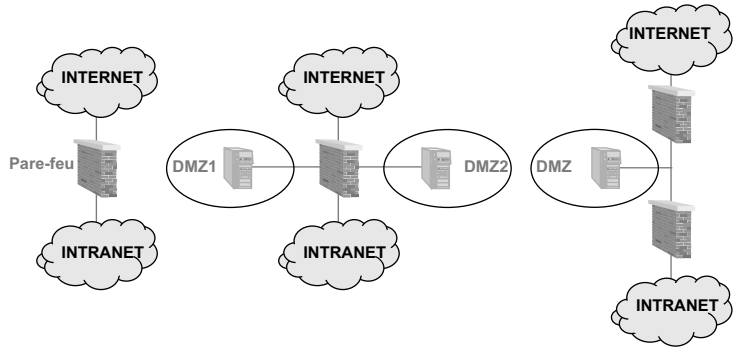


Figure 23.32 Les différentes architectures de sécurité.

La définition des filtres est similaire à celle réalisée pour les routeurs, seule, la portée de l'analyse est plus profonde. Tout datagramme non autorisé est rejeté. En cas de tentative de violation d'une règle, les pare-feu émettent des alertes. Un fichier (logs) conserve une trace de tous les événements. La figure 23.33 présente quelques exemples de règles de filtrage.

Règles	Destination		Source		Flag	Action	Commentaire
	Adresse	Port	Adresse	Port			
1	Externe	25	Interne	>1023		accept	Connexion vers serveurs SMTP
2	Interne	>1023	Externe	25	ACK	accept	Réponses aux connexions SMTP
3	Externe	23	Interne	>1023		accept	Connexion à des services Telnet
4	10.0.0.5	23	194.28.12.1	>1023		accept	Station externe autorisée Telnet
5	194.28.12.1	>1023	10.0.0.5	23		accept	Trafic Telnet station 194.28.12.1
6	Interne	23	Externe	>1023	ACK	accept	Réponses au trafic Telnet

Figure 23.33 Les exemples de règles de filtrage.

8. Un pare-feu au fil de l'eau est généralement désigné sous le terme de bastion ou proxy.

© Dunod – La photocopie non autorisée est un délit

L'énoncé des règles 1 et 2 autorise le trafic de toutes les stations du réseau interne vers des serveurs SMTP externes, mais n'autorise pas les connexions d'origine externe en provenance d'un service sur le port 25 puisque les messages d'origine externe doivent avoir le bit ACK (TCP) positionné, de même pour les règles 2 et 6. Cependant, pour autoriser une station spécifique à ouvrir depuis l'extérieur une session Telnet, nous avons inséré les règles 4 et 5. Si celles-ci avaient été placées après la règle 6, aucune connexion en provenance de l'extérieur à destination d'un service Telnet interne n'était autorisée (bit ACK)

➤ Les passerelles applicatives

Les passerelles applicatives (*Application Layer Gateway* ou *Proxy-Server*) établissent une double connexion (figure 23.34). Le filtrage s'effectue alors au niveau de chaque service offert. Les services internes sont invisibles de l'extérieur. La passerelle peut réaliser des conversions de protocoles (messagerie...).

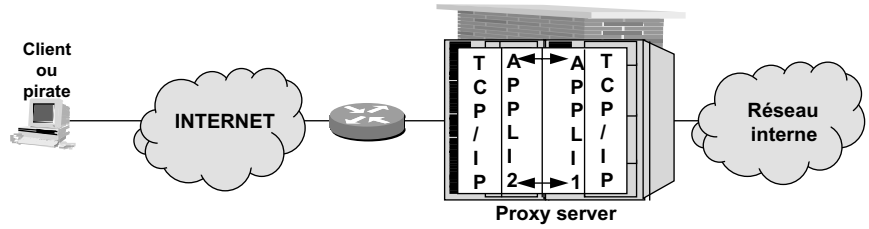


Figure 23.34 Le filtrage par un proxy-server.

Les passerelles applicatives, à l'instar des pare-feu, mémorisent toutes les connexions et peuvent en éditer la liste. L'association pare-feu à séparation de réseau et proxy-server (pare-feu au fil de l'eau) constitue une protection efficace contre les intrusions. Mais quels que soient les moyens mis en œuvre, les virus et chevaux de Troie restent indécelables.

➤ Les codes malicieux (virus)

Un virus est un programme « parasite » qui s'attache à un programme principal dont il modifie l'environnement de travail avec un objectif généralement destructeur. Les programmes virus ont aussi la possibilité de se propager de machine en machine directement avec le programme infecté (copie de programme), mais aujourd'hui de plus en plus par exploitation du carnet d'adresses de la machine infectée.

Les virus fonctionnent en tâche fond. Lorsqu'une certaine condition (date, type d'activité...) est réalisée, le virus effectue la tâche pour laquelle il a été programmé. Les virus peuvent altérer les données, les diffuser vers des adresses aléatoires ou pré-programmées, modifier le comportement du système allant de l'instabilité à la paralysie, voire à la destruction de certains composants du système (effacement du BIOS...).

Des logiciels, dits antivirus, permettent de se protéger des virus connus. Cependant, malgré les mises à jour, les « pirates » ont toujours un virus d'avance. La seule parade efficace consiste à n'échanger des données avec personne et de ne jamais raccorder son ordinateur à un réseau !

La protection des accès, les VPN

Autoriser des utilisateurs nomades d'accéder au système d'information de l'entreprise nécessite la mise en œuvre d'un système d'accès distant (**RAS**, *Remote Access Service*) qui garantisse l'authentification et la confidentialité des données. La figure 23.35 illustre les différents modes d'accès aux réseaux d'une entreprise.

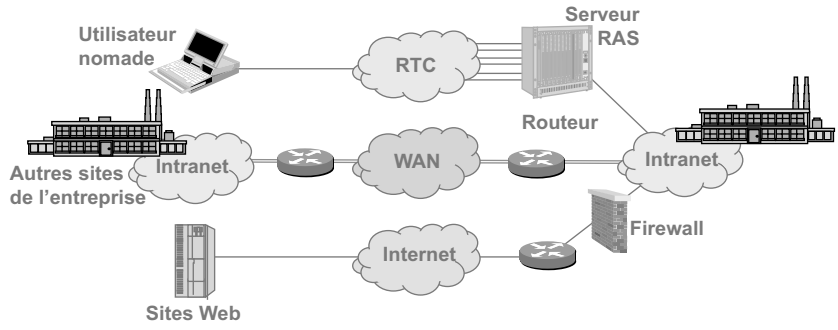


Figure 23.35 Les différents accès possibles au réseau d'une entreprise.

Cette approche traditionnelle en multipliant les modes d'accès complexifie la maintenance du système et, en terme de sécurité le fragilise. Les **VPN** (*Virtual Private Network*), en unifiant les technologies d'accès et en sécurisant les données, apportent une solution aux problèmes précédents. Un VPN[9] sécurisé correspond à la réalisation dans un réseau public de tunnels chiffrés simulant ainsi un réseau privé de liaisons point à point. La figure 23.36 illustre l'évolution du réseau de la figure 23.35 vers un VPN. Le service de VPN peut être offert par un opérateur (Telcos) ou réalisé à travers Internet.

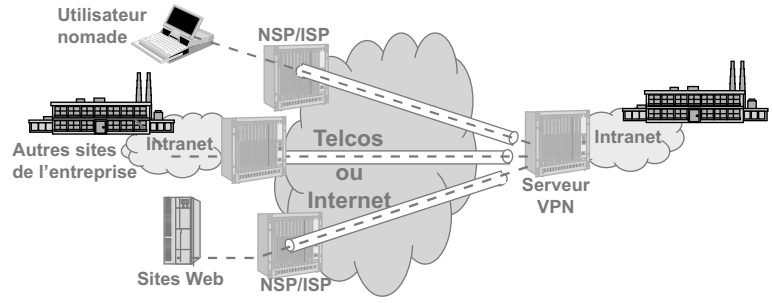


Figure 23.36 L'évolution du réseau vers le VPN.

Réaliser un tunnel consiste à assurer le transport des données utilisateur dans un protocole qui masque ces dernières (encapsulation). Selon que ce soit le terminal client ou l'opérateur qui initialise le tunnel, le tunnel est dit tunnel client ou tunnel opérateur.

Le tunnel opérateur est initialisé par l'opérateur (figure 23.37), le client se connecte de façon transparente.

9. Les VPN ont été introduits à l'occasion de l'étude de MPLS, se reporter au chapitre 15 pour plus de détails.

© Dunod – La photocopie non autorisée est un délit

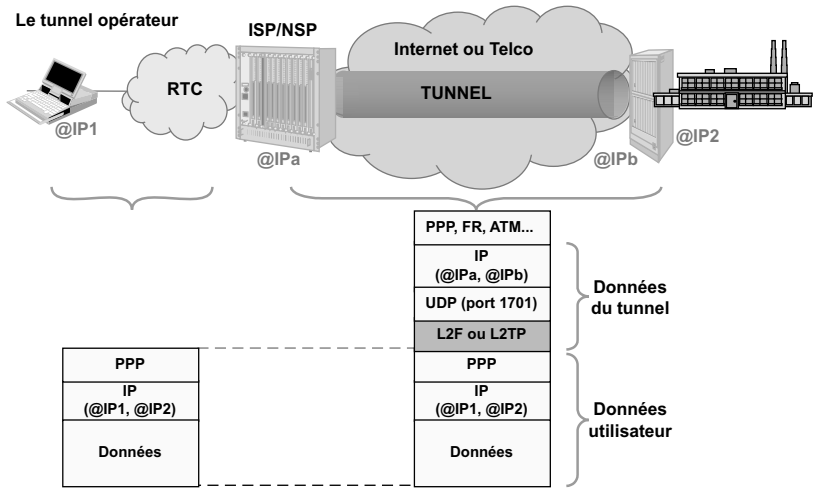


Figure 23.37 Le tunnel opérateur (L2F, L2TP).

Avant d'établir le tunnel vers l'entreprise, l'opérateur (ISP) identifie et authentifie le client. Si l'utilisateur est reconnu, l'ISP ouvre un tunnel vers l'entreprise qui, de même, authentifie le client avant d'accepter la connexion. Lorsque le tunnel est initialisé par le client (tunnel client ou de bout en bout), celui-ci doit être doté d'un logiciel spécifique (figure 23.38).

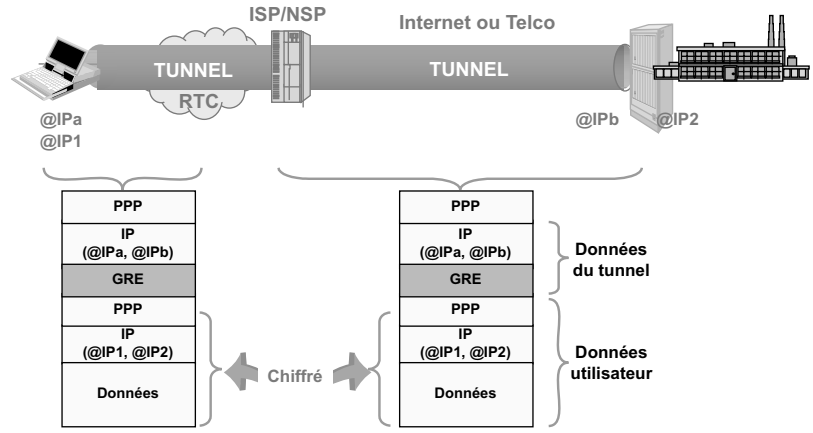


Figure 23.38 Le tunnel client (PPTP).

Selon le niveau de l'encapsulation, on distingue des tunnels de niveau 2 ou 3 (IPSec[10]). Trois protocoles permettent de réaliser des tunnels de niveau 2 :

– **L2F**, *Layer 2 Forwarding*, d'origine Cisco est un tunnel dit opérateur, il est initialisé par le fournisseur d'accès (**ISP**, *Internet Service Provider*) et se termine chez le client par un équipement spécifique. Le protocole L2F n'assure l'authentification de l'utilisateur qu'à la

10. Les tunnels de niveau 3 de type IPSec ont été étudiés dans ce chapitre § 23.3.2.

connexion. Le tunnel L2F ne garantit pas la confidentialité des données (pas de chiffrement). Cependant, un chiffrement utilisateur de bout en bout peut être mis en œuvre.

– **PPTP**, *Point-to-Point Tunneling Protocol*, d'origine Microsoft est une technique de tunnel de bout en bout (le tunnel est initialisé par le client). La session client PPP est transportée de bout en bout dans une encapsulation spécifique (**GRE**, *Generic Routing Encapsulation*). Les datagrammes peuvent être chiffrés par le protocole d'origine Microsoft **MPPC** (*Microsoft Point-to-Point Encryption*).
– **L2TP**, *Layer 2 Tunneling Protocol*, d'origine IETF, L2TP est un protocole de tunnel opérateur (ouvert par le *provider*), il autorise les appels *outbounds* (appels initiés depuis l'intranet destination), il peut être utilisé conjointement à IPSec pour chiffrer les données, en-tête IP d'origine comprise.

23.4 LE COMMERCE ÉLECTRONIQUE

Le problème essentiel du commerce électronique consiste à garantir la sécurité des transactions (authentification des interlocuteurs, confidentialité des échanges, sécurité bancaire...). Deux approches du commerce électronique sont envisageables selon que l'organisme bancaire participe directement à la transaction (paiement *on-line*) ou que l'organisme bancaire est étranger à la transaction (paiement *off-line*).

23.4.1 Le paiement *off-line* (*e-cash*)

Dans ce mode de paiement, le client approvisionne un compte local en monnaie électronique (monnaie virtuelle) et réalise la transaction commerciale avec elle. La figure 23.39 illustre ce principe.

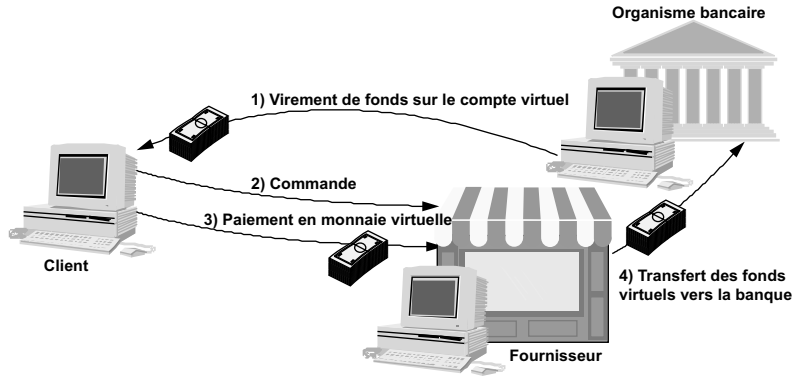


Figure 23.39 Le paiement off-line.

23.4.2 Le paiement *on-line*

Dans ce type de relation, le paiement s'effectue à l'aide d'une carte bancaire. Le client joint à son bon de commande (crypté avec la clé publique du vendeur) son numéro de carte bancaire (crypté avec la clé publique de la banque). Le vendeur transmet à la banque le numéro de carte crypté et le montant de l'achat. La banque effectue le transfert de fonds (figure 23.40)

© Dunod – La photocopie non autorisée est un délit

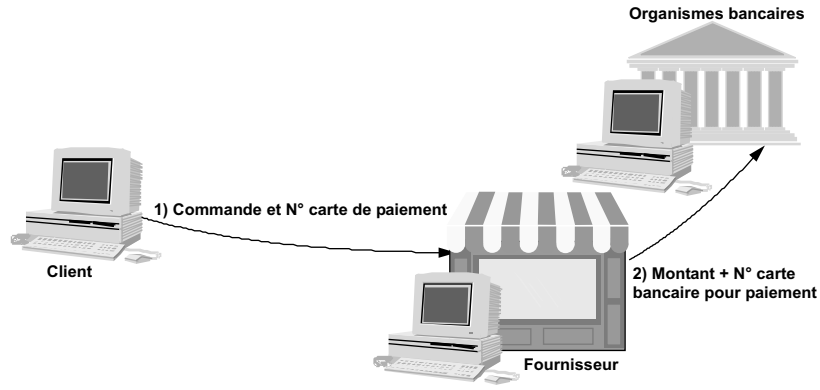


Figure 23.40 Principe du paiement on-line.

Cette approche (**SET**, *Secure Electronic Transaction*) est retenue par la plupart des organismes de cartes de crédit (Visa, Mastercard, American Express...) et les constructeurs comme Microsoft, Netscape et IBM.

Cependant, elle présente l'inconvénient de multiples transferts de clés entre le vendeur, le client et les banques. Le protocole **JEPI** (*Joint Electronic Payment Initiative*), défendu par le World Wide Web Consortium et Commerce Net, vise à minimiser les échanges et à permettre les petits paiements.

23.5 CONCLUSION

Quels que soient les moyens mis en œuvre, du fait de l'ouverture vers l'extérieur, les réseaux seront de plus en plus vulnérables. Dans ses conditions, il appartient à chaque entreprise de mesurer le risque et le coût d'une indisponibilité du système, de la divulgation d'information... et déterminer une politique dite de sécurité, d'en mesurer les coûts et d'assurer en permanence une veille technologique pour que les moyens employés restent efficaces devant l'évolution des menaces.

EXERCICES

Exercice 23.1 MTTR/MTBF

Soit deux systèmes informatiques identiques interconnectés *via* les services d'un opérateur et une liaison téléphonique de secours (figure 23.41). Quel est, pour l'ensemble du système, la disponibilité, l'indisponibilité et la MTBF du système, compte tenu des éléments ci-dessous (par hypothèse, on admettra que la MTBF de l'opérateur inclut la liaison d'abonné et les modems d'extrémité) ?

	MTBF	MTTR
Système 1	4 mois	8 heures
Système 2	4 mois	8 heures
Modem	2 ans	5 heures
RTC	2 ans	24 heures
Telcos	2 ans	2 heures

On considérera qu'un mois représente 200 heures et une année 2 400 heures

Figure 23.41 Le système avec ligne de secours.

Exercice 23.2 Systèmes à clés symétriques ou secrètes

Un système de messagerie sécurisé met en relation N utilisateurs. Dans un système à clés secrètes, chaque utilisateur doit, pour communiquer avec les autres abonnés, connaître la clé secrète de chacun des autres abonnés aux systèmes. En supposant, l'administration centralisée des clés, déterminez le nombre de clés que le système devra gérer. Que devient ce nombre dans un système à clés publiques ?

Exercice 23.3 Algorithme à translation de César

Retrouvez le clair du message codé à l'aide de l'algorithme de César « HTIFLJIJHJXFW ».

Exercice 23.4 Algorithme de substitution de Vigenère

Le système de Vigenère utilise la substitution polyalphabétique. Son principe est relativement simple. Dans un tableau, dit carré de Vigenère, on remplace la lettre du message à chiffrer par la lettre obtenue à l'intersection de la colonne repérée par cette lettre, et de la ligne définie par la lettre de la clé associée à la lettre du message.

Soit, par exemple à coder le message « ABACADRABRA » à l'aide de la clé « CLE ».

Méthode :

– Supprimer tous les blancs du message d'origine.

© Dunod – La photocopie non autorisée est un délit

– Recopier autant de fois que nécessaire la clé. Afin d'obtenir un texte de longueur identique à celle du message.
– Déterminer la lettre du cryptogramme en pratiquant comme suit :
  – La lettre du cryptogramme est la lettre obtenue à l'intersection de la colonne de la lettre sélectionnée dans le message et de la ligne déterminée par la lettre en correspondance dans le texte (clé).

Clair → A B A C A D R A B R A
Clé → C L E C L E C L E C L

  – La lettre D du message est en correspondance avec la lettre E de la clé, elle sera codée par la lettre obtenue à l'interception de la colonne D et de la ligne E soit H (figure 23.42).

Retrouvez le clair du crypte « LEDCITMHGMMZWRGII » codé à l'aide de la clé « SECRET ».

	↓																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	A	B	C	***D***	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V	W	X	Y	Z	A
3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
→ 5	***E***	F	G	**H**	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	B	E	F
8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y	Z	A	B	C	D	E	F	G
9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K
19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R
20	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V
24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 23.42 Le carré de Vigenère.

Exercice 23.5 Systèmes à clés asymétriques

Le système de cryptographie à clé asymétrique le plus répandu, le RSA, repose sur l'arithmétique des grands nombres.

– La fonction de chiffrement est de la forme :

$$\text{Crypte} = \text{Clair}^{\text{clé } C} \text{ modulo } n$$

où Crypte est le message codé,
Clair le message à coder,
clé C, la clé de chiffrement,
n, un produit de nombres premiers.

– La fonction de déchiffrement est identique :

$$\text{Clair} = \text{Crypte}^{\text{clé } D} \text{ modulo } n$$

où Crypte est le message codé,
Clair le message à coder,
clé D, la clé de déchiffrement,
n, un produit de nombre premier.

– L'algorithme de détermination des clés est rappelé ci-dessous :
  – Choisir deux nombres premiers p et q grands et différents ($> 10^{100}$).
  – Calculer n tel que $n = p \times q$.
  – Choisir les clés telles que $C \times D = 1 + M\,[(p-1) \times (q-1)]$, où M est un entier qui satisfasse l'égalité.
  – Définir la longueur maximale (L) du bloc de bits sur lequel on applique l'opération de sorte que $2^L < n$.

1. Calculez les plus petites clés possibles (pour des raisons tenant aux possibilités de calcul p et q seront choisis les plus petits possibles). Pour ces clés et pour toutes les valeurs (fonction de L) que peuvent prendre les messages clairs, établissez la matrice de codage et de décodage en renseignant le tableau ci-dessous.

Clair	N = Clair^C	Crypte = N mod n	N = Crypte	Clair = N mod n

2. Est-il possible d'utiliser cette combinaison de clés pour transmettre un message chiffré ? Expliquez pourquoi et indiquez la ou les condition(s) supplémentaire(s) à introduire dans l'algorithme.
3. Compte tenu de la question précédente, déterminez les plus petites clés utilisables et établissez la matrice de codage et de décodage.
4. On désire envoyer le message clair « MODEM » codé en ASCII sur 8 bits (le bit de poids fort est positionné à zéro), déterminez le crypte.

Exercice 23.6 Système de Diffie-Hellman

Déterminez la clé de session Diffie-Hellman, si Alice communique à Bob les nombres $G = 3$ et $N = 23$, sachant qu'Alice tire le nombre aléatoire $A = 5$ et Bob le nombre B = 7 ?

© Dunod – La photocopie non autorisée est un délit

Chapitre **24**

Notions d'ingénierie des réseaux

24.1 GÉNÉRALITÉS

Pour satisfaire les besoins de télécommunication des entreprises, les opérateurs (prestataires de service de télécommunication) offrent deux types de service, les services supports et les téléservices.

Les **services supports** consistent à fournir à un abonné (l'entreprise) un lien de communication (support physique ou virtuel) entre deux points (ligne point à point) ou entre un et plusieurs points (ligne multipoint). Les services offerts peuvent être simples comme la location d'un lien (liaison louée). L'opérateur met alors à disposition de l'entreprise un lien et les organes d'extrémités d'accès (modems). Lorsque ce support est numérique l'opérateur s'engage sur le débit nominal du lien et le taux d'erreur nominal. Quand il s'agit d'un lien analogique seuls la bande passante en fréquence et le rapport signal sur bruit sont garantis. Les liaisons louées sont utilisées pour réaliser des liaisons point à point et les réseaux privés d'entreprise.

Une alternative à la réalisation d'un réseau privé consiste à relier les divers établissements d'une entreprise *via* un réseau de transport public. L'opérateur assure alors le raccordement des sites de l'abonné à son réseau. Les caractéristiques du raccordement dépendent alors du réseau de l'opérateur (débit, protocole...).

Les **téléservices** constituent une offre plus élaborée. L'opérateur fournit alors un moyen complet de communication. Dans cette catégorie, on trouve la téléphonie analogique (RTC) et numérique (RNIS), les services de messagerie, les services télématiques (vidéotex)...

Le type de service requis est déterminé en fonction des services attendus (téléservices) ou de critères techniques (services supports). La politique tarifaire de l'opérateur, l'évolution prévisible des besoins et la reprise de l'existant sont les éléments déterminants devant guider le choix.

L'ingénierie des réseaux recouvre l'ensemble des moyens mis en œuvre pour le choix d'une solution de télécommunication et la réalisation de réseaux de télécommunication (topologie, dimensionnement, évaluation des performances, optimisation...).

24.2 LES SERVICES ET LA TARIFICATION

D'une manière générale, toute fourniture de service comprend : des frais d'accès au service (frais d'établissement ou de mise en service), un abonnement et une redevance d'usage. Les frais d'établissement sont comptés pour chaque raccordement au service. Ainsi, lors de l'installation d'une liaison louée, la redevance est due pour chaque extrémité du lien. La redevance d'usage dépend de certains critères dont :

– le temps et la distance (réseau téléphonique), ces éléments pouvant subir des modulations tarifaires en fonction des créneaux horaires d'utilisation ;
– le volume de données transféré (réseaux X.25) ;

La redevance peut aussi être forfaitaire et déterminée en fonction des caractéristiques du raccordement. Ainsi pour les liaisons louées, la redevance d'usage est fixée en fonction de la distance séparant les sites raccordés et du débit nominal de la ligne. Quant à la redevance d'usage des réseaux de données, elle dépend du débit nominal du lien et des descripteurs de trafic définis à l'abonnement (débit moyen garanti, débit de crête permis, nombre de liaisons virtuelles utilisées...). L'opérateur fournit généralement les moyens d'accès : modems, routeurs... Dans ce cas, leur location est comprise dans la redevance mensuelle.

Le choix entre la réalisation d'un réseau privé, à base de liens privés ou publics, ou le recours aux services d'un opérateur est essentiellement motivé par des économies d'échelle, la maîtrise des coûts et des techniques (protocole, voix/données...) ou certaines spécificités de l'entreprise comme la sécurité des informations (confidentialité...).

24.3 LES ÉLÉMENTS D'ARCHITECTURE RÉSEAUX

24.3.1 La structure de base des réseaux

En principe, un réseau comporte deux sous-ensembles : le **réseau dorsal** ou réseau de transit (*Backbone*) et le **réseau de desserte** ou réseau capillaire ou encore réseau de bas niveau (figure 24.1). Le premier est un réseau de concentration qui assure la mise en relation (connectivité) des différentes composantes du réseau de desserte. Le second assure la distribution du service aux abonnés, il est composé d'un ensemble de liens et de concentrateurs. Un niveau de concentration élevé optimise le réseau mais le fragilise.

Le choix de la localisation et du nombre de points d'accès détermine le coût de raccordement des abonnés (sites terminaux de l'entreprise ou abonnés d'un opérateur). De ce fait, il existe une relation étroite entre le graphe du réseau dorsal et le graphe du réseau de desserte.

La réalisation d'un réseau privé dans le contexte d'une entreprise donnée est relativement simple, l'emplacement des points d'accès au réseau est parfaitement déterminé. Dans ces réseaux, ce sont les points de concentration et le mode de liaison entre les différents sites qu'il convient d'optimiser. La topologie est généralement arborescente, le maillage n'intervient qu'en second lieu et essentiellement pour des critères de sécurité (redondance de liens).

Celle des réseaux publics est plus complexe, non seulement les points d'accès sont nombreux, mais les points de concentration ne sont pas prédéterminés et les contraintes de qualité de service sont plus strictes (respect des engagements), mais aussi plus variées (multitude de clients). La solution optimale est généralement le résultat d'un compromis obtenu par itérations successives en formulant différentes hypothèses de positionnement des nœuds d'accès et de concentration.

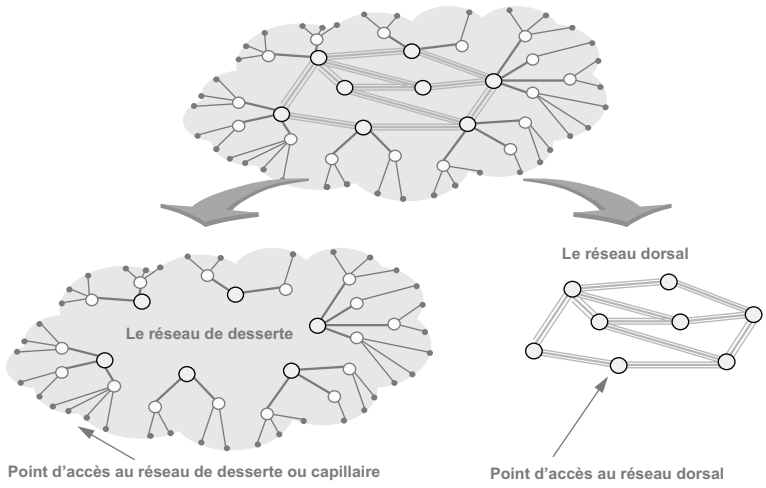


Figure 24.1 L'architecture générale d'un réseau.

Quelles que soient les hypothèses formulées, un réseau résultera de compromis entre performance, fiabilité et coût. En effet, un niveau de performance élevé nécessite un maillage élevé du réseau dorsal et un faible niveau de concentration dans le réseau de desserte, ce qui en accroît la fiabilité mais en augmente aussi le coût.

Il existe de nombreuses méthodes pour optimiser la topologie des réseaux selon un critère prédéterminé (coût, débit, performance...). Certaines essaient de trouver la solution optimale, elles sont difficiles à mettre en œuvre et résistent mal à l'introduction de nouvelles contraintes ou à une évolution des besoins. D'autres méthodes, dites heuristiques, ne cherchent pas à déterminer la solution optimale mais à s'en rapprocher le plus possible. Elles prennent facilement en compte de nombreuses contraintes. Leur principe est simple, à partir d'hypothèses sur le positionnement des composants, elles les réunissent deux à deux par le lien de moindre coût.

24.3.2 La conception du réseau de desserte

Du fait de la densité des points de concentration et des liaisons, le réseau de desserte est généralement le plus coûteux à réaliser. Aussi, c'est à partir de lui que la localisation des points d'accès au réseau dorsal est déterminée. Ainsi, le réseau de desserte est étudié nœud par nœud en formulant diverses hypothèses sur la localisation des nœuds du niveau supérieur. Après avoir défini les niveaux de concentration, on affecte les concentrateurs de niveau N aux concentrateurs de niveaux $N–1$, en respectant les contraintes de nombre de branches (fiabilité), de débit, de coût...

Les deux méthodes exposées ci-dessous dérivent de l'algorithme de Prim et de Krustal. L'algorithme de Prim sous contrainte consiste à :

- formuler une hypothèse sur le positionnement du nœud de concentration principal (accès au réseau dorsal...),
- définir les points à raccorder,
- déterminer le coût (C_{xy}) de toutes les liaisons une à une (matrice des coûts) entre les différents nœuds du réseau,
- trier les liens par ordre croissant des coûts,

© Dunod – La photocopie non autorisée est un délit

– considérer le nœud de concentration comme nœud central et l'inclure en premier dans l'arbre,
– tant que les contraintes fixées pour les raccordements sont respectées (débit maximal à concentrer, nombre de liens regroupés...) relier le point dont le coût de connexion est le plus faible à l'un des points déjà contenus dans l'arbre,
– réitérer l'action précédente jusqu'à ce que tous les nœuds soient reliés, en ne retenant que les liaisons ne faisant pas de boucle et qui respectent les contraintes imposées.

La mise en œuvre de l'algorithme de Kruskal sous contrainte est aussi simple, elle comprend les étapes suivantes, les quatre premières étapes étant identiques à celles de l'algorithme de Prim :

– construire la première branche en réunissant les deux nœuds dont le coût de la liaison est le plus faible ;
– réitérer l'action précédente jusqu'à ce que tous les nœuds soient reliés, en ne retenant que les liaisons ne faisant pas de boucle et qui respectent les contraintes imposées (débit global, nombre de liens sur un même point de concentration...) ;
– quand pour une branche, un regroupement ne peut plus être opéré (contrainte atteinte), le regroupement est considéré comme un sous-arbre qui sera relié au nœud de concentration supérieur élu, par son nœud le plus proche.

La figure 24.2 illustre ces deux méthodes. Pour ces exemples, le coût est considéré comme une fonction linéaire de la distance séparant les différents nœuds, le nœud « ***A*** » pouvant représenter le nœud de concentration de niveau supérieur ou le site informatique principal d'une entreprise vers lequel tous les sites doivent converger. La contrainte retenue ici a été le débit, celui-ci ne devant pas excéder pour cet exemple 8. Le débit requis par chaque nœud figure à droite de son identification. Bien que les graphes résultants diffèrent, les coûts sont ici très proches.

	a	b	c	d	e	f	g	h	i	j	k
a		35	40	74	69	42	40	64	60	25	43
b			31	61	80	75	55	95	91	60	76
c				35	50	84	32	88	95	84	82
d					49	89	51	111	124	96	116
e						58	29	74	96	77	97
f							38	23	37	29	41
g								60	74	50	70
h									25	41	44
i										35	27
j											20

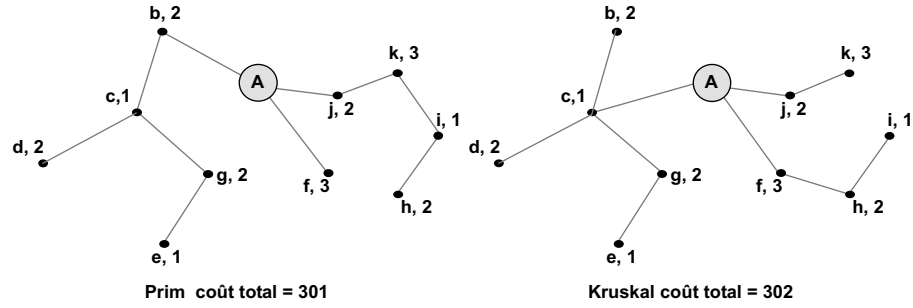
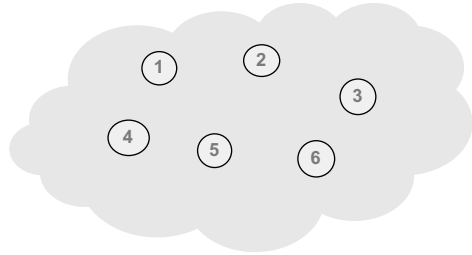


Figure 24.2 La matrice des coûts et les arbres à coût minimal de Prim et Kruskal.

24.3.3 La conception du réseau dorsal

La recherche de performance et de fiabilité conduit à multiplier les liens inter-noeuds (maillage) de façon à assurer une redondance de route (fiabilité) et à minimiser le nombre de sauts (performance). Plusieurs méthodes existent, l'une des plus simples, la méthode de Steiglitz, donne des résultats satisfaisants pour la plupart des réseaux d'entreprise. Cette méthode, illustrée figure 24.3, consiste à :

- définir le positionnement de tous les nœuds et leur connectivité (nombre de liens aboutissant à un nœud),
- attribuer, arbitrairement, un poids à chaque nœud (valeur indiquée sur la figure dans le cercle matérialisant le nœud),
- relier le nœud de plus faible connectivité (en cas d'égalité prendre le nœud de plus faible poids) à son voisin de moindre coût,
- répéter l'opération tant que la connectivité de chaque nœud n'est pas atteinte,
- modifier les poids attribués, refaire le graphe jusqu'à trouver celui de coût minimal.



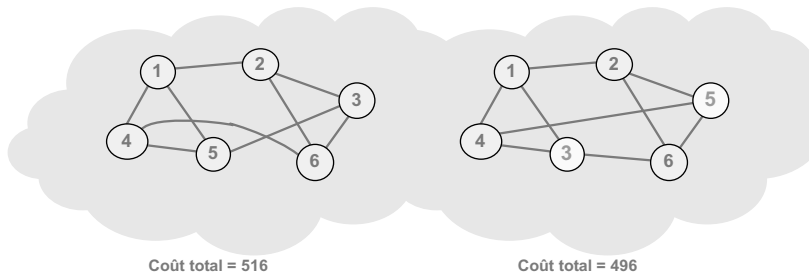
Points d'accès au réseau dorsal

	1	2	3	4	5	6
1		52	101	40	52	95
2	52		50	85	57	55
3	101	50		123	80	32
4	40	85	123		48	107
5	52	57	80	48		60
6	95	55	32	107	60	

Matrice des coûts

Figure 24.3 La conception du réseau dorsal.

Au début, tous les nœuds ont la même connectivité (0), on choisit le nœud de poids le plus faible soit 1, le nœud 4 est le voisin à coût minimal, on relie 1 à 4. Ensuite, on prend le suivant 2 (poids le plus faible), on le relie à 3 (coût le plus faible)... En final on obtient le réseau de la figure 24.4 (gauche). La partie droite de la figure représente le même réseau obtenu en changeant la valeur des divers poids.



Coût total = 516 Coût total = 496

Figure 24.4 Le graphe du réseau dorsal.

© Dunod – La photocopie non autorisée est un délit

En principe, la réalisation d'un réseau d'entreprise est plus simple : les points de concentration coïncident avec les points de consommation et sont déterminés (établissements de l'entreprise), beaucoup d'entreprises mettent en œuvre une topologie étoile autour de leur centre informatique principal. Lorsque les contraintes sont faibles en terme de débit, mais fortes en terme de coût, l'algorithme de Kruskal vu précédemment donne d'excellents résultats.

24.4 LE DIMENSIONNEMENT ET L'ÉVALUATION DES PERFORMANCES

24.4.1 Généralités

Évaluer les performances d'un réseau est une tâche essentielle, tant lors de la conception que durant tout le cycle de vie du système. Indépendamment de mesures concrètes (débit, temps de transit...), on utilise généralement un modèle mathématique du réseau (modélisation) permettant de déterminer le comportement du réseau en fonction de certains paramètres et de leur variation (trafic, état d'un lien...). Les éléments pris en compte diffèrent selon que le réseau est en mode circuit ou en mode paquet (figure 24.5) :

– Dans les réseaux en mode circuit (circuits physiques ou IT d'un lien numérique), la bande passante est affectée en permanence à un utilisateur, le mode de transfert est dit synchrone (bande passante fixée par le réseau). La problématique consiste à définir le nombre de liens (IT) en fonction du nombre de sessions utilisateurs par unité de temps (taux d'arrivée) et de la durée moyenne d'une session.
– Dans les réseaux en mode paquet, il n'y a pas de ressource affectée, la bande passante est partagée. Il n'y a pas de relation directe entre le débit de la source et celui du réseau, le mode de transfert est dit asynchrone. Soumis à des trafics sporadiques, et souvent sous-dimensionnés par rapport au trafic total à écouler, ils sont sensibles à la congestion. Les réseaux en mode connecté avec réservation de ressource relèvent à la fois du modèle des réseaux en mode circuit pour le nombre de connexions admises et du modèle des réseaux en mode paquet en ce qui concerne les performances.

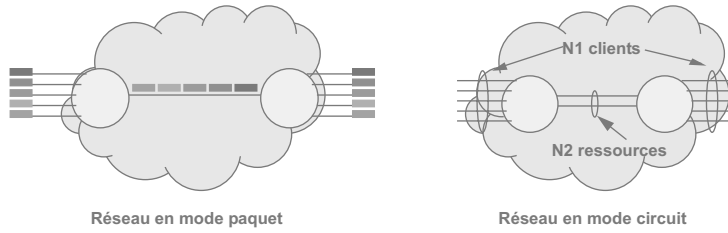


Figure 24.5 Les deux types de réseaux.

24.4.2 Les réseaux en mode circuit

Notion d'intensité de trafic

Lorsqu'un système établit une connexion permanente, le nombre de liens à établir est simple à définir. Si N sites doivent être reliés simultanément à un autre site, généralement désigné par site

central, il est nécessaire de disposer de *N* lignes. Mais lorsque les systèmes d'extrémité n'établissent qu'une connexion temporaire, ce serait un gâchis de ressource que d'équiper le site central d'autant de lignes qu'il y a de possibilité de mise en relation. C'est notamment le cas pour un serveur de messagerie auquel se connectent une fois par jour les itinérants des sociétés pour y relever leur courrier, transférer leurs commandes et éventuellement télécharger les nouveaux tarifs.

Partant du principe que les sources sont indépendantes les unes des autres (les arrivées sont supposées suivre une loi de Poisson), il n'est pas improbable que, dans certaines circonstances, les arrivées dépassent les capacités de traitement du système. Dans ces conditions, les requêtes en surnombre sont soit éliminées, soit mises en attente de libération d'un organe de traitement (support, ou autre). Sur ce principe, Erlang (mathématicien danois) a développé deux modèles l'un dit à refus ou blocage (**modèle B**), l'autre dit à attente (**modèle C**).

Les modèles ont été élaborés à partir de l'expression de la quantité de trafic à satisfaire dénommé **intensité de trafic** et exprimée en erlang par la relation :

$$E = \frac{1}{T}\int_0^T n(t)dt$$

ou plus simplement

$$E = NT/\,3\,600$$

où T est exprimé en secondes,
N nombre de sessions par heure,
E représente la charge de trafic en erlang[1].

Ainsi, 1 erlang représente l'occupation permanente d'un organe pendant 1 heure, ou l'occupation effective de deux organes à 50 % (1/2 heure chacun) pendant la même période. L'intensité de trafic sur une ligne représente le taux de connexion de celle-ci, c'est-à-dire le temps d'appropriation de l'organe par unité de temps.

Le modèle d'Erlang à refus (modèle B)

➤ Formule d'Erlang

Dans un système dit à pénurie de ressource, c'est-à-dire que le nombre de clients (***n***) est supérieur au nombre d'organes de traitement (***m***), Erlang a établi que la probabilité ***p*** de refus d'appel (facteur de blocage) par suite d'encombrement ou autre pour un trafic à écouler de ***E*** erlang est donnée par la relation (figure 24.6) :

$$p = \frac{E^m/m!}{\sum_{k=0}^{k=m} E^k/k!}$$

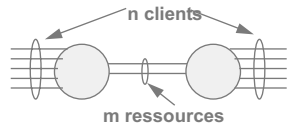


Figure 24.6 La formule d'Erlang à refus.

Cette formule a permis d'établir un abaque de dimensionnement appelé abaque d'Erlang représenté figure 24.7.

1. L'intensité de trafic est un nombre sans dimension.

© Dunod – La photocopie non autorisée est un délit

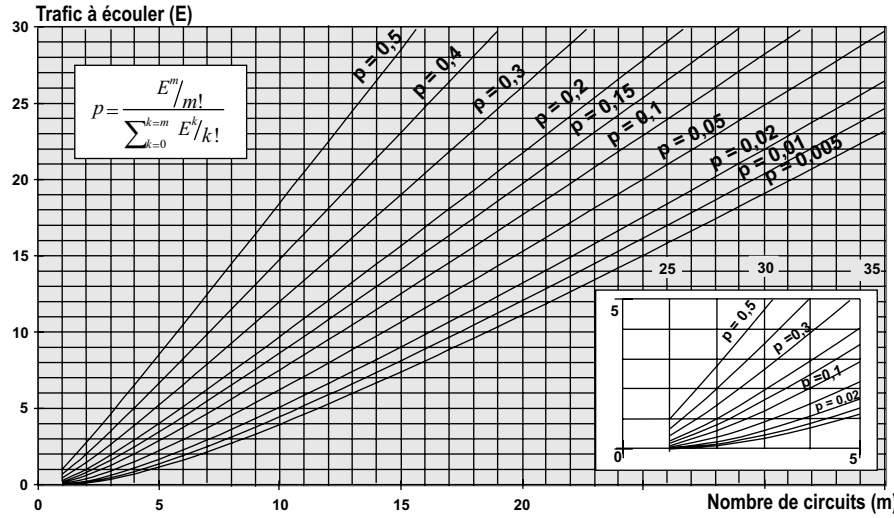


Figure 24.7 L'abaque d'Erlang (refus).

➤ Trafic demandé, trafic écoulé, trafic perdu

Par suite des collisions d'appel (organes occupés), une partie du trafic à écouler ou trafic demandé est perdue. Le trafic perdu et celui demandé sont liés par la relation :

$$\text{Trafic perdu} = \text{Trafic demandé} \quad p$$

où p est la probabilité de refus d'appel.

Le trafic réellement écoulé est alors :

$$\begin{aligned}\text{Trafic écoulé} &= \text{Trafic demandé} - \text{Trafic perdu} \\ &= \text{Trafic demandé } (1 - p)\end{aligned}$$

La figure 24.8 fournit quelques exemples pour un trafic de 0,9 erlang lorsque la ressource passe de 1 à 5 organes.

Trafic demandé	Ressources m	Probabilité de perte	Trafic perdu	Trafic écoulé
0,9 E	1	0,47	0,43	0,47
0,9 E	2	0,17	0,16	0,74
0,9 E	3	0,05	0,05	0,85
0,9 E	4	0,01	0,01	0,89
0,9 E	5	0,002	0,00	0,90

Figure 24.8 Le trafic demandé, perdu et écoulé.

Le modèle d'Erlang à attente (Modèle C)

Le modèle à attente suppose que toute demande ne pouvant être satisfaite est mise dans une file d'attente de capacité infinie et sera traitée dès qu'un organe se libère. C'est le cas notamment des processus dans les systèmes relais[2] (routeur...). Cependant, on peut admettre que ce modèle s'applique aussi aux appels entrants des centraux téléphoniques d'entreprise. En effet, dans ces centraux, en cas d'occupation de l'appelé, l'appel entrant n'est généralement pas refusé mais mis en attente. Ce procédé monopolise une ressource en arrivée et n'écoule aucun trafic. Dans le modèle d'Erlang C, la probabilité p_a de mise en attente est donnée par la relation :

$$p_a = \frac{(E^m/m!) \cdot \left(\dfrac{m}{m-E}\right)}{\left(\displaystyle\sum_{k=0}^{k=m-1} E^k/k!\right) + \left[(E^m/m!) \cdot \left(\dfrac{m}{m-E}\right)\right]}$$

24.4.3 Les réseaux en mode paquet

Principe de la modélisation des réseaux

L'échange d'information entre deux applications ou entre une application et un terminal est généralement variable en termes de volume à échanger et de fréquence des échanges. Si l'on prend en compte l'écart de débit entre les systèmes locaux et les liens d'interconnexion, l'organe d'interconnexion du système de transmission (routeur, FRAD[3], modem...) constitue un goulet d'étranglement. Il en résulte que les messages ne seront pas transmis instantanément, ils seront placés dans une file d'attente (queue) avant d'être traités par le système de transmission. En première approximation, on peut modéliser un système de transmission comme étant constitué d'une simple ligne reliant les deux systèmes d'extrémité (figure 24.9).

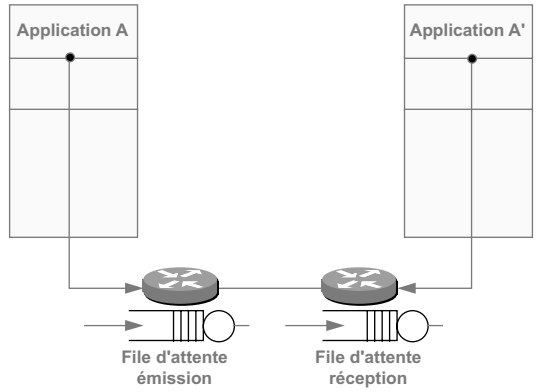


Figure 24.9 La modélisation simplifiée d'un système de transmission.

2. On admettra que les mémoires sont, vis-à-vis du trafic, suffisamment dimensionnées pour être assimilable à une mémoire de capacité infinie.
3. FRAD, *Frame Relay Access Device*.

© Dunod – La photocopie non autorisée est un délit

Le temps de réponse du système pour un message peut s'exprimer par la relation :

$$T_r = T_p + T_t + T_q$$

où T_r est le temps de réponse du système
T_p le temps de propagation sur le support
T_t le temps de traitement par les systèmes d'interconnexion
T_q le temps de séjour dans les systèmes ou temps de queue.

Lorsque le nombre de messages à traiter augmente, T_q devient prépondérant par rapport aux autres éléments, ces derniers pourront alors être négligés. Le problème consiste donc à calculer le temps de queue en fonction des caractéristiques du système (nombre d'items traités par unité de temps ou μ), de la longueur du message (L) et du débit de la ligne du système (D). Il est possible aussi, à partir de ces éléments, de déterminer les caractéristiques du système pour répondre aux contraintes temporelles des applications.

Notions de files d'attente

➤ Relation de base, formule de Little

Dans un système à file d'attente en équilibre (figure 24.10), c'est-à-dire que le nombre moyen d'entrées (λ) est égal au nombre moyen de sorties par unité de temps, le nombre moyen d'items (clients) dans le système N est donné par la formule :

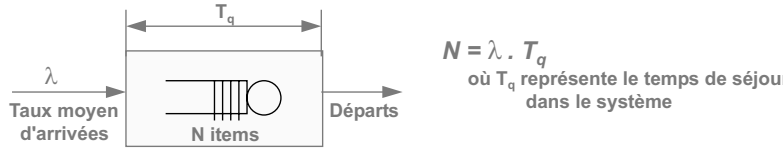


Figure 24.10 La formule de Little.

Si la condition d'équilibre est respectée, la relation de Little s'applique à tous les types de files d'attente.

➤ Les files d'attente M/M/1/∞

Le modèle M/M/1/∞ est le modèle plus simple retenu pour la modélisation des réseaux. Selon la notation de **Kendal**, cette file est caractérisée par :

– **M**, processus Markovien en entrée (distribution exponentielle des arrivées),
– **M**, processus Markovien en sortie,
– **1**, il n'y a qu'un seul processeur (système monoserveur),
– ∞, la file d'attente a une capacité infinie, aucun item entrant n'est perdu.

Dans ce type de processus, on considère les arrivées indépendantes les unes des autres, ce qui est généralement le cas des processus informatiques où les systèmes d'extrémité s'échangent des messages indépendamment les uns des autres.

Dans le système M/M/1/∞ (figure 24.11), on désigne par λ le taux d'arrivée des items dans la file, par t_a le temps de séjour dans la file d'attente, par t_s le temps de traitement par le système (son

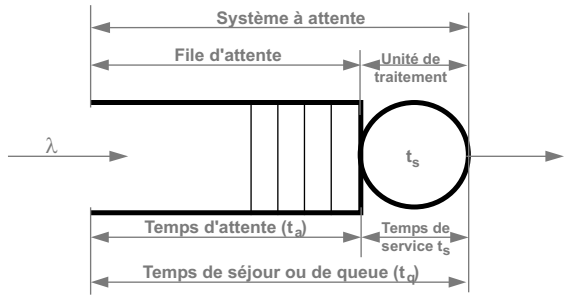


Figure 24.11 La modélisation d'une file M/M/1/∞.

inverse 1/ts représente le nombre d'items traités par unité de temps ou taux de service et est désigné par μ) et $\boldsymbol{t_q}$ le temps qui s'écoule entre l'entrée d'un item dans le système et sa sortie (temps de séjour). Le nombre d'items en attente de traitement ***Na*** et le nombre d'items en cours de traitement ***Ns*** sont une fonction directe du temps d'attente ou de traitement et du taux d'arrivée :

$$Na = \lambda\, t_a$$
$$Ns = \lambda\, t_s$$

Le nombre d'items N dans le système peut s'écrire (décomposition de la formule de Little) :

$$N = Na + Ns = \lambda\,(t_a + t_s) \qquad \text{(relation 1)}$$

Pour tout nouvel entrant dans le système, le temps d'attente correspond au temps nécessaire pour traiter tous les items déjà présents dans la file soit :

$$t_a = N \times t_s \qquad \text{(relation 2)}$$

Dans la relation 1, en remplaçant la valeur de $\boldsymbol{t_a}$ par celle obtenue dans la relation 2 :

$$N = \lambda\,(t_a + t_s) = \lambda\,(N \times t_s + t_s) = N \times \lambda t_s + \lambda t_s$$
$$N - N \times \lambda t_s = \lambda t_s$$
$$N\,(1 - \lambda t_s) = \lambda t_s$$
$$N = \lambda t_s \,/\, (1 - \lambda t_s)$$

Si on pose $\mu = 1/t_s$ (taux de service du système), la charge du système ρ est représentée par la relation :

$$\rho = \lambda/\mu = \lambda t_s$$

on obtient :

$$N = \frac{\rho}{1 - \rho}$$

En reportant cette valeur dans la relation 2, on obtient :

$$t_a = \frac{\rho}{1 - \rho} t_s$$

© Dunod – La photocopie non autorisée est un délit

Le temps de séjour dans le système ou temps de queue est alors :

$$t_q = t_a + t_s = t_s \left(1 + \frac{\rho}{1-\rho}\right) = t_s \left(\frac{1}{1-\rho}\right)$$

Étudions la variation du temps de séjour dans la file d'attente quand la charge du système varie de 10 à 100 % par pas de 10 %.

Le temps de séjour dans la file est relativement faible jusqu'à une charge de 50 %. Au-dessus de cette charge, le temps de séjour croît très vite (figure 24.12). Compte tenu qu'un système n'est généralement étudié que pour un trafic moyen, pour garantir, lors de trafic de crête, des performances acceptables, il convient de le dimensionner pour que la charge moyenne de celui-ci n'excède pas 50 %.

Charge	10 %	20 %	30 %	40 %	50 %	60 %	70 %	80 %	90 %	100 %
$\rho/(1-\rho)$	0,1/0,9	0,2/0,8	0,3/0,7	0,4/0,6	0,5/0,5	0,6/0,4	0,7/0,3	0,8/0,2	0,9/0,1	1/0
ta=ts . $\rho/(1-\rho)$	0,11	0,25	0,42	0,66	1	1,5	2,3	4	9	∞
	Temps d'attente acceptable					Temps d'attente prohibitif				

Figure 24.12 L'évolution du temps de séjour en fonction de la charge.

➤ Application au calcul du débit d'une ligne

En exprimant la charge d'une ligne en fonction des caractéristiques du message (L, longueur en bits) et du système (D, débit de la ligne en bit/s), on obtient :

$$\rho = \frac{\lambda}{\mu} = \frac{\lambda}{\frac{1}{t_s}} = \lambda t_s = \frac{\lambda L}{D}$$

Le temps séjour dans le système ou temps de queue est alors :

$$t_q = t_s \left(\frac{1}{1-\rho}\right) = \frac{L}{D}\left(\frac{1}{1-\frac{\lambda L}{D}}\right) = \frac{L}{D-\lambda L}$$

$$\text{avec } D > \lambda L$$

Mais, compte tenu que nous venons d'établir qu'un système ne doit pas être chargé à plus de 50 %, le débit minimal requis (D_{min}) pour la ligne est de :

$$D_{min} \geqslant 2\,\lambda\,L$$

➤ File d'attente en série

Lorsque deux files d'attente sont en série, si la file d'attente d'entrée est du type M/M/1/∞, les arrivées suivent une loi de Poisson ainsi que les sorties. Dans ces conditions, les entrées de la suivante respectent une loi de Poisson ; cette file est donc aussi poissonienne et de type M/M/1/∞. Le temps de traversée global est la somme des temps de traversée de chacune des files (figure 24.13).

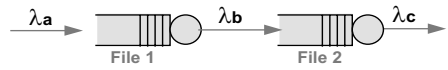


Figure 24.13 Le réseau ouvert de files d'attente en série.

Un réseau peut être modélisé comme une succession de files d'attente, et chaque élément actif du réseau (routeur, commutateur, FRAD...) peut lui-même être considéré comme deux files d'attente en série (figure 24.14).

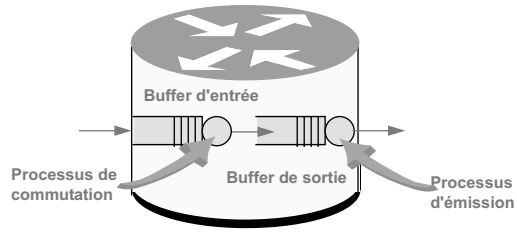


Figure 24.14 La modélisation simplifiée d'un élément actif.

➤ File d'attente à entrées multiples

On montre que, si les messages ont la même longueur moyenne sur toutes les voies incidentes, la file d'attente est équivalente à une file d'attente à une seule entrée où le taux d'arrivée est la somme des taux d'arrivée : $\lambda = \Sigma\ \lambda_i$ (principe de la superposition, figure 24.15).

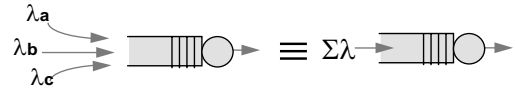


Figure 24.15 La file d'attente à entrées multiples.

Par exemple, une file d'attente à entrées multiples peut correspondre à un nœud intermédiaire sur lequel convergent plusieurs liens

➤ Les files d'attente M/M/1/K

Le modèle M/M/1/∞ considère la file d'attente comme infinie, c'est-à-dire que tout item entrant sera traité, cette hypothèse simplificatrice est satisfaisante dans la majorité des cas. Mais lorsque le réseau est chargé, les files d'attente physiques (tampon ou buffer) n'étant pas de taille illimitée, la probabilité pour qu'un item entrant ne puisse être accepté n'est pas nulle (figure 24.16).

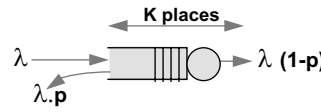


Figure 24.16 La file d'attente à capacité limitée.

© Dunod – La photocopie non autorisée est un délit

Si K est la taille de la file d'attente et que celle-ci contient déjà n items, la probabilité pour qu'un nouvel arrivant soit perdu (p_n) est :

$$\text{si } \rho \neq 1 \quad p_n = \frac{\rho^n(1-\rho)}{1-\rho^{K+1}} \quad \text{avec } 0 \leqslant n \leqslant K$$

$$\text{si } \rho{=}1 \quad p_n = \frac{1}{K+1} \quad \text{avec } 0 \leqslant n \leqslant K$$

Application à la modélisation d'un réseau

Soit le réseau représenté par la figure 24.17, si on admet que tout item entrant est sortant (système en équilibre), il peut être modélisé simplement en remplaçant chaque élément actif par une file d'attente. Il est alors possible à partir d'un trafic d'entrée (E) de déterminer le comportement du réseau pour les données en transit de E vers S.

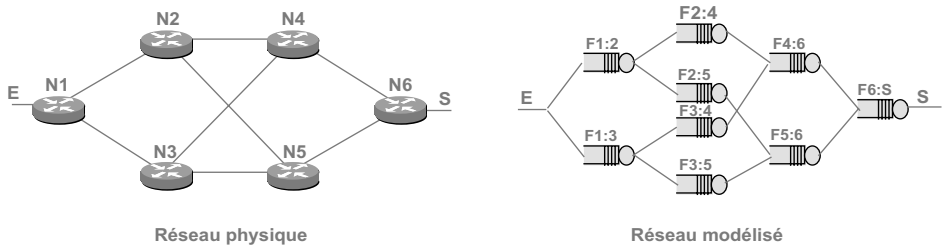


Figure 24.17 La modélisation d'un réseau.

Pour définir le comportement global du réseau, il faut quantifier le trafic entre tous ses points d'entrée et de sortie (matrice de trafic). En superposant chacun des trafics élémentaires dans chaque file, on en détermine le comportement point à point puis on en déduit le comportement global du système.

24.5 CONCLUSION

Ce chapitre a pour objectif d'initier aux méthodes utilisées pour la réalisation, le dimensionnement et les mesures de performances des réseaux. Ces techniques conduisent à construire des modèles mathématiques de plus en plus élaborés dont l'étude sort du cadre de cet ouvrage. Devant la complexité des réseaux et les exigences des utilisateurs, les modèles deviennent de plus en plus complexes et la recherche de nouvelles techniques de modélisation permanente.

EXERCICES

Exercice 24.1 Service de vidéotex

Une entreprise de vente par correspondance outre les accès Internet continue d'offrir à ses clients un service de prise de commande et de consultation de l'état de celles-ci sur Minitel. Compte tenu de la baisse d'activité de ce service, l'entreprise doit le redimensionner. Les données en prendre en compte sont : une transaction de commande dure en moyenne 2 minutes et on admet qu'à l'heure de pointe il y a 600 demandes de connexion. Pour satisfaire pleinement sa clientèle, l'entreprise désire que le taux de refus, suite d'un manque de ressource, ne soit pas supérieur à 1 %. Le service vidéotex est disponible sur un réseau X.25 et accessible *via* le réseau téléphonique commuté.

1. Combien de circuits virtuels l'entreprise doit-elle souscrire à l'opérateur X.25 ?
2. Dans les conditions établies précédemment, combien de demandes de connexion pourront être formulées en 1 heure, si on admet un taux de refus de 2 % ?

Exercice 24.2 Informatisation d'un magasin

Une chaîne de distribution d'électroménager désire construire une nouvelle surface de vente. Le nouveau magasin sera équipé de terminaux passifs reliés au système informatique central de l'entreprise. Les applications informatiques sont de quatre natures :

- accueil clientèle et vente : des terminaux (terminal point de vente) permettent aux vendeurs de renseigner les clients sur la disponibilité d'un produit, le poste est alors immobilisé une minute environ. Lorsque le client acquiert l'objet (6 fois sur 10 en moyenne), la prise de commande et la mise à jour des stocks monopolisent le poste environ 3 minutes supplémentaires ;
- le poste d'enlèvement des achats sera doté de terminaux pour la consultation de la localisation des objets retirés : l'immobilisation du poste est estimée à une minute par enlèvement (chaque vente donne lieu à enlèvement immédiat) ;
- l'encaissement : on estime qu'il ne doit y avoir jamais plus de cinq clients en attente devant un poste d'encaissement et qu'un client s'impatiente si son temps d'attente, avant traitement, dépasse 10 minutes ; l'opération d'encaissement dure en moyenne 3 minutes ;
- le système comportera en plus les postes comptables au nombre de 2 (1 par agent). Chaque comptable effectue au plus 20 transactions/jour régulièrement réparties dans la journée et travaille 8 heures/jour.

On estime qu'à l'heure de pointe, le jour le plus chargé, 100 clients en moyenne seront renseignés par les vendeurs. On demande :

1. le nombre de terminaux de caisse ;
2. le nombre de terminaux au poste enlèvement, si on admet que dans 80 % des cas, les magasiniers doivent trouver un terminal disponible ;
3. le nombre de terminaux à disposition des vendeurs, compte tenu qu'on estime que dans 95 % des cas, le vendeur doit trouver un terminal disponible ;

4. compte tenu des caractéristiques des applications données par la figure 24.18, déterminer le temps de réponse de l'application. Les différents éléments à prendre en compte pour ce calcul sont :
   – le temps de traitement d'une transaction par le serveur central est de 0,2 s ;
   – les terminaux sont connectés à un concentrateur local par une ligne à 9 600 bit/s ;
   – le magasin est relié au site central par une liaison louée à 64 000 bit/s ;
   – on admettra que les bits de transparence et les données de service (ACK...) accroissent la taille des unités de 20 % ;
   – les grilles d'écran des terminaux points de vente sont organisées de telle manière que l'écran de consultation permette de saisir la vente du produit consulté ou la référence d'un autre produit à consulter (un seul échange pour la consultation suivie d'une vente) ;
   – les saisies s'effectuent sur une grille vierge ou en surcharge sur une grille de réponse. Seuls, les caractères saisis sont transmis ;
   – le temps de saisie n'est pas décompté dans le temps de réponse ;
   – le temps d'affichage des écrans sera considéré comme négligeable.

Terminal	Point de vente	Caisse	Point d'enlèvement	Comptable
Saisie	20c	100c	20c	200c
Réponse ou grille de saisie vierge	800c	500c	600c	800c

Figure 24.18 Les caractéristiques des transactions.

Exercice 24.3 Réalisation d'un réseau privé d'entreprise

Pour remplacer ses abonnements à un réseau public de transport de données dont le débit d'abonnement est actuellement de 19 200 bit/s, une entreprise désire réaliser un réseau privé à partir de liaisons louées (LL) à 64 kbit/s. Le siège est à Paris. Les différentes implantations en province sont : Amiens, Lille, Metz, Nancy, Strasbourg, Rennes, Nantes, La Rochelle, Bordeaux, Toulouse, Clermont-Ferrand, Dijon, Lyon, Marseille et Nice.

1. Déterminez le réseau primaire (sans tenir compte d'aucune contrainte de débit), pour cela, vous utiliserez l'algorithme de Kruskal ;
2. Intégrez une contrainte de débit, en garantissant un débit minimal de 19 200 bit/s à chaque site. C'est-à-dire qu'un nœud de concentration ne doit pas concentrer plus de deux sites. De plus, on souhaite que le nombre de bonds soit au maximum de deux pour chaque site ;
3. Comparez les coûts des deux solutions (l'unité sera le km).

Les distances intersites peuvent être obtenues sur le 36 14 code RLS.

Exercice 24.4 Caractéristique mémoire d'un routeur

Un réseau local est interconnecté à un autre réseau *via* un routeur par une ligne à 64 kbit/s. Plusieurs stations sont connectées sur le réseau local. L'analyse de trafic en arrivée montre que :

– 2 stations ont un trafic vers l'extérieur de 4 paquets/s ;

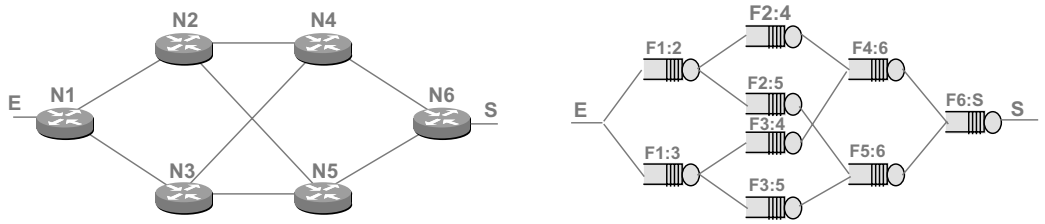
– 2 stations ont un trafic vers l'extérieur de 2 paquets/s ;
– 3 stations ont un trafic vers l'extérieur de 6 paquets/s ;
– 5 stations ont un trafic vers l'extérieur de 5 paquets/s.

Les arrivées suivent une loi de Poisson. Les paquets, en arrivée, ont une longueur moyenne de 128 octets. On ne tiendra pas compte des données protocolaires. Déterminez :

1. le taux d'arrivée (λ) ;
2. le taux de service du routeur (μ) ;
3. l'intensité de trafic ou la charge du système (ρ) ;
4. le nombre moyen de paquets dans le routeur ;
5. le temps moyen d'attente ;
6. le nombre moyen de paquets en attente ;
7. le temps de réponse ;
8. la taille du buffer d'entrée dimensionnée au plus juste pour ce trafic, celle-ci sera arrondie au ko supérieur ;
9. la taille du buffer n'étant plus de longueur infinie, quelle est dans ces conditions la probabilité de rejet d'un nouvel entrant ?

Exercice 24.5 Temps de transit dans un réseau

Le réseau de la figure 24.19 est constitué de liens à 64 kbit/s, il utilise un routage aléatoire, les analyses de trafic montrent que le trafic entrant par le nœud E est en moyenne de 30 paquets par seconde de longueur moyenne de 128 octets. On admettra qu'il n'y a pas d'autre source de trafic dans le réseau. Tout le trafic entrant en E sort en S et se répartit statistiquement comme l'indique la figure 24.19. Déterminez le temps de transit moyen d'un paquet dans le réseau.



Réseau physique — Réseau modélisé

Lien	Proportion du trafic écoulé
N1-N2	75 %
N2-N4	50 %
N3-N5	25 %

Figure 24.19 La modélisation du réseau.

© Dunod – La photocopie non autorisée est un délit

Solutions des exercices

CHAPITRE 1

Exercice 1.1 Code ASCII, algorithme de changement de casse

Dans le code ASCII, pour passer des majuscules aux minuscules, il suffit de rajouter 32 à la valeur du code.

```
---------- Solution en pseudo-code
Tant que le caractère actuel n'est pas la marque de fin de chaîne faire
Début
   | Si le code du caractère n'est pas celui de l'espace alors
   |   | ajouter 32
   | Finsi
   |  passer au caractère suivant
Fin


---------- Solution en langage C
While (*chaine1)
   {
   if (*chaine1!=32)
      (*chaine1)+=32;
   chaine1++;
   }
```

Exercice 1.2 Codage de Huffman

Longueur moyenne du code idéal : l'entropie (H) du système exprime la longueur moyenne du code idéal.

$$H = \sum_{i=1}^{i=n} p_i \log_2 \frac{1}{p_i}$$

$$H = -3{,}32\ (0{,}23 \log_{10} 0{,}23 + 0{,}09 \log_{10} 0{,}09 + 0{,}3 \log_{10} 0{,}3 + 0{,}19 \log_{10} 0{,}19$$
$$+ 0{,}14 \log_{10} 0{,}14 + 0{,}05 \log_{10} 0{,}05) = 2{,}38 \text{ bits}$$

2) Construction de l'arbre de Huffman (figure 1.42)

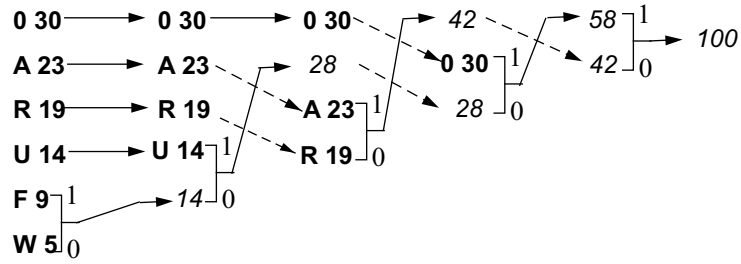


Figure 1.42 Le codage de Huffman.

Le codage résultant est :

$$O = 11\ ;\ A = 01\ ;\ R = 00\ ;\ U = 101\ ;\ F = 1001\ ;\ W = 1000$$

Nombre de bits utilisés pour coder le message de 2 000 caractères :

$$2\,000\ (A \times 0{,}23 + F \times 0{,}09 + O \times 0{,}30 + R \times 0{,}19 + U \times 0{,}14 + W \times 0{,}05)$$

Soit :

$$2 \times 460 + 4 \times 180 + 2 \times 600 + 2 \times 380 + 3 \times 280 + 4 \times 100 = 4\,840 \text{ bits}$$

3) Longueur moyenne du mot code :

$$4\,840/2\,000 = 2{,}42 \text{ bits}$$

Remarquons que cette longueur est proche de celle du codage idéal.

4) Taux de compression par rapport au code Baudot : le code Baudot est un code de longueur fixe à cinq moments. Le taux de compression (τ) vaut :

$$\tau = 2{,}42 / 5 = 0{,}484$$

5) Temps de transmission

Temps de transmission (t) du message :

En ASCII (7 bits) t = Volume/débit = $2\,000 \times 7 / 4\,800 = 2{,}91$ s
Codé Huffman t = Volume/débit = $4\,840 / 4\,800 = 1{,}008$ s

Remarquons que le temps calculé pour la transmission en Huffman ne prend pas en compte l'envoi du dictionnaire.

Exercice 1.3 Télécopieur

À partir de la figure 1.43, établissons les statistiques d'utilisation de chaque groupement de pixels. Pour simplifier la résolution, à chaque séquence de blancs ou de noirs, nous associerons une lettre.

Groupement de	Nb occurrences Blanc		Nb occurrences Noir	
1 pixel	6	A	32	E
2 pixels	14	B	4	F
3 pixels	16	C	5	G
4 pixels			2	H
5 pixels	2	D		

Figure 1.43 Tableau des occurrences d'apparition des groupements de pixels.

Le code de Huffman résultant est déduit de la figure 1.44.

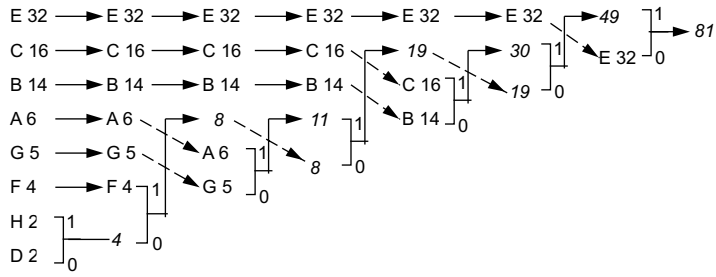


Figure 1.44 L'arbre de Huffman.

Pour obtenir le code de Huffman de chaque symbole, il suffit de lire, de la racine à la feuille, les valeurs binaires inscrites. Ces valeurs sont indiquées dans la figure 1.45.

Groupement de	Blancs		Noirs	
1 pixel	1011	A	0	E
2 pixels	110	B	1001	F
3 pixels	111	C	1010	G
4 pixels			10001	H
5 pixels	10000	D		

Figure 1.45 La table de codage.

Remarques : compte tenu de la petitesse de l'échantillon d'écriture utilisé pour cet exercice, le codage de Huffman est plus volumineux qu'un simple codage de « 1 » pour un point noir et de « 0 » pour 1 point blanc !

L'arbre a été construit à partir des occurrences et non des statiques, ce qui donne évidemment le même résultat.

© Dunod – La photocopie non autorisée est un délit

Exercice 1.4 Numérisation du son

1) Débit binaire nécessaire

CD audio $44{,}1 \cdot 10^3 \times 16 = 705{,}6$ kbit/s
DVD audio $192 \cdot 10^3 \times 24 = 4{,}608$ Mbit/s
SACD $2{,}8224 \cdot 10^6 \times 1 = 2{,}8224$ Mbit/s

2) Volume à stoker pour une heure de musique

1 kilo-octet (ko) = 1 024 octets
CD audio $705{,}6 \cdot 10^3 \times 3\,600 / (8 \times 1\,024) = 310\,078{,}125$ ko = 302 Mo
DVD $4{,}608 \cdot 10^6 \times 3\,600/8 \times 1\,024) = 2\,025\,000$ ko = 1 0977,53 Mo = 1,9311 Go
SACD $2{,}8224 \cdot 10^6 \times 3\,600/8 = 1\,240\,312{,}5$ ko = 1 211,24 Mo = 1,182 Go

Ces résultats concernent une voie, il est nécessaire de les multiplier par deux pour des enregistrements en stéréophonie.

Exercice 1.5 Numérisation et débit binaire

1) Détermination du débit : la fréquence minimale d'échantillonnage étant le double de la fréquence maximale du signal à discrétiser cette fréquence est de :

Information de luminance (Y) $F_{echy} = 6{,}75 \times 2 = 13{,}5$ MHz
Informations de chrominance (Db et Dr) $F_{echc} = 13{,}5$ MHz/2

Le nombre total d'échantillons quantifiés est de :

$$13{,}5 \cdot 10^6 + 2\,(13{,}5 \cdot 10^6/2) = 27 \cdot 10^6 \text{ échantillons}$$

En quantifiant chaque échantillon sur 8 bits le débit nécessaire est de :

$$27 \cdot 10^6 \times 8 = 216 \text{ Mbit/s}$$

2) Nombre de couleurs : les informations de couleur sont quantifiées sur 8 bits soit 256 niveaux pour chacune des trois primaires. Dans ces conditions le nombre de couleurs reproductibles est de :

$$\text{Nombre de couleurs} = 256^3 \text{ soit 16 millions de couleurs}$$

Exercice 1.6 Rapport signal sur bruit et loi de quantification A

Le signal de base est quantifié dans une représentation logarithmique à sept segments (ligne 1 de la figure 1.46). Chaque segment est divisé en seize intervalles égaux (ligne 2). Cependant, l'amplitude représentée par chaque segment double pour chaque segment, sauf les deux premiers (ligne 3).

Ainsi, par exemple le segment 5 s'étend sur 256 niveaux (ligne 3) pour un intervalle de définition total de 2 048 échelons (11 bits) ; l'amplitude de chaque échelon quantifié est donc dans le rapport 256/16 (256 niveaux codés sur 16, ligne 4 du tableau). Si on admet que l'erreur de quantification maximale correspond à un demi-intervalle de quantification, on en déduit que pour les deux premiers segments cette erreur est de 0,5 ; pour le segment 3 elle est de 1... Si on prend comme signal

de référence la valeur centrale de chaque segment (ligne 6), on établit la valeur du rapport signal sur bruit (ligne 7).

Sans prétendre à la rigueur mathématique, cet exercice illustre de façon simple l'intérêt de la loi de quantification logarithmique qui permet un rapport signal sur bruit pratiquement indépendant de l'amplitude du signal.

Segment	0	1	2	3	4	5	6	7
Codage	0-15	16-31	32-47	48-63	64-79	80-95	96-111	112-127
Amplitude (11 bits)	0-15	16-31	32-63	64-127	128-255	256-511	512-1023	1024-2047
Amplitude d'un échelon	16/16 = 1	16/16 = 1	32/16 = 2	64/16 = 4	128/16 = 8	256/16 = 16	512/16 = 32	1024/16 = 64
Erreur de quantification	0,5	0,5	1	2	4	8	16	32
Signal de référence	8	24	48	96	192	384	768	1536
S/B	16	48	48	48	48	48	48	48

Figure 1.46 La loi de quantification A.

Exercice 1.7 Image RVB

La télévision numérique transmet le signal de luminance (Y) en pleine bande (720 points/ligne) et les informations de différence de couleur (Dr et Db) en demi-bande (360 points/ligne). Le nombre de points quantifiés est donc de 1 440 points/ligne. En mode RVB, les détails de l'image sont apportés par chaque information (720 points/ligne). Le nombre de points transmis par ligne est donc 2 160 points/ligne (720 $\times$ 3).

Le mode Y, Dr, Db réalise donc une compression. Le taux de compression[1] (τ) de celle-ci vaut :

$$\tau = 1\,440 / 2\,160 = 0{,}66$$

Exercice 1.8 Type de flux voix et données (data)

La voix est un flux isochrone et les informations de voix doivent être traitées en séquence. La voix peut être considérée comme un flux temps réel, c'est-à-dire que les informations fournies par la source doivent immédiatement être traitées par le récepteur au temps de transmission et de traitement près. Pour respecter ceci, il convient que les temps de transmission et de traitement soient identiques pour tous les éléments d'information (flux isochrone). Enfin, les informations doivent être traitées en séquence, la reprise sur erreur dans de telles conditions impliquerait un silence en l'attente des informations retransmises, une mise en mémoire tampon (bufferisation) de ces informations par la source et un décalage temporel dans le traitement en réception de celles-ci. La reprise sur erreur est donc incompatible avec les flux voix ; d'ailleurs l'oreille humaine ne

1. Rappelons qu'en toute rigueur, la grandeur « taux de compression » n'a de signification qu'en cas de compression sans perte.

© Dunod – La photocopie non autorisée est un délit

discernera pas les informations erronées si celles-ci ont une durée inférieure à un phonème (30 à 50 ms). Il n'en est pas de même pour les flux de type données, ou la validité de l'information prime sur les temps de transmission et de traitement.

CHAPITRE 2

Exercice 2.1 Notion de décibel

Le rapport exprimé en décibel de A sur B est donné par la relation :

$$A/B_{\text{dB}} = 10 \log_{10} (A/B)$$

Remarquons que si $A = 2B$, on a le rapport $A/B_{\text{dB}} = 10 \log_{10} (2/1) = 10 \times 0{,}3 = 3$ dB. 3 dB est une valeur caractéristique qui représente un rapport de moitié (–3 dB) ou du double (3 dB) des grandeurs comparées. La figure 2.38 fournit les résultats de l'exercice.

Valeur en décibel	Rapport en nombre naturel
3 dB	2
10 dB	log (A/B) = 1 ⇒ A/B = 10^1 soit 10 Le logarithme d'un nombre est le nombre par lequel il faut élever la base pour retrouver ce nombre.
100 dB	log (A/B) = 10 ⇒ A/B = 10^{10}
103 dB	À chaque fois que l'on ajoute 3 dB (100+3), on double le rapport. Soit : 2 · 10^{10}
77 dB	77 dB = 80 – 3 ⇒ A/B = 10^8 / 2

Figure 2.38 Les grandeurs réelles et les décibels.

Exercice 2.2 Portée d'une liaison hertzienne

Portée théorique : les faisceaux hertziens utilisent la propagation par onde directe ou propagation à vue. Dans ces conditions, la limite de portée correspond au moment où le faisceau est tangent à la Terre (figure 2.39).

Si on ne considère qu'un seul triangle, on peut écrire :

$$(R + h)^2 = d^2 + R^2$$

Soit :

$$d^2 = (R + h)^2 - R^2 = h^2 + 2Rh$$

Avec $h^2 \ll 2Rh$ (R = 6 300 km, et h quelques mètres) d'où :

$$d^2 = 2Rh \Rightarrow d = \sqrt{2Rh} = \sqrt{2R}\sqrt{h}$$
$$d = 3{,}6\sqrt{h}$$

avec d en km et h en m

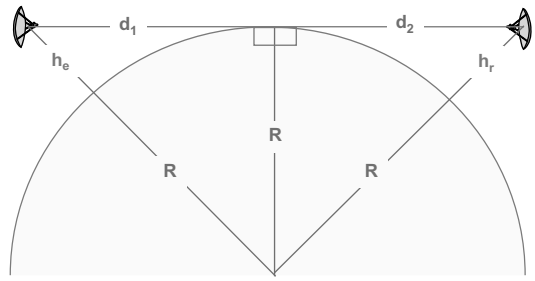


Figure 2.39 Limite de la portée à vue des antennes.

En posant $P = d_1 + d_2$

$$P = 3{,}6\left(\sqrt{h_e} + \sqrt{h_r}\right)$$

avec P portée optique de la liaison en kilomètres,
h_e, h_r hauteur en mètres au-dessus de l'horizon,
des antennes d'émission et de réception.

Portée de l'émetteur de la tour Eiffel : la tour Eiffel (312 m) abrite depuis 1956 des antennes d'émission de télévision, celles-ci sont situées à 318 m du sol.

$$P = 3{,}6\left(\sqrt{h_e} + \sqrt{h_r}\right) = 3{,}6\left(\sqrt{318} + \sqrt{10}\right) = 75 \text{ km}$$

Exercice 2.3 Puissance de réception

1) Densité de puissance à 10 m : la puissance d'émission est « uniformément répartie » à la surface de la sphère.

– Surface de la sphère $S = 4\,\pi\,R^2 = 3{,}14159 \times 4 \times 10 \times 10 = 12{,}566 \cdot 10^2$ m^2
– Densité de puissance $D = P / S = 100 \cdot 10^{-3} / 12{,}566 \cdot 10^2 = 7{,}9 \cdot 10^{-5}$ W

2) Puissance recueillie par l'antenne : $P = D \cdot Sa = 7{,}9 \cdot 10^{-5} \times 10^{-2} = 7{,}9 \cdot 10^{-7}$ W

Exercice 2.4 Bande passante d'une fibre optique

Dans une fibre multimode, pour une impulsion émise, N impulsions sont reçues suivants les N trajets empruntés (figure 2.40). Pour distinguer deux bits successifs, il faut que les N impulsions du bit précédent soient arrivées. Le temps séparant l'émission de 2 bits successifs doit donc être au minimum égal au temps s'écoulant entre la réception de l'impulsion ayant parcouru le plus faible trajet (I_1) et celle ayant parcouru la plus grande distance (I_n).

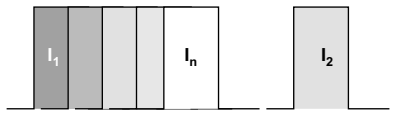


Figure 2.40 Les impulsions successives dues aux multiples trajets.

© Dunod – La photocopie non autorisée est un délit

Il faut donc calculer le temps qui sépare l'arrivée des deux impulsions extrêmes (multimode). Pour cela, déterminons la différence de trajet. L'ouverture numérique correspond à l'angle limite des rayons incidents (θ_1), elle permet de calculer le trajet le plus important (figure 2.41).

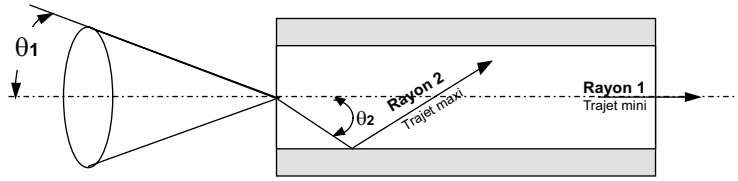


Figure 2.41 Les trajets dans la fibre.

1) Calcul de la bande passante pour une longueur d'un km

– *Calcul de l'angle de réfraction* : l'angle maximal d'acceptance et l'ouverture numérique sont liés par la relation :

$$ON = \sin \theta_1$$

$$\text{Or} \quad n_0 \sin\theta_1 = n_1 \sin\theta_2,$$

avec à l'interface air/cœur de la fibre
n_0 indice de réfraction de l'air soit 1,
n_1 indice de réfraction du cœur de la fibre soit 1,465.

Dans ces conditions, dans la fibre on peut écrire :

$$\sin\theta_1 = n_2 \sin\theta_2 \quad \text{soit} \quad \sin \theta_2 = \sin \theta_1 / n_2 = 0{,}22 / 1{,}465 = 0{,}1501$$

ce qui donne un angle de réfraction de 8°.

– *Détermination du trajet maximal* : les rayons R_1 et R_2 sont liés par la relation :

$$R_1 = R_2 \cos \theta_2$$

$$R_2 = R_1 / \cos \theta_2$$

Soit, pour un trajet R_1 de 1 km, un trajet R_2 de :

$$R_2 = 1/ \cos \theta_2 = 1\,000 / 0{,}990 = 1\,010 \text{ m}$$

soit une différence de trajet (ΔD) de 10 m.

La différence de temps de trajet (Δt) est de :

$\Delta t = \Delta D/v$ où v est la vitesse de la lumière dans la fibre optique

$$\Delta t = 10 / 2 \cdot 10^8 = 5 \cdot 10^{-8} \text{ s}$$

– *Calcul de la bande passante* : le temps calculé précédemment représente l'écartement minimal nécessaire (cadence d'émission maximale) entre deux bits du trajet R_1 soit une bande passante (BP) maximale de :

$$\text{BP} = 1 / 5 \cdot 10^{-8} = 20 \text{ Mbit/s}$$

2) Détermination de n_2 : rappelons que l'ouverture numérique et les indices de réfraction sont liés par la relation :

$$ON = \sqrt{n_1^2 - n_2^2}$$

Avec $ON = 0{,}22$ et $n_2 = 1{,}465$ on obtient :

$$n_1 = \sqrt{n_2^2 - ON^2} = \sqrt{2{,}146 - 0{,}484} = 1{,}448$$

Exercice 2.5 Conversion de l'expression d'une puissance

La puissance exprimée en dBmW est donnée par la relation :

$$P_{\text{dB}} = 10 \log_{10} (P_2/P_1) \text{ avec } P_1 \text{ puissance de référence et valant un mW}$$

Soit :

$$2 = 10 \log_{10} (P_2)$$

$$0{,}2 = \log_{10} (P_2) \text{ ce qui donne } P_2 = 1{,}58 \text{ mW}$$

Exercice 2.6 Caractéristique d'une ligne

1) Niveau minimal du signal à l'extrémité de la ligne : la puissance (P) et la tension (U) sont reliées par la relation :

$$P = U^2 / R \quad \text{soit} \quad U^2 = P \cdot R \quad \text{d'où} \quad U = \sqrt{P \cdot R}$$

avec $P = 1$ mW et $Rc = 600\ \Omega$ on obtient :

$$U = \sqrt{(10^{-3} \times 600)} = 0{,}775 \text{ V}$$

Si l'on prend 1 mW comme puissance de référence, la tension de référence permettant d'effectuer la conversion de tension, est égale à 0,775. L'indication absolue s'exprime alors en dBm (dBmW). Les relations de base sont alors :

Rapport en puissance	$10 \log_{10} P$ / 1 mW (dBm)
Rapport en tension	$20 \log_{10} U$ / 0,775 (dBm)

Ces relations ne sont applicables que si le récepteur a une impédance de 600 Ω.

Attention : ne pas confondre avec dBV = $20 \log_{10} (E_2 / E_1)$ (dB volt) qui exprime la valeur d'une tension par rapport à une valeur de référence, ici E_1 volt.

Remarquons que 43 dB = 40 dB + 3 dB, cette décomposition facilite la résolution du problème ; en effet, une variation de 3 dB correspond à un rapport de deux en puissance et de $\sqrt{2}$ en tension.

Soit – 40 dB = $10 \log_{10} P$ soit $-4 = \log_{10} P$, ce qui donne P = 10^{-4} mW ce qui correspond à 0,00775 V.

Dans ces conditions, – 43 dB correspondent à $0{,}00775/\sqrt{2} = 0{,}00549$ V.

© Dunod – La photocopie non autorisée est un délit

2) L'affaiblissement entre deux points A et B est donné par la relation

$$\text{A en dB} = 20 \log_{10} E_B / E_A$$

Qui représente l'affaiblissement en tension du signal au point B par rapport au signal mesuré au point A.

$$\text{D'où} \quad A = 20 \log_{10} (9 / 90) = 20 \log_{10} 0{,}1 = 20 \times (-1) = -20 \text{ dB}$$

Remarque : les téléphonistes utilisent aussi le dBmp, qui signifie dBm psophométrique ; c'est l'unité de mesure de niveau à travers un filtre psophométrique (filtre aux caractéristiques liées à la sensibilité de l'oreille, utilisé pour des mesures de niveau de bruit).

Exercice 2.7 Effet Doppler

L'écart de fréquence résultant de l'effet Doppler est donné par la relation :

$$\Delta F = f_0 \frac{v}{c} \cos \alpha$$

où ΔF est l'écart de fréquence,

f_0 la fréquence porteuse,

v la vitesse du mobile,

c la vitesse de propagation des ondes dans l'air admise comme étant égale à la vitesse de la lumière dans le vide, la lumière n'étant qu'un cas particulier des ondes électromagnétique ($c = 3 \cdot 10^8$ m/s).

1) Déplacement en voiture à 100 km/h

– Effet sur la porteuse $\Delta F = f_0 \frac{v}{c} \cos \alpha = 1800 \cdot 10^6 \frac{10^5}{3600 \times 3 \cdot 10^8} = 166 \text{ Hz}$

– Effet sur la voix $\Delta F = f_0 \frac{v}{c} \cos \alpha = 10 \cdot 10^3 \frac{10^5}{3600 \times 3 \cdot 10^8} = 0{,}0009 \text{ Hz}$

2) Déplacement en TGV à 300 km/h

– Effet sur la porteuse $\Delta F = f_0 \frac{v}{c} \cos \alpha = 1800 \cdot 10^6 \frac{3 \cdot 10^5}{3600 \times 3 \cdot 10^8} = 500 \text{ Hz}$

– Effet sur la voix $\Delta F = f_0 \frac{v}{c} \cos \alpha = 10 \cdot 10^3 \frac{3 \cdot 10^5}{3600 \times 3 \cdot 10^8} = 0{,}00027 \text{ Hz}$

Dans les deux cas l'effet sur la voix est insignifiant. Cependant la dérive de fréquence de la porteuse est plus sensible.

CHAPITRE 3

Exercice 3.1 Organisation des échanges

La figure 3.72 décrit succinctement les modes d'échange et fournit un exemple pour chacun d'eux.

Mode d'échange	Communication	Exemple
Simplex	1 seul sens (diffusion)	Radiodiffusion
Half duplex	Dans les deux sens successivement	CB (*Citizen Band*)
Full duplex	Dans les deux sens simultanément	Téléphone

Figure 3.72 Les modes d'échange.

Exercice 3.2 Transmission parallèle

Dans une *transmission parallèle*, lorsque le retour est commun il faut autant de fils que de bits à acheminer plus 1 pour le retour, soit dans notre cas 33 conducteurs. Si le retour n'est pas commun, chaque bit nécessite 2 fils, soit 64 conducteurs. Une *transmission série* n'aurait nécessité que deux conducteurs.

Exercice 3.3 Transmission synchrone et asynchrone

Lorsque le signal d'horloge de l'émetteur est transmis ou que celui-ci est déduit des données transmises, on parle de *transmission synchrone*. Sinon, la transmission est dite *asynchrone*. La figure 3.73 illustre les liaisons entre un ETTD (DTE) et son ETCD (DCE) dans les deux cas.

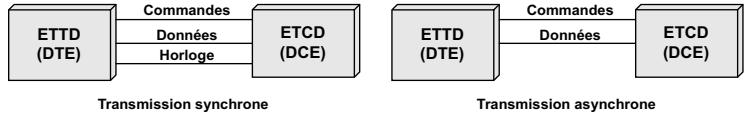


Figure 3.73 Liaison asynchrone et liaison synchrone.

Exercice 3.4 Efficacité

La trame PPP (figure 3.74) comporte huit octets de service[2] (deux fanions d'un octet, un octet pour le champ adresse, un pour le champ contrôle, deux pour le champ protocole et deux pour le champ FCS) pour une charge utile de 1 500 octets d'information (*payload*).

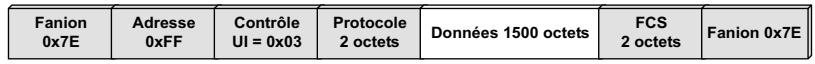


Figure 3.74 Trame PPP.

L'efficacité dans le mode synchrone correspond au rapport du nombre d'octets utiles au nombre d'octets transmis, soit :

$$Eff = \frac{1500}{1508} = 0{,}994$$

2. Pour la signification de chacun de ces champs voir chapitre 4.

© Dunod – La photocopie non autorisée est un délit

En mode asynchrone, il faut ajouter un bit de start et un bit de stop à chaque octet, soit 10 bits pour 8 d'utiles. L'efficacité dans ces conditions est :

$$Eff = \frac{1500 \times 8}{1508 \times 10} = 0{,}795$$

Attention : les termes synchrone et asynchrone ont, selon ce qu'ils qualifient, des significations différentes. Un tableau en annexe résume les différentes utilisations de ces termes dans le monde des télécommunications.

Exercice 3.5 Éléments d'accès au réseau

La figure 3.75 rappelle le schéma de principe d'une liaison de transmission de données. Le DTE (ETTD) traite les données. Le format interne de représentation électrique des données n'est pas adapté aux supports de transmission. Il est nécessaire de réaliser une adaptation, c'est le rôle du DCE.

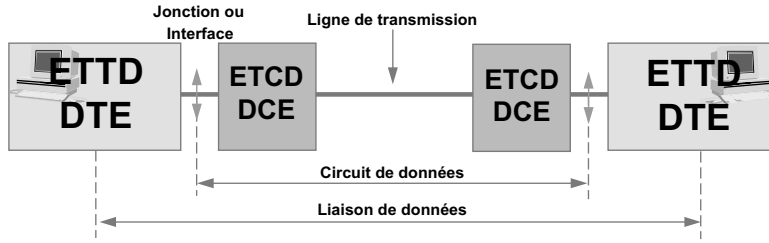


Figure 3.75 Éléments de liaison de données.

Par conséquent, la réponse à la question est non, il est nécessaire d'intercaler un DCE entre le DTE et la ligne.

Exercice 3.6 Transmission asynchrone

La durée d'un bit correspond à une période d'horloge soit une milliseconde.

Durant cette période l'horloge dérive d'un centième soit :

$$1 \text{ ms} \times 10^{-2} = 0{,}01 \text{ ms/période}$$

Si la dérive acceptable est de 10 % d'un temps bit, la dérive maximale peut aller jusqu'à :

$$1 \text{ ms} \times 0{,}1 = 0{,}1 \text{ ms}$$

Ce qui correspond à :

Nombre de bits = Dérive maximale/dérive par temps d'horloge,
Nombre de bits = 0,1/0,01 = 10 bits.

Exercice 3.7 Durée d'un transfert d'information

La sauvegarde ne peut avoir lieu que lorsque tous les traitements sont terminés, c'est-à-dire dans le créneau 22 h 00-6 h 00 soit durant une période de 8 h 00.

1) Durée de la transmission à 2,048 kbit/s

– Volume de données : $10 \cdot 10^9 \times 8 = 80 \cdot 10^9$ bits
– Durée de la transmission $80 \cdot 10^9$ / $2{,}048 \cdot 10^6$ = 390 625 s soit 10 h 51 min

La transmission ne peut être réalisée durant le temps imparti.

2) Les solutions envisageables

– disposer d'un raccordement à débit plus élevé et si 2,048 Mbit/s est le débit maximal réalisable sur un raccordement, utiliser plusieurs (2) raccordements en parallèle ;
– ne faire qu'une sauvegarde incrémentielle, c'est-à-dire ne sauvegarder que les données qui ont été modifiées ;
– réaliser la sauvegarde localement sur un support magnétique et transférer le support par voie normale (routière ou autre) au site de *backup*.

Exercice 3.8 Caractéristiques d'un modem

1) Valence du signal : un signal à huit états ou phases et à deux niveaux par phase correspond à une représentation de 16 valeurs.

2) Rapidité de modulation du signal envisageable sur le canal :

$$R = 2 \cdot BP = 2 \times (2\,900 - 500) = 4\,800 \text{ bauds}$$

La rapidité de modulation utilisée indique le nombre de changements d'état du signal ; dans le cas présent, 16 états sont possibles par temps élémentaire. Dans ces conditions, si :

$$D = R \log_2 n$$

on obtient $R_{effective}$ = Débit / $\log_2 n$ soit 9 600/4 = 2 400 bauds.

3) Rapport signal sur bruit : la capacité de transmission maximale du canal est donnée par la relation de Shannon :

$$C = BP \log_2 (1 + S/N)$$

Cependant, pour appliquer cette formule ici, il faut tenir compte non pas de la bande passante réelle du circuit, mais de celle utilisée par le modem, ce qui peut s'écrire :

$$C = (R/2) \log_2 (1 + S/N)$$

avec $C_{(capacité)}$ = 9 600 bit/s et $R_{(effective)}$ = 2 400 bauds

$$\log_2 (1 + S/N) = 9\,600 / 1\,200 = 8$$

© Dunod – La photocopie non autorisée est un délit

d'où $2^8 = 1 + S/N$

$$S/N = 256 - 1 = 255$$

On aurait pu directement appliquer $n = \sqrt{(1 + S/N)}$, ce qui aurait évidemment donné le même résultat.

Soit un rapport signal sur bruit (S/N) limite de 255.

Exercice 3.9 Débit possible sur un canal TV

Rapidité de modulation : $R = 2 \times \text{BP}$

$$R_{max} = 2 \times 6 \text{ MHz} = 12 \text{ Mbauds}$$

Le canal est susceptible d'admettre une capacité de modulation de 12 Mbauds. Compte tenu de l'utilisation d'un signal de valence 4, le débit possible est :

$$D = R \log_2 (n) = 12 \cdot 10^6 \times \log_2 (4) = 24 \cdot 10^6 \text{ bit/s}$$

Exercice 3.10 Rapport Signal/Bruit

Détermination du rapport Signal/Bruit (S/N, *Signal/Noise*) en dB :

$$S/B_{\text{dB}} = 10 \log_{10} (S/N)$$

$$30 \text{ dB} = 10 \log_{10} (S/N)$$

$$\log_{10} (S/N) = 30 / 10 = 3$$

Le logarithme d'un nombre est le nombre par lequel il faut élever la base pour retrouver ce nombre soit : $X = 10^3 = 1\,000$.

Le rapport signal sur bruit en grandeur réelle est donc de 1 000.

En appliquant la relation de Shannon :

$$\text{C} = \text{BP} \times \log_2 (1 + S/N)$$

$$\text{C} = 3\,100 \times \log_2 (1\,000) \quad \text{en effet} \quad (1 + 1\,000) \approx 1\,000$$

Pour mémoire, rappelons une solution simple de conversion de logarithme en base 10 en logarithme en base 2 :

$$\log_2 x = N \log_{10} x \quad \text{soit} \quad N = \log_2 x / \log_{10} x$$

$$\text{avec} \quad x = 2, \quad N = 1 / \log_{10} 2 = 1 / 0{,}30109 = 3{,}32$$

Soit :

$$\text{C} = 3\,100 \times 3{,}32 \times \log_{10} (1\,000)$$

$$\text{C} = 3\,100 \times 3{,}32 \times 3 = 30\,876 \text{ bit/s}$$

La capacité maximale théorique du canal est donc de 30 876 bit/s.

Remarque : une solution plus simple aurait été d'admettre que $\log_2 (1\,000) = 10$. L'erreur est minime puisque $2^{10} = 1\,024$.

Exercice 3.11 Null modem

Signaux à câbler

N° de circuit	Appellation	Fonction
102	*Signal Ground* (SG)	Terre de signalisation ou retour commun.
103	*Transmitted Data* (TD)	Circuit par lequel l'ETTD transmet les données à émettre.
104	*Receive Data* (RD)	Circuit par lequel l'ETCD transmet à l'ETTD les données qu'il a reçues.
105	*Request To Send* (RTS)	Circuit par lequel l'ETTD demande à l'ETCD de se mettre en position de recevoir des données à transmettre.
107	*Clear To Send* (CTS)	En réponse au 105, l'ETCD répond qu'il est connecté à la ligne et prêt à émettre des données.
108	*Data Set Ready* (DSR)	L'ETTD demande à l'ETCD de se connecter à la ligne.
109	*data Carrier Detect* (CD)	L'ETCD signale qu'il reçoit un signal (porteuse) conforme à son attente.

Figure 3.76 Signaux à gérer.

Réalisation du câble : la réalisation d'un câble de connexion directe entre deux ETTD n'est pas aussi simple qu'il peut y paraître. En effet, il faut envisager plusieurs modes de fonctionnement et donc plusieurs solutions de câblage. La figure 3.77 représente le cas le plus simple. Dans ce mode de fonctionnement aucun contrôle n'est réalisé, les seuls circuits à câbler sont le 103, 104 (en les croisant) et le 102 (terre de signalisation).

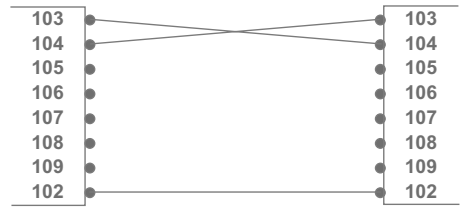


Figure 3.77 Éliminateur de modems.

L'étape suivante consiste à fournir à l'ETTD les réponses qu'il attend de l'ETCD. Pour cela, il faut boucler le 108 et le 107 (réponse au 108) ainsi que le 105 et le 106 (réponse au 105). Reste à résoudre le problème du 109. Le 109 est activé quand l'ETCD reçoit la porteuse du distant. Cette porteuse a été envoyée suite à la levée du 105. Par conséquent, le 105 local sera raccordé au 109 distant (figure 3.78).

D'autres solutions sont envisageables selon le contrôle de l'interface que l'on désire réaliser. La solution présentée ci-dessus n'est qu'une parmi d'autres possibles.

© Dunod – La photocopie non autorisée est un délit

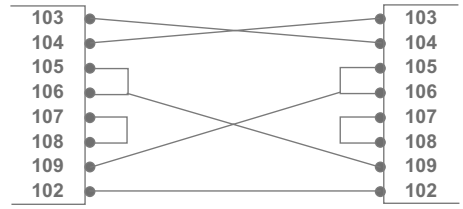


Figure 3.78 Exemple de câble null modem.

Exercice 3.12 Contrôle de flux matériel

Lors de l'échange de données entre l'ETTD et l'ETCD, la mémoire tampon (*buffer*) de l'un ou de l'autre peut être pleine et par conséquent, si de nouvelles données sont envoyées, elles seront perdues. En positionnant les signaux RTS (105, ETTD prêt) et CTS (106, ETCD prêt) à OFF, l'ETTD ou l'ETCD informe l'autre qu'il ne peut plus accepter de données. Cette technique de contrôle du débit à l'interface s'appelle contrôle de flux matériel. La figure 3.79 représente un câble gérant les signaux RTS/CTS.

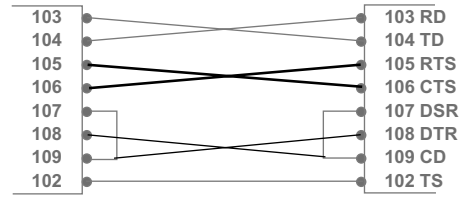


Figure 3.79 Contrôle de flux matériel et null modem.

Exercice 3.13 Modem dissymétrique

1) Rapport signal sur bruit : la figure 3.80 indique les éléments générateurs de bruit à prendre en compte dans chaque sens de la liaison :

Usager ⟶ Entreprise	Ligne analogique	Codec	RTPC	Ligne numérique
Entreprise ⟶ Usager	Ligne analogique		RTPC	Ligne numérique

Usager ⟶ Entreprise	$2 \cdot 10^5$	$1 \cdot 10^3$	$1 \cdot 10^8$	$2 \cdot 10^5$
Entreprise ⟶ Usager	$2 \cdot 10^5$		$1 \cdot 10^8$	$2 \cdot 10^5$

Figure 3.80 Éléments de la liaison.

a) S/B Usager ⟶ Entreprise $[S/B]^{-1} = 0{,}5 \cdot 10^{-5} + 10^{-3} + 10^{-8} + 0{,}5 \cdot 10^{-5} = 10^{-3}$
b) S/B Entreprise ⟶ Usager $[S/B]^{-1} = 0{,}5 \cdot 10^{-5} + 10^{-8} + 0{,}5 \cdot 10^{-5} = 10^{-5}$

2) Caractéristiques de la liaison

a) *Rapidité de modulation* : la bande passante étant la même dans les deux sens, la rapidité de modulation est identique :

$$R = 2 \text{ BP} = 2 \times 3\,400 = 6\,800 \text{ bauds}$$

b) *Débit maximal dans chacun des deux sens :* rappelons que le débit maximal ou capacité du support est fonction de la bande passante et du rapport signal sur bruit du lien :

$$C = \text{BP} \log_2 (1 + S/B)$$

Usager ⟶ Entreprise $C = 3\,400 \times 3{,}32 \log_{10} 10^3 = 3\,400 \times 3{,}32 \times 3$
$= 33\,864$ (33 000) bit/s

Entreprise ⟶ Usager $C = 3\,400 \times 3{,}32 \log_{10} 10^5 = 3\,400 \times 3{,}32 \times 5$
$= 56\,440$ (56 000) bit/s

c) *Valence du signal et nombre d'états*

$$D = 2 \text{ BP} \log_2 v \qquad \log_2 v = D / 2 \text{ BP}$$

Usager ⟶ Entreprise $\log_2 v = 33\,000 / 6\,800 = 4{,}85$ soit MAQ 32 (32 états)
Entreprise ⟶ Usager $\log_2 v = 56\,000 / 6\,800 = 8{,}63$
soit MAQ 512 (512 états)

Exercice 3.14 Rapidité de modulation

Le codage du signal dans un réseau 802.3 est en Manchester (biphase), ce type de codage se caractérise par une transition au milieu de chaque temps bit, il y a donc deux états par temps bit ; la rapidité de modulation est le double du débit soit 20 Mbauds.

Autre explication : le codage Manchester correspond à un codage *n*B*m*B. En effet, un 0 correspond à l'émission de 01 (niveau électrique) et un 1 correspond à l'émission de 10 (niveau électrique).

La vitesse de signalisation sur la ligne ou rapidité de modulation est bien le double du débit binaire.

CHAPITRE 4

Exercice 4.1 Calcul de CRC

Le polynôme générateur :

$$x^4 + x^2 + x + 1$$

donne la séquence binaire :

$$1(x^4) + 1(x^2) + 1(x^1) + 1(x^0) \quad \text{soit } 10111.$$

La division est, en réalité, un OU exclusif qui peut être exécuté dans des registres à décalage. Le degré du polynôme générateur étant de 4, on doit ajouter quatre zéros à la trame de données. La

© Dunod – La photocopie non autorisée est un délit

division est représentée ci-après. Le résultat n'est pas exprimé, il est sans intérêt, seul le reste de cette division présente une utilité.

```
1 0 1 0 0 1 0 1 1 1 0 0 0 0 | 1 0 1 1 1
1 0 1 1 1                   | 100 110 0100
0 0 0 1 1 1 0 1             | ce quotient est sans intérêt
      1 0 1 1 1
      0 1 0 1 0 1
        1 0 1 1 1
        0 0 0 1 0 1 0 0
              1 0 1 1 1
              0 0 0 1 1 0 0
```

Le reste, de degré $n - 1$ par rapport au polynôme générateur, est exprimé sur 4 bits. Ce reste est de 1100, le CRC4 est donc de 1100. Le message à transmettre sera :

$$10100101111\mathbf{1100}$$

Vérification :

```
   message     reste
1010010111     1100   | 1 0 1 1 1
10111                 |
00011101              |
   10111              |
   010101             |
     000101    11     |
        101    11     |
        000    0000   |
```

Exercice 4.2 Probabilité de recevoir un message erroné

Si T_e est la probabilité pour qu'un bit soit erroné, la probabilité de recevoir un bit correct est de $(1 - T_e)$; pour un bloc de N bits la probabilité est de $(1 - T_e)^N$. Soit, pour un message de 100 caractères comportant 7 bits/caractère (code CCITT N° 5) :

$$100 \times 8 = 800 \text{ bits (on transmet des octets en entier)}$$

La probabilité P_c de réception d'un bloc correct est de :

$$P_c = (1 - 0{,}0001)^{800} = (0{,}9999)^{800} = 0{,}923$$

La probabilité P_e de recevoir un bloc erroné est donc :

$$P_e = 1 - 0{,}923 = 0{,}077$$

Exercice 4.3 Taux de transfert

1) Taux de transfert d'information sans erreur

L'efficacité du protocole sans erreur est : *Eff* = Nb. bits utiles/Nb. bits transmis

Nombre de bits utiles :

$$1\ 000 \times 7 = 7\ 000 \text{ bits (code CCITT N°5 codé sur 7 bits)}$$

Nombre de bits transmis :

$$1\ 000 \times (7 + 1) = 8\ 000 \text{ bits (7 pour 1 car. + 1 bit de parité)}$$

L'efficacité est de :

$$Eff = 7\ 000/8\ 000 = 0{,}875$$

Le taux de transfert d'information (TTI) est de :

$$\text{TTI} = \text{Débit théorique} \times \text{Efficacité}$$

$$\text{TTI} = 9\ 600 \times 0{,}875 = 8\ 400 \text{ bit/s}$$

2) Taux de transfert d'information en milieu erroné : en milieu erroné, l'efficacité du protocole est le produit de l'efficacité sans erreur et de la probabilité de réception correcte du message. La probabilité de recevoir un message correct de *N* bits pour un taux d'erreur de Te :

$$P = (1 - Te)^N = (1 - 0{,}0001)^{8\,000} = 0{,}9999^{\,8\,000} = 0{,}449$$

Le taux de transfert avec erreur est $\text{TTI}_{\text{avec erreur}} = \text{TTI}_{\text{sans erreur}} \times P$

Soit :

$$\text{TTI}_{(\text{avec erreur})} = 8\ 400 \times 0{,}449 = 3\ 770 \text{ bit/s}$$

Exercice 4.4 Échange de trames HDLC version LAP-B

La figure 4.58 (page suivante) représente l'échange, les commentaires nécessaires à la compréhension de chaque échange sont fournis à la ligne correspondante.

CHAPITRE 5

Exercice 5.1 Intensité de trafic et taux d'activité

Lors de l'étude d'un système d'interconnexion de systèmes informatiques, deux critères essentiels, dépendant du type d'application, sont à prendre en compte :

– l'intensité de trafic qui caractérise la durée de la ou des session(s) ;
– le taux d'activité, qui exprime la proportion de temps d'utilisation la session.

L'intensité de trafic (E) et le taux d'activité (θ) varient de 0 à 1. On peut représenter la relation entre ces valeurs par un carré et déterminer quatre aires spécifiques (figure 5.52).

La figure 5.53 commente ces différentes aires.

© Dunod – La photocopie non autorisée est un délit

Valeur des compteurs après l'échange (après émission et après réception)	A Vs	A Vr	Échange	B Vs	B Vr
Exemples de représentation des trames : Indiquer le type (I, U, S) Éventuellement la trame (REJ, SABME...) Les valeurs des compteurs Nr, Ns La valeur du bit P/F			(I) Ns=4 Nr=6 P=0 ⟶ (S) RNR Nr=3 P=0 ⟵		
Initialisation :	0	0		0	0
1) Ouverture en mode asynchrone normal	0	0	(U) SABM P=0 ou 1 ⟶	0	
2) Acceptation par B	0	0	(U) UA F=0 ou 1 ⟵	0	0
Échange :					
3) Trame d'information de A vers B	1	0	(I) Ns=0, Nr=0 P=0 ⟶	0	1
4) Trame d'information de A vers B erronée	2	0	(I) Ns=1, Nr=0 P=0 ⟶ *non prise en compte*	0	1
5) Trame d'information de A vers B	3	0	(I) Ns=2, Nr=0 P=0 ⟶ *rejet décalage des compteurs*	0	1
6) *La trame précédente à été rejetée* *Demande de retransmission*	1	0	(S) REJ Nr=1 P=0 ⟵	0	1
7) Trame d'information de A vers B	2	0	(I) Ns=1, Nr=0 P=0 ⟶	0	2
8) Trame d'information de A vers B	3	0	(I) Ns=2, Nr=0 P=0 ⟶	0	3
9) Trame d'information de B vers A	3	1	(I) Ns=0, Nr=3 P=0 ⟵	1	3
10) Trame d'information de A vers B	4	1	(I) Ns=3, Nr=1 P=0 ⟶	1	4
11) Trame d'information de A vers B	5	1	(I) Ns=4, Nr=1 P=0 ⟶	1	5
12) Trame d'information de A vers B	6	1	(I) Ns=5, Nr=1 P=0 ⟶	1	6
13) Trame d'information de A vers B	7	1	(I) Ns=6, Nr=1 P=1 ⟶	1	7
14) *Envoi d'un acquittement*	7	1	S) RR Nr=7 F=1 ⟵	1	7
Fermeture de la connexion :					
15) Demande de fermeture			(U) DISC P=1 ⟶		
16) Acquittement par B			(U) UA F= 1 ⟵		

Figure 4.58 Échange LAP-B.

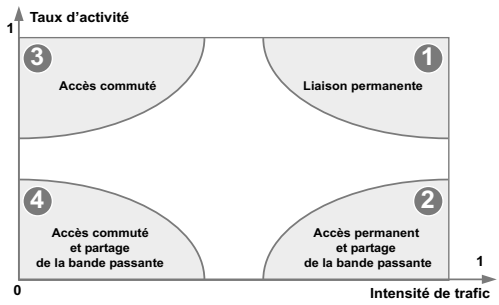


Figure 5.52 Les quatre aires définies par E et θ.

Intensité de trafic (*E*)	Taux d'activité (θ)	Commentaires		Service	Type d'application (exemples)
Voisin de 1	Voisin de 1 Aire 1	La ligne est occupée en permanence, une liaison permanente est nécessaire	La bande est totalement utilisée, tout partage est impossible	LS	Télémesure, Conduite de processus
	Faible Aire 2		La bande offerte est peu utilisée, son utilisation peut être partagée	– Réseau de transmission de données – en local multiplexage concentrateur	Système transactionnel (réservation...), Réseau bancaire
Faible	Voisin de 1 Aire 3	La ligne est faiblement occupée, il n'est pas nécessaire de disposer d'une liaison permanente, un service de commutation est envisageable	Durant l'utilisation de la ligne, la bande est intégralement occupée par le terminal ; aucun partage n'est envisageable	Réseau téléphonique	Transfert de fichiers
	Faible Aire 4		Durant l'utilisation du média, toute la bande n'est pas occupée, une double concentration est envisageable	Accès téléphonique à un réseau de transmission de données	Minitel

Figure 5.53 Rationalisation des moyens.

Exercice 5.2 Application numérique *E* et θ

1) L'intensité du trafic de la ligne

$$E = NT / 3\,600 = 1 \times 10 / 60 = 0{,}166 \text{ erlang}$$

avec N, nombre de session =1
T, durée de la session = 10 mn

2) Le taux d'activité de la ligne

$$\theta = \frac{\text{Durée de l'échange de données}}{\text{Durée de la session}} = \frac{\text{Volume des données échangées}}{\text{Débit} \times \text{Durée de la session}}$$

© Dunod – La photocopie non autorisée est un délit

Soit :

$$\theta = (n \times L) / (D \times T)$$

n = nombre de messages échangés durant la session
L = longueur moyenne des messages exprimée en bits
D = débit effectif du système
T = durée de la session en s

$$\theta = (1 \times 120\,000 \times 8) / (2\,400 \times 600) = 0{,}666$$

3) Type d'application : le taux d'activité est important alors que le taux de connexion est faible. Cette application pourrait être un transfert de fichier utilisant le réseau téléphonique commuté (RTC, 2 400 bits/s).

Exercice 5.3 Trame MIC

1) Fréquence de récurrence d'une trame : la trame MIC est reproduite 8 000 fois par seconde (8 000 Hz) soit une période de 125 μs.

2) Débit d'une voie : la voix est quantifiée sur 256 niveaux soit 8 bits. Le débit, pour une voie, est donc de 8 000 $\times$ 8 = 64 kbit/s

3) Fréquence de récurrence du motif de signalisation : le motif se reproduit une fois toutes les 16 trames, soit 8 000/16 = 500 Hz

4) Bande allouée : la bande allouée est donc de 500 $\times$ 4 = 2 kbit/s

Exercice 5.4 Multiplexeur

1) Longueur de l'IT : la longueur de l'IT, exprimée en bits, correspond à l'ensemble des informations nécessaires à la reconstitution d'un échantillon du signal. Celui-ci étant quantifié sur 256 niveaux, chaque échantillon contiendra 8 bits (2^8 = 256). La longueur de l'IT est donc de 8 bits.

2) Rythme et longueur de la trame : pour assurer un débit de 64 000 bit/s par IT de 8 bits et 1 IT par trame, il faut 64 000/8 = 8 000 IT pour chaque voie soit 8 000 trames/s. Compte tenu de l'IT de synchronisation chaque trame écoule 32 IT (30 + 2) soit une longueur de trame, exprimée en bits de 32 $\times$ 8 = 256 bits.

3) Débit du lien composite : sauf pour les multiplexeurs statistiques, le débit composite (D_c) d'un multiplexeur doit être au moins égal à la somme des débits des voies basse vitesse (D_{bv}), le débit à écouler est de :

$$D_c = \sum D_{bv}$$

$$D_c = 32 \times 64\,000 = 2\,048 \text{ kbit/s}$$

4) Efficacité du multiplexeur : l'efficacité du multiplexeur est le rapport entre le débit utile écoulé sur la voie composite et le débit du lien. Le débit utile correspond aux 30 IT de voix, l'efficacité est alors de :

$$E = 30/32 = 0{,}9375 \text{ soit } 94\ \%$$

CHAPITRE 6

Exercice 6.1 Évaluation du nombre de liaisons

Pour un réseau de $n - 1$ nœuds complètement interconnectés, il faut, pour interconnecter le $n^{ème}$ nœud, $(n - 1)$ liaisons. Soit pour les n nœuds du réseau $n\ (n - 1)$ liaisons. Cette manière de compter dénombre deux fois la même liaison : A → B et B → A. Le nombre de liaisons (N) est donc :

$$N = n\ (n - 1)/2$$

Pour 100 équipements

$$N = 100 \times 99 / 2 = 4\ 950 \text{ lignes.}$$

Exercice 6.2 Table de routage

Soit la *matrice de routage* (figure 6.50) :

$$M = \begin{bmatrix} 0 & 7 & 0 & 0 & 0 & 4 \\ 7 & 0 & 3 & 0 & 2 & 0 \\ 0 & 3 & 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 & 7 & 4 \\ 0 & 2 & 0 & 7 & 0 & 3 \\ 4 & 0 & 0 & 4 & 3 & 0 \end{bmatrix}$$

de \ à	A	B	C	D	E	F
A	0	7	0	0	0	4
B	7	0	3	0	2	0
C	0	3	0	5	0	0
D	0	0	5	0	7	4
E	0	2	0	7	0	3
F	4	0	0	4	3	0

Figure 6.50 La matrice de routage.

Rappelons que la matrice de routage indique le coût (métrique) d'un lien entre deux nœuds. Une table de routage est un ensemble de quadruplets :

<Nœud origine, Destination, Nœud suivant, Coût>

– Nœud d'origine ⇒ dénomination de la table
– Destination ⇒ ensemble de lignes de la table
– Nœud suivant ⇒ ensemble de colonnes qui désigne les successeurs du nœud
– Coût ⇒ évaluation du coût pour joindre une destination en prenant cette direction.

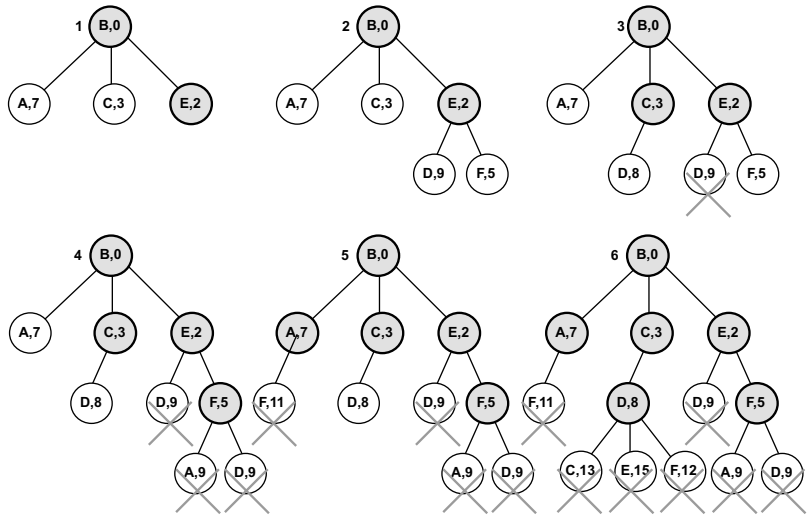
La lecture de la table permet à un paquet de trouver la route à prendre pour rejoindre sa destination. Elle établit une correspondance entre l'adresse destinataire, contenue dans le paquet, et les nœuds voisins. Le choix du nœud voisin peut être unique, ou multiple, selon la politique de routage mise en œuvre.

Arbre de coût minimal du nœud B, figure 6.51, ce qui correspond à la table de routage de la figure 6.52.

Cartographie du réseau : la cartographie ou topologie physique est déduite par simple lecture des liens dans la matrice de routage. La figure 6.53 décrit les différentes étapes.

La lecture de la matrice de routage à partir du nœud A montre qu'on peut atteindre les nœuds B et C (1). De B on joint E et C (2). De C on accède à D. Enfin, de D on rejoint E et F. L'analyse des nœuds E et F n'apporte aucune connaissance nouvelle.

© Dunod – La photocopie non autorisée est un délit



Routes validées	Routes découvertes	Routes en attente
B,0	BA,7 (en attente, →) BC,3 (en attente, →) BE,2 (Validée)	BA,7 BC,4
BE,2	EF,5 (en attente, →) ED,9 (en attente, →)	EF,5 ED,9 BA,7 BC,3
BC,3	CD,8 (en attente, →) ED,9 (Fin, on sait maintenant aller en D pour 8)	CD,8 EF,5 BA,7
EF,5	FA,9 (Fin, on sait déjà aller en A pour 7) FD,9 (Fin, on sait déjà aller en D pour 8)	CD,8 BA,7
BA,7	AF,11 (Fin on sait déjà aller en F pour 5)	CD,8
CD,8	DC,13 (Fin, on sait déjà aller en C pour 3) DE,15 (Fin, on sait déjà aller en E pour 2) DF,12 (Fin, on sait déjà aller en F pour 5)	Vide

Figure 6.51 L'arbre de coût minimal du nœud B.

Nœud destination	Nœud suivant	Coût total
A	A	7
B	Local	0
C	C	3
D	C	8
E	E	2
F	E	5

Figure 6.52 La table de routage du nœud B.

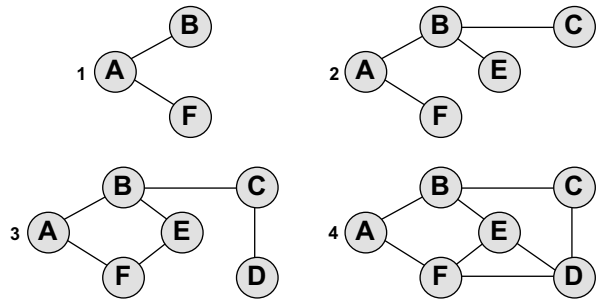


Figure 6.53 La topologie du réseau.

Exercice 6.3 Temps de transfert sur un réseau

Taille des unités de données : le MTU correspond à la taille maximale d'une unité de données du niveau réseau (données du protocole comprises). C'est aussi la charge utile du protocole de niveau liaison. La charge utile du bloc émis par le LAN correspond à la MTU diminuée de la taille de l'en-tête, soit :

1 500 – 20 = 1 480 octets, ce qui correspond à la taille du message à transmettre.

En commutation de circuits et en commutation de messages, le bloc de données issu du LAN est directement encapsulé dans une unité de données du protocole de liaison ; seul un en-tête de huit octets est rajouté. L'unité de données à transmettre est donc de :

1 500 + 8 = 1 508 octets

En commutation de paquets et en mode datagramme, l'en-tête de niveau réseau est recopié dans chaque datagramme. La figure 6.54 fournit, en fonction des MTU respectives, la charge utile effective et le nombre de datagrammes.

MTU	CU (Charge utile)	Nombre de paquets 1 480/CU	Taille de l'en-tête H = Hn + Hl
57	37	40	28
168	148	10	28
316	296	5	28

Figure 6.54 La détermination de la charge des paquets.

Pour résoudre ce problème, nous utiliserons la formule générale :

$$Tp = \left(\frac{L + pH}{D}\right)\left(1 + \frac{N}{p}\right)$$

avec Tp temps de traversée du réseau
L longueur du message,
p nombre de paquets,
H taille des en-têtes
N nombre de nœuds

© Dunod – La photocopie non autorisée est un délit

1) Temps de transfert en mode commutation de circuits (CC)

Pour le message, en CC

$$N = 0, \quad p = 1.$$

L'en-tête vaut Hcc = Hn + Hl = 28 octets

$$Tc = (1\,480 + 28) \times (8/64\,000) = 0{,}1885 \text{ s}$$

2) Temps en mode commutation de messages (CM)

En CM

$$p = 1, \quad N = 5$$

$$[(1\,480 + 28) \times (8/64\,000)](1 + 5) = 1{,}131 \text{ s}$$

3) Temps en mode commutation de paquets

Avec $N = 5$, $H = 28$, le temps de transfert est :

– Pour MTU 57 $[(1\,480 + 40 \times 28)\,(8/64\,000)]\,(1 + 5/40) = 0{,}325 \times 1{,}125 = 0{,}365$ s

– Pour MTU 168 $[(1\,480 + 10 \times 28)\,(8/64\,000)]\,(1 + 5/10) = 0{,}22 \times 1{,}5 = 0{,}33$ s

– Pour MTU 316 $[(1\,480 + 5 \times 28)\,(8/64\,000)]\,(1 + 5/5) = 0{,}2025 \times 2 = 0{,}405$ s

De manière générale, plus le paquet est de petite taille, meilleur est le temps de transfert. Ce principe a déjà été vu lors de l'étude des multiplexeurs. Cependant en commutation de paquets (multiplexage par étiquette), on ajoute à chaque unité de données un en-tête, de ce fait il existe un rapport harmonieux entre la taille des unités de données et la taille de l'en-tête.

Exercice 6.4 Routage et commutation

La différence entre les différents éléments d'acheminement réside dans le paramètre pris en compte pour sélectionner une voie. La figure 6.55 présente ces différences.



Figure 6.55 Routeur, commutateur, brasseur.

Exercice 6.5 Commutation de circuits et de paquets

Caractéristiques	Commutation de circuits	Commutation de paquets	
		Mode orienté connexion (circuit virtuel, CV)	Mode datagramme
Circuit dédié	Oui	Non	
Débit disponible	Fixe	Dynamique	
Optimisation de l'utilisation de la bande passante	Non, toute la bande passante est allouée à la communication (silence)	Oui, toute la bande passante est allouée à l'unité de données.	
Établissement du circuit (connexion) lors de la séquence d'appel	Nécessaire		Non
Adressage	Lors de la mise en relation	Chaque paquet contient le numéro du CV	Chaque paquet contient les adresses complètes de la source et du destinataire
Information de routage	Lors de la mise en relation	À chaque circuit établi correspond une entrée dans la table de commutation (réseau à état)	Le réseau ne conserve aucune information de routage des paquets (réseau sans état)
Routage	La route est déterminée lors de la mise en relation	La route est établie à l'initialisation du CV ; chaque paquet suit cette route	Chaque paquet a un routage indépendant
Conséquence d'une défaillance de routeur	Tous les circuits traversant l'équipement sont détruits. Nécessité de réinitialiser les connexions.		Aucune, sauf la perte des datagrammes présents dans le routeur incriminé
Quand peut apparaître la congestion ?	À l'établissement d'un circuit (refus de connexion, si pas de ressource disponible)		À chaque paquet transmis
Contrôle de congestion	Pas nécessaire, refus de connexion	Nécessaire, allocation statistique des ressources. Mécanisme relativement facile lorsqu'il est possible d'allouer suffisamment d'espace mémoire à l'établissement du circuit (virtuel ou non)	Difficile et complexe. Réseau best effort, non fait par le réseau, reporté aux organes d'extrémité
Principe de facturation	À la distance et à la durée	Au volume d'information transmise (X.25) Au forfait, FR et ATM selon le SLA	En principe au forfait

Figure 6.56 Synthèse commutation de circuits et de paquets.

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 7

Exercice 7.1 Fonctions et couches OSI

1. Le niveau physique réceptionne un flux de bits et le formate en trame pour remise à la couche liaison de données.
2. Le chemin à travers le réseau est déterminé par la couche réseau.
3. La synchronisation des échanges de données est gérée par la couche session.

Exercice 7.2 Adresse SAP d'une émission FM

Le point d'accès à une entité réseau est la caractéristique qui identifie, sans confusion possible (adresse), un service. Une station d'émission d'un réseau de radio diffusion est identifiée par sa fréquence d'émission. Le SAP d'une station est sa fréquence d'émission.

Il ne faut pas confondre la NSAP qui identifie le point d'accès à un service réseau avec la SNAP qui identifie le point d'accès au sous-réseau physique de transport, par exemple une adresse X.121.

Exercice 7.3 Encapsulation

Dans le modèle OSI, ce sont les paquets qui encapsulent les TPDU (figure 7.40). Quand une TPDU arrive au niveau de la couche réseau, la totalité de l'en-tête et des données constituent le champ de données du paquet (N_SDU).

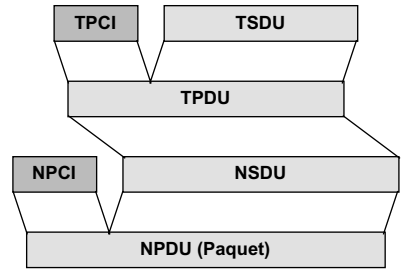


Figure 7.40 L'encapuslation des messages de transport.

Exercice 7.4 Mode connecté et mode non connecté

C'est à partir des fonctionnalités de chacun des modes de mise en relation et des services de chacune des couches que l'on peut définir le mode de mise en relation le mieux approprié pour telle ou telle couche (figure 7.41).

– **Couche transport** – Cette couche a essentiellement pour fonction de rendre le service réseau transparent aux couches de traitement, quelle que soit la qualité du sous-réseau de transport utilisé. De ce fait, c'est elle qui a en charge la correction des erreurs pouvant subsister et la délivrance des messages dans le bon ordre. Cette couche dite de bout en bout a aussi la charge

de s'assurer que les données émises peuvent être reçues (contrôle de flux de bout en bout). Dans ces conditions, un service connecté est requis.

– **Couche réseau** – Cette couche doit assurer le routage des paquets à travers un réseau, tous les types de services peuvent être imaginés selon la politique de routage mise en œuvre (aléatoire ou déterministe). Les services en mode non connecté ou connecté sont envisageables.
– **Couche liaison** – Cette couche est la première couche au-dessus du système physique. Si les erreurs « physiques » sont nombreuses, il convient de les corriger au plus vite (reprise sur temporisation ou NACK plus efficace). Ici, un service en mode connecté s'impose. Par contre, si le taux d'erreur est faible, un service non connecté peut être envisagé, la reprise sur erreur dans ce cas pouvant être effectuée par la couche transport (cas des réseaux locaux par exemple).

CRITÈRES	MODE CONNECTÉ	MODE NON CONNECTÉ
Établissement	Oui	Non
Contrôles : – erreurs – flux – séquencement	 Oui Oui Oui	 Non Non Non
Adressage	À l'établissement	Dans chaque entité
Négociation des options	Oui	Non
Type de service	Fiable	Non fiable

Figure 7.41 Synthèses des fonctionnalités selon le mode de mise en relation.

Exercice 7.5 Terminal virtuel

Le protocole de terminal virtuel permet aux applications orientées présentation (ex. : les éditeurs de texte) de travailler avec un grand nombre de terminaux incompatibles (interopérabilité). L'émulation « transforme » le terminal réel en terminal du système que l'on émule.

Exercice 7.6 Contrôle de flux et transferts isochrones

Le mécanisme de contrôle de flux consiste à ralentir, voire arrêter l'émission, la conséquence directe est un asynchronisme dans la réception des données. Cet asynchronisme est incompatible avec une transmission de données dite isochrone comme le nécessitent la voix et la vidéo.

Exercice 7.7 Contrôle de flux et classe de transport 0

Les différentes classes de transport ont été définies pour pallier les insuffisances des sous-réseaux de transport utilisés. La couche transport rend transparent, aux services de session, le sous-réseau physique utilisé.

Dans ces conditions, compte tenu que la classe 0 est faite pour s'appuyer sur un service réseau « parfait » elle n'implémente qu'un minimum de mécanismes. Les TPDU ne comportent pas de champ numéro de TPDU, un service de fenêtrage n'est donc pas réalisable. Le contrôle de flux peut, éventuellement, être effectué par les couches inférieures.

© Dunod – La photocopie non autorisée est un délit

Exercice 7.8 Référencement d'une connexion de transport

TP4 peut définir des connexions multiples entre toutes les paires de TSAP. Dans ce cas, les connexions sont identifiées par les champs source référence et destination référence dans les TPDU et non par l'adresse TSAP. (Remarquons que dans la TPDU_CR le champ « référence destination » est toujours à zéro.)

Exercice 7.9 Connexion de transport et connexion de session

Les principales similitudes sont :

– Service orienté connexion.
– Établissement et libération des connexions, avant et après utilisation.
– Primitives de transfert régulier de données.
– Délivrance de données fiables.

Les différences sont :

– La session : libération brutale ou négociée, transport : libération brutale uniquement.
– La connexion de transport n'autorise que des flux de données normales et exprès, la session comporte quatre types de flux de données (voir exercice 7.10).
– Les connexions « session » ont un dialogue de gestion, les connexions « transport » un dialogue de transfert.
– Pas de notion de synchronisation, d'activité, ni de jeton dans les connexions transport.
– Une connexion session peut utiliser plusieurs connexions transport.

Exercice 7.10 Les types de variables d'ASN-1

L'ASN-1 est un langage de description de données. Il définit des types simples ou structurés (comme tous les langages de haut niveau) ; l'ASN-1 est proche, en cela, du langage de programmation PASCAL.

BOOLEAN	Représente un type de variable à deux états.
BIT STRING	Définit un type de chaîne de caractères binaires. À une chaîne de caractères on associe un chiffre binaire ex. : '100011'B .
ISO646STRING	Est un identificateur d'objet construit, la première valeur identifie l'organisme de normalisation, la seconde la norme, la troisième le type, ici string (chaîne de caractères).
CHOICE	Modélise une variable parmi une collection, chaque élément étant associé à une étiquette spécifique.
SEQUENCE	Représente une collection d'objets ordonnés de même type (SEQUENCE, tableau), ou de type différent (SEQUENCE OF, *record* ou enregistrement).

Le type SET ou SET OF est de nature identique au type SEQUENCE ou SEQUENCE OF. La structure SEQUENCE impose une délivrance ordonnée des données au destinataire. La structure SET autorise une délivrance désordonnée.

IMPLICIT	Est utilisé quand il n'est pas utile de transmettre le type, le récepteur pouvant le reconnaître.
OPTIONAL	Le champ ne sera transmis que s'il est utile à la transaction en cours.
DEFAULT	Permet d'initialiser une variable.
NULL	Un champ de ce type n'est pas transmis.

Prenons, par exemple, la description d'un enregistrement identifiant un compte bancaire :

– Le titulaire du compte est identifié par une chaîne de 20 caractères (champ nom).
– Le code confidentiel d'accès ne sera jamais transmis, il ne peut être utilisé que localement (champ code).
– Le solde du compte ne sera transmis que s'il est utile à l'opération en cours (champ solde).
– L'autorisation de découvert n'est jamais implicite, le champ est initialisé à FALSE (champ découvert).

Soit la structure :

```
compte : : = IMPLICIT  SEQUENCE
          {
           nom[0]       IMPLICIT OCTET STRING, -- 20 caracteres
           code[1]      IMPLICIT INTEGER NULL,
           solde[2]     IMPLICIT REAL OPTIONAL,
           decouvert[3] IMPLICIT BOOLEAN DEFAULT FALSE
          }
```

Exercice 7.11 Couche transport

La couche transport est la couche charnière d'une architecture réseau. À la frontière entre le sous-réseau réel de transport et les applications, elle doit garantir à ces dernières une même qualité de service quelle que soit la qualité du (ou des) sous-réseau(x) physique(s) réel(s) traversé(s).

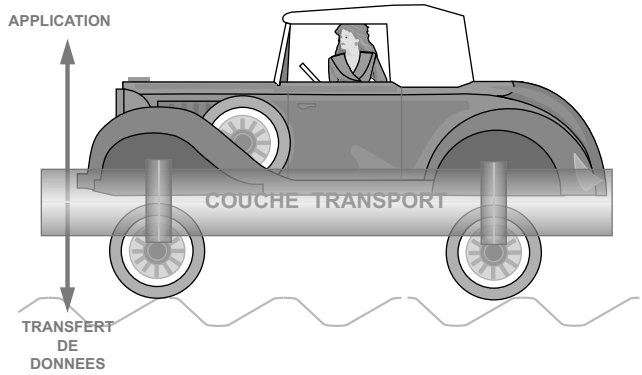


Figure 7.42 Analogie entre le réseau routier et un réseau de transport de données.

Elle joue le même rôle que les amortisseurs dans une automobile qui tente d'assurer aux passagers un confort identique quelles que soient les imperfections du réseau routier (figure 7.42).

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 8

Exercice 8.1 Masque de sous-réseau

1) La valeur binaire du premier octet permet de définir la classe d'adressage :

196D = 1100 0100B, soit une classe C (110)

Autre solution admissible : la classe C couvre les adresses

192.0.0.1 à 223.255.255.254

2) Comme on doit pouvoir adresser dix sous-réseaux, il faut donc dix adresses IP dérivées de l'adresse initiale. La valeur décimale 10 se code par 1010 en binaire ($2^3 < 10 > 2^4$), il faut donc disposer de 4 bits. Le masque de sous-réseau à construire est donc :

11111111.11111111.11111111.11110000

soit encore : 255.255.255.240

3) Compte tenu des bits affectés au masque de sous-réseau, il reste 4 bits pour identifier les machines, la valeur 0 représentant le sous-réseau lui-même, la valeur tout à 1 représente l'adresse de *broadcast*, chaque sous-réseau ne pourra comporter que 14 machines au maximum.

4) L'adresse de *broadcast* correspond à tous les bits du champ Host_ID à 1, soit pour le sous-réseau 3, en ne considérant que le dernier octet :

0011 1111

Où le premier quartet désigne le sous-réseau 3, le second désignant le Host_ID a tous ses bits à 1. Ce qui, pour cet octet, correspond en décimal à 63, soit l'adresse de diffusion :

196.179.110.63

Attention : Il n'y a pas ambiguïté dans l'affectation de la valeur du sous-réseau, la valeur 0 ne devrait, pour des raisons de compatibilité, jamais être utilisée. En effet, une vieille version de UNIX considère le champ à zéro comme étant l'adresse de diffusion (UNIX BSD).

Exercice 8.2 Masque de sous-réseau et dysfonctionnement

Source Destination	150.150.1.28 (255.255.255.0)	150.150.1.57 (255.255.0.0)	150.150.2.28 (255.255.255.0)	150.150.2.57 (255.255.0.0)
150.150.1.28		oui	non	oui
150.150.1.57	oui		non	oui
150.150.2.28	non	oui		oui
150.150.2.57	non	oui	oui	

Figure 8.38 Matrice de communication.

Exercice 8.3 Masque de sous-réseau variable

Nombre de bits nécessaires à l'identification des sous-réseaux : l'adresse 194.18.20.0 est une adresse de classe C, elle autorise la numérotation de 254 machines. Mais compte tenu qu'avec N bits on ne peut numéroter que $2^N - 2$ sous-réseaux (l'adresse tout à zéro identifie le réseau, l'adresse tout à un est l'adresse de diffusion), pour numéroter les trois sous-réseaux il faut donc 3 bits ($2^3 = 8$, soit six sous-réseaux). Dans ces conditions, il reste 5 bits pour numéroter les stations soit $2^5 - 2 = 30$ stations. Ce qui est insuffisant pour numéroter les machines du réseau 3 !

Solutions envisageables :

– conserver un masque de sous-réseau sur 3 bits, et partager le sous-réseau 3 en deux sous-réseaux de moins de 30 machines, les communications entre les machines de cet ex sous-réseau devront transiter *via* un routeur. Si les échanges sont nombreux, cela peut pénaliser fortement le fonctionnement de cette entité.

– utiliser un masque de sous-réseau variable, 3 bits pour les réseaux 1, 2 et 2 bits pour le réseau 3. Nous retiendrons cette solution.

Plan d'adressage (masque de sous-réseaux de longueur variable ou **VLSM**, *Variable Length Subnet Mask*) : un plan d'adressage de longueur variable se réalise en déroulant un arbre hiérarchique selon le modèle suivant (figure 8.39).

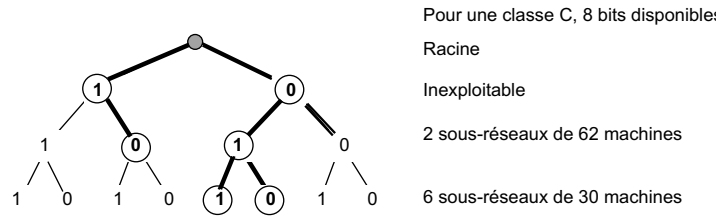


Figure 8.39 Développement d'un masque de sous-réseau variable.

L'arbre se développe jusqu'à satisfaire les besoins d'identification. Attention, les solutions tout à 1 et tout à 0 doivent être éliminées. Le tableau suivant (figure 8.40) présente une des solutions envisageables

N° Réseau	Bits du masque de sous-réseau (seuls ceux qui identifient le S/R	Adresse du sous-réseau	Adresse de la première station adressable	Adresse de la dernière station adressable	Nombre de stations adressables
1	011	194.18.20.96	194.18.20.97	194.18.20.126	30
2	010	194.18.20.64	194.18.20.65	194.18.20.94	30
3	10	194.18.20.128	194.18.20.129	194.18.20.190	62

Figure 8.40 Plan d'adressage de l'entreprise.

Remarques : cette solution présente quelques difficultés :

– tous les routeurs n'acceptent pas les masques de sous-réseaux variables ;

© Dunod – La photocopie non autorisée est un délit

– un plan d'adressage de ce type est complexe à définir, le risque d'erreur est important et peut donc engendrer des problèmes de routage.

CHAPITRE 9

Exercice 9.1 Table ACCM (*Asynchronous Control Character Map*)

1) Séquence de bits émise : si celle à émettre en mode synchrone est :

« 00111111111111111001111000111110111111010111110 »

La transparence binaire est réalisée par la technique dite du bit de bourrage. Cette technique consiste à insérer 1 bit à « 0 » tous les 5 bits à « 1 », la séquence émise sera (figure 9.24) :

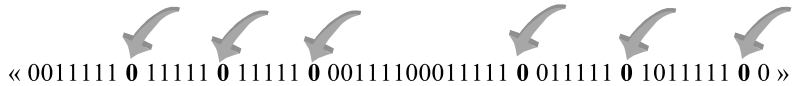


Figure 9.24 La séquence de bits émise.

2) Séquence de caractères émise : en mode asynchrone, la transparence au fanion est réalisée par le remplacement du caractère 0x7E (fanion) par la séquence : ESC_PPP, ESC_FLAG soit 0x7D, 0x5E. Le caractère d'échappement ESC_PPP, 0x7D est remplacé par la séquence : ESC_PPP, ESC_ESC soit 0x7D, 0x5D soit (figure 9.25).

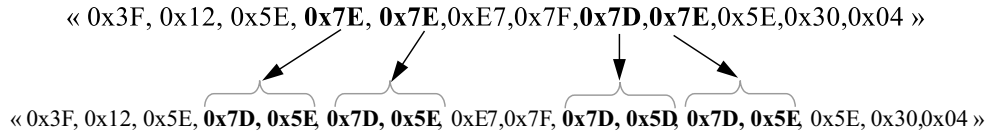


Figure 9.25 La séquence de caractères émise.

3) Nombre de bits transmis : sachant qu'en transmission asynchrone, chaque caractère à émettre est précédé d'un dit de Start et se termine par un bit de Stop, pour chaque caractère émis 10 bits sont transmis, soit pour les 16 caractères du message 160 bits.

4) Table ACCM par défaut « mode asynchrone » : si les 32 premiers caractères doivent être masqués, tous les bits de la table ACCM sont à 1 soit la valeur en hexadécimal :

« 0xFF, 0xFF, 0xFF, 0xFF »

5) Table ACCM par défaut « mode synchrone » : si aucun caractère ne doit être masqué, la valeur est :

« 0x00, 0x00, 0x00, 0x00 »

6) Transparence aux caractères « STX, ETX, ACK » par le modem

a) Signification, rang et valeur des caractères des caractères « STX, ETX, ACK »

Commande	Signification	Rang	Valeur binaire	Valeur hexa.
STX	Start Of Text	3	0000 0010	0x02
ETX	End Of Text	4	0000 0011	0x03
ACK	Acknowledge	7	0000 0110	0x06

Figure 9.26 Le codage et la signification des caractères.

b) Valeur de la table ACCM en binaire et en hexadécimal : les caractères de rang 3, 4 et 7 doivent être masqués, les bits de même rang seront mis à 1 :

« 0000 000B, 0000 000B, 0000 0000B, 0100 1100B »

« 0x00, 0x00, 0x00 »

c) Transparence aux commandes et aux fanions : la transparence aux commandes est obtenue par le remplacement de ces caractères par la séquence : ESC_PPP, ESC_Commande où la valeur de ESC_Commande est la valeur ASCII de la commande avec le sixième bit complémenté (inversé). Les caractères dont la transparence doit être réalisée sont en gras dans l'extrait du champ données :

...C8 F4 AB **7E** A3 C0 FA **02** C9 F3 05 C9 **7D 03** 04 **7E** 0F F1 **06** E4 F1 34 5F...

Caractère à remplacer	Signification	Séquence de remplacement
0x7E	Fanion	0x7D 0x5E
0x02	STX	0x7D 0x22
0x7D	ESC_PPP	0x7D 0x5D
0x03	ETX	0x7D 0x23
0x7E	Fanion	0x7D 0x5E
0x06	ACK	0x7D 0x26

Figure 9.27 Le codage et la signification des caractères.

d) Séquence émise :

...C8 F4 AB **7D 5E** A3 C0 FA **7D 22** C9 F3 05 C9 **7D 5D 7D 23** 04 **7E 5E** 0F F1 **7D 26** E4 F1 34 5F...

CHAPITRE 10

Exercice 10.1 Table ARP

1) Net_ID du réseau : en classe A, le Net_ID est exprimé sur un octet, soit dans cet exercice la valeur 10 (adresses privées de classe A).

© Dunod – La photocopie non autorisée est un délit

2) Masque de sous-réseau pour distinguer deux sous-réseaux : pour distinguer le nombre de bits nécessaires, il suffit d'examiner la valeur binaire du premier octet du Host_ID, si cela est insuffisant du second... jusqu'à trouver la combinaison binaire qui réponde au problème posé (figure 10.40).

Station	1er octet du Host_ID	Sous-réseau
99	**01** 100011	SR1
163	**10** 100011	SR2
189	**10** 111101	SR2
126	**01** 111110	SR1

Figure 10.40 Détermination des sous-réseaux.

L'examen de la figure 10.40 montre que seuls deux bits sont nécessaires pour distinguer dans le plan d'adressage donné les deux sous-réseaux. Le masque de sous réseau correspondant est :

255.192.0.0

3) Masque de sous-réseau pour identifier quatre sous-réseaux : la plus petite combinaison binaire pour distinguer quatre sous-réseaux distincts dans les adresses données est de quatre. Le masque de sous-réseau est alors :

255.240.0.0

4) Adresse IP des deux sous-réseaux : l'adresse réseau de chacun des deux sous-réseaux constitués est :

10D.01000000B.0D.0D

10D.10000000B.0D.0D

Notation provisoire utilisée pour indiquer comment sont déterminées les adresses réseaux : D signifie Décimal, B binaire, soit en notation décimale pointée :

10.64.0.0 masque 255.192.0.0

10.128.0.0 masque 255.192.0.0

La figure 10.41 illustre le réseau.

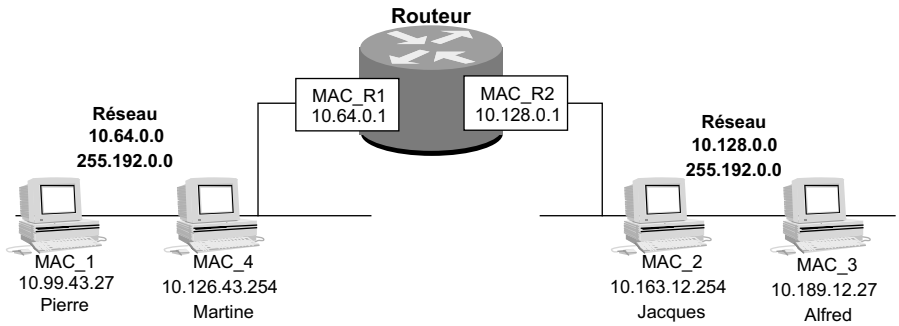


Figure 10.41 Le schéma du réseau.

5) Table ARP de la station de Pierre (figure 10.42)

@IP	@MAC
10.126.43.254	MAC_4
10.163.12.254	MAC_R1
10.189.12.27	MAC_R1

Figure 10.42 La table ARP de la station de Pierre.

6) Accès à Internet : l'entreprise utilise l'adresse 10 qui est une adresse non routable sur Internet. Elle devra faire la demande d'attribution d'adresses officielles. Si elle ne veut pas avoir à revoir la configuration de toutes ses machines, elle devra mettre en œuvre un translateur d'adresses pour avoir accès à Internet (NAT).

CHAPITRE 11

Exercice 11.1 Trace TCP/IP

Généralités

a) *Notion d'analyseur* : avant d'examiner la trace de cet exercice, il convient de dire quelques mots sur les appareils qui permettent de les obtenir : les analyseurs. Un analyseur de protocoles est un outil qui permet d'ausculter le réseau. Il permet :

- de mesurer les performances du réseau (statistiques) ;
- de générer un trafic en vue, par exemple, de déterminer des seuils de dysfonctionnement, de tester des évolutions de version de logiciel...
- d'horodater les messages et de déterminer, ainsi, les temps inter-événements ;
- de filtrer certains événements particuliers, par exemple des demandes de connexion...
- d'effectuer des tests et de réaliser la mise au point des protocoles.

Il existe deux types d'analyseurs, les analyseurs WAN et les analyseurs LAN :

- Les analyseurs WAN sont utilisés dans les réseaux WAN, sur une liaison de données, au niveau d'une jonction ETTD/ETCD. Les analyseurs WAN se connectent en mode passif ou actif. Dans le mode passif ou espion, ils surveillent le trafic de la station sans en perturber le fonctionnement. En mode actif, ils simulent un ETTD, auquel ils se substituent pour tester le fonctionnement d'un ETCD (ou réseau).
- Les analyseurs LAN sont utilisés dans les réseaux locaux, ils se connectent comme n'importe quelle station et interceptent toutes les informations circulant sur le réseau. Les analyseurs LAN peuvent générer un trafic afin de déterminer les performances du réseau.

En principe un analyseur peut indifféremment être utilisé sur un LAN et sur un WAN. Ce sont les programmes d'analyse et les interfaces physiques qui distinguent ces deux fonctionnalités. La figure 11.25 compare ces deux modes de fonctionnement des analyseurs.

© Dunod – La photocopie non autorisée est un délit

Critères de comparaison	Analyseur WAN	Analyseur LAN
Raccordement	Au niveau de la jonction ETCD/ETTD, la connexion nécessite l'ouverture momentanée de la jonction.	Le raccordement est identique à celui d'une station. La mise en service d'un analyseur LAN ne perturbe pas le réseau.
Vitesse de fonctionnement	Débit actuellement limité à 256 kbit/s.	Conformément aux débits en vigueur sur les réseaux locaux, les analyseurs LAN utilisent des débits qui vont de 1 à 100 Mbit/s.
Nature du trafic	Analyse le trafic transitant sur la liaison.	Analyse tout le trafic transitant sur le réseau.
Sécurité	Nécessite l'ouverture de la liaison, l'introduction de l'analyseur peut être détectée.	L'analyseur peut être programmé pour ne pas répondre au *broadcast*, il est indécelable. Si les mots de passe ne sont pas cryptés, il peut les intercepter.

Figure 11.25 Comparaison des différents types d'analyseurs.

Un analyseur de protocoles de niveau N décode les données de service du niveau N (type de PDU, compteurs...) et fournit, en hexadécimal, le contenu du champ Data, c'est-à-dire de la (N)SDU ou la (N+1)PDU.

La trace proposée est une reproduction d'une trace obtenue avec un analyseur de protocole Ethernet. L'analyseur extrait le préambule, les fanions et ne présente que les données utiles. Le contenu de la trame en hexadécimal est interprété (codage ASCII), ce qui facilite le travail d'analyse.

En effet, le décodage du champ Données laisse clairement apparaître son contenu : UNIX®System V... De ce fait, l'on sait déjà que l'on peut s'attendre à ce que le protocole réseau utilisé soit IP du DoD (*Department of Defense*). La valeur des octets 13 et 14 (Ethertype ou type de protocole) confirment ces dires. Le protocole supérieur est TCP/IP (valeur 0x0800).

b) *Méthode d'analyse* : à partir de la structure du bloc de données rappelée dans l'énoncé. On découpe les données lues par l'analyseur en blocs de données à analyser (figure 11.26), en supposant *a priori* qu'aucune option n'est invoquée.

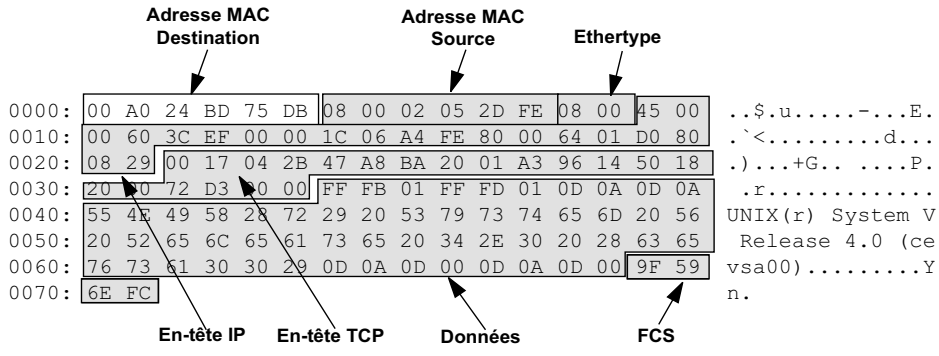


Figure 11.26 Le découpage de la trame en blocs à interpréter.

Il ne reste plus alors qu'à interpréter champ par champ, octet par octet ou bit par bit, le résultat.

Décodage la trame MAC 1

a) *En-tête MAC*

Champ	Valeur hexa.	Commentaires
Adresse destination	00 A0 24 BD 75 BD	00 A0 24 Identification du fournisseur 3COM BD 75 BD N° séquentiel de fabrication de la carte
Adresse source	08 00 02 05 2D FE	08 00 02 Identification du fournisseur (ici 3 COM-Bridge)
Type de protocole	08 00	IP du DoD

Figure 11.27 Le décodage de l'en-tête MAC.

b) *En-tête IP*

Champ	Valeur hexa.	Commentaires
Identification Version	4 -	Sur 4 bits, IP version 4
Longueur en-tête	- 5	IHL (*Internet Head Length*), sur 4 bits, en multiple de 4 octets la valeur normale est 5 soit 20 octets (pas d'option).
Type de service	00	Champ de bits 7 6 5 4 3 2 1 0 Priorité (routine) – – – – 0 0 0 0 Délai acheminement (Normal) – – – – 0 – – – Débit (Normal) – – – 0 – – – – Fiabilité (Normale) – – 0 – – – – – Réservés 0 0 – – – – – –
Longueur totale	00 60	Exprime la longueur totale du datagramme (données utiles de la couche MAC). Ici, la valeur 60 soit 96 octets est supérieure à 48, il n'y a donc pas eu d'opération de bourrage.
Identification	3C EF	Identifie tous les fragments d'un même datagramme.
Drapeau	00	Sur les trois derniers bits – bit 7, non utilisé – bit 6, DF (*Don't Fragment*), à 0 : fragmentation possible – bit 5, MF (*More Fragment*), à 1 indique qu'un fragment suit. Les autres bits appartiennent au champ suivant.
Offset	00	Sur 13 bits, indique la position du fragment depuis le début.
Durée de vie	1C	*Time to Live*, durée de vie du fragment, initialement exprimé en seconde, représente aujourd'hui le nombre de sauts restants.
Protocole supérieur	06	Identifie TCP
Total de contrôle	A4 FE	
@ IP Source	80 00 64 01	@IP = 128.0.100.1, Adresse de classe B.
@ IP Destination	DO 80 08 29	@IP = 208.128.8.41, Adresse de classe C. En principe, les machines sur un même réseau appartiennent à un même espace d'adressage. Ce n'est pas le cas ici. On peut donc penser que la machine source n'est pas sur le même réseau physique que la station destinataire du message.

Figure 11.28 Le décodage de l'en-tête IP.

© Dunod – La photocopie non autorisée est un délit

c) *En-tête TCP*

Champ	Valeur hexa.	Commentaires
Port source	00 17	Cette valeur identifie le terminal Telnet, le contenu des traces est donc un dialogue Telnet.
Port destinataire	04 2B	Attribué lors de l'établissement de la connexion.
N° de séquence	47 A8 BA 20	Le numéro de séquence initial est défini à la connexion, il est ensuite incrémenté du nombre d'octets transmis.
N° de seq. acquitté	01 A3 96 14	N° du prochain octet attendu (N° de séquence).
Longueur en-tête	50	Sur 4 bits, en multiple de 4 octets. L'en-tête TCP fait 20 octets (il n'y a pas d'option).
Drapeau	18	Champ de bits (6 bits valides) FIN (pas de demande de déconnexion) - - - - - - - 0 SYN (utilisé seulement à la connexion) - - - - - - 0 - RST (pas de demande de réinit.) - - - - - 0 - - PSH (délivrance immédiate) - - - - 1 - - - ACK (valide N° seq acquitté) - - - 1 - - - - URG (pas de données urgentes) - - 0 - - - - -
Fenêtre	20 00	Fenêtre en réception de 8 192 octets (dynamique).
Total de contrôle	72 D3	Calculé sur l'ensemble du segment et pseudo en-tête IP.
Pointeur data URG	00 00	Pointeur sur données urgentes, non validé par le flag URG.

Figure 11.29 Le décodage en-tête TCP/IP.

d) *Champ données de TCP*

```
                              FF FB 01 FF FD 01 0D 0A 0D 0A   .r..............
0040: 55 4E 49 58 28 72 29 20 53 79 73 74 65 6D 20 56  UNIX(r) System V
0050: 20 52 65 6C 65 61 73 65 20 34 2E 30 20 28 63 65   Release 4.0 (ce
0060: 76 73 61 30 30 29 0D 0A 0D 00 0D 0A 0D 00         sa00)........
```

Figure 11.30 Le découpage de la trame en blocs à interpréter.

Le champ données, reproduit ici, est partiellement décodé par l'analyseur (caractères interprétables). Cependant, l'analyse des premiers caractères du champ présente un intérêt certain :

'FF FB 01' et 'FF FD 01' sont des commandes Telnet (négociation d'options).

Toutes les commandes Telnet débutent par 'FF' (IAC, *Interpret As Command*, interpréter l'octet suivant comme une commande), si ce caractère apparaît dans le champ données il est doublé (caractère de transparence).

Le caractère suivant identifie la commande, il est éventuellement suivi d'un caractère qui précise une commande optionnelle. Les figures 11.31 et 11.32 fournissent la liste des principales commandes et des options Telnet.

Dialogue Telnet, paramétrage de l'écho :

'FF FB 01' IAC WILL ECHO, *Will Use Echo Data*
'FF FD 01' IAC DO ECHO, *Start Use Echo Data*

Commande	Valeur déc.	Valeur hexa.	Signification
IAC	255	FF	Interpréter le caractère suivant comme une commande
DON'T *xx*	254	FE	Refus d'une option, le caractère suivant '*xx*' identifie l'option refusée
DO *xx*	253	FD	Acceptation de l'option '*xx*' (*Start Use*)
WON'T *xx*	252	FC	Acquittement négatif de l'option '*xx*'
WILL *xx*	251	FB	Acquittement positif de l'option '*xx*' (*Will Use*)
GA	249	F9	Continuer (*Go Ahead*)
EL	248	F8	Effacer une ligne (*Erase Line*)
EC	247	F7	Effacer un caractère (*Erase Character*)
AO	245	F5	Arrêter l'édition (*Abort Ouput*)
IP	244	F4	Interrompre le processus (*Interrupt Process*)
BRK	243	F3	Break
NOP	241	F1	Opération nulle (*Non OPeration*)
EOR	239	EF	Fin d'enregistrement (*End of Record*)

Figure 11.31 Les exemples de commandes Telnet.

Nom	Valeur déc.	Valeur hexa.	Signification
Transmit Binaire	00	OO	Transmission en mode 8 bits
Echo	01	01	Écho des données introduites au clavier (*Echo Data*)
Carriage Return	10	0A	Retour chariot, positionne le curseur en début de ligne
Line Feed	13	10	Passage à la ligne suivante

Figure 11.32 Les exemples d'options Telnet.

e) *Champ FCS de la trame MAC :* Valeur du FCS : 9F 59 6E FC

Décodage de la trame MAC 2 (figure 11.33)

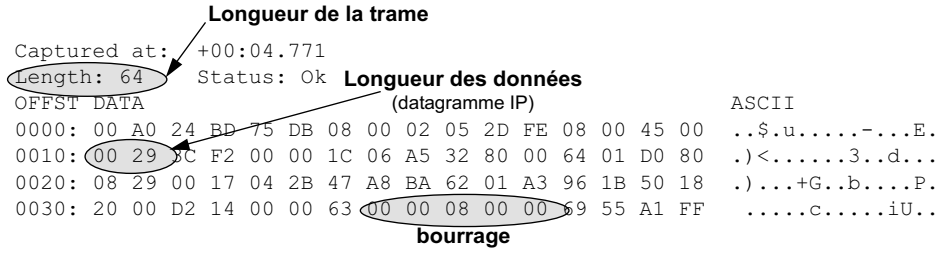


Figure 11.33 La trame MAC numéro 2.

L'analyseur précise que la longueur de la trame MAC est de 64 octets (figure 11.29), c'est-à-dire la longueur minimale d'une trame MAC Ethernet. Lorsque les données à transmettre ont une longueur inférieure à 64 octets, la couche MAC procède à un bourrage pour ramener la longueur du champ données MAC à 46 octets (64 octets en-tête MAC et FCS compris). Si on examine le champ longueur du datagramme IP (figure 11.33), on constate qu'effectivement la longueur du datagramme

© Dunod – La photocopie non autorisée est un délit

est de 0x29 (41 octets), il y a donc 5 octets de bourrage, ces 5 octets sont quelconques, c'est le contenu du *buffer*.

Exercice 11.2 Efficacité de TCP

Efficacité du protocole : l'efficacité d'une liaison peut s'exprimer comme étant le rapport entre le temps utilisé effectivement pour l'émission au temps total d'utilisation du support. La figure 11.34 illustre ce concept dans le cas d'un protocole à anticipation.

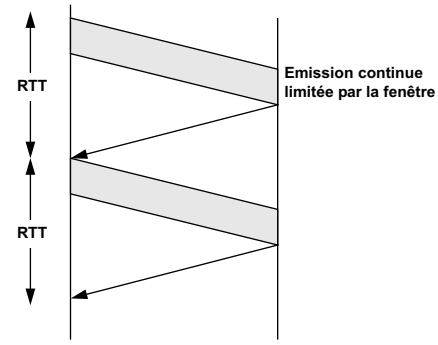


Figure 11.34 L'efficacité d'un protocole.

Soit :

$$Eff = \frac{\text{Temps d'émission}}{RTT}$$

La fenêtre étant déterminée sur 16 bits, l'anticipation peut atteindre 65 535 octets (2^{16}), ce qui correspond à un temps d'émission de :

$$\text{Temps d'émission} = (65\,535 \times 8) / 10^9 = 0{,}0005 \text{ s}$$

Efficacité du protocole :

$$Eff = \frac{\text{Temps d'émission}}{RTT} = \frac{0{,}0005}{0{,}5} = 0{,}001 \qquad \text{soit } 0{,}1\ \%$$

Débit de la liaison : l'efficacité du protocole sera maximale quand le temps d'émission des 65 535 octets (taille de la fenêtre) correspondra au RTT soit un débit de :

$$\text{Débit} = \frac{\text{Volume de données}}{RTT} = \frac{65535 \times 8}{0{,}5} = 1\,048\,560$$

Ce qui correspond à une liaison à 1 Mbit/s (ceci confirme le rendement de 0,001 sur la liaison à 1 Gbit/s).

Exercice 11.3 Comparaison transport TCP et transport ISO

Les principales similitudes et différences sont indiquées par la figure 11.35.

	Transport ISO	TCP
Similitudes	Fourniture d'un service de transport de bout en bout en mode orienté connexion (fiable).	
Différences	En-tête de 5 octets	En-tête standard 20 octets
	Déconnexion brutale	Déconnexion négociée
	Contrôle de flux par la couche réseau	Contrôle de flux et de congestion par la couche transport
	Négociation de la qualité de service	Pas de négociation de qualité de service

Figure 11.35 Comparaison succincte du transport ISO et TCP.

CHAPITRE 12

Exercice 12.1 Transfert de fichiers

Le transfert de fichiers FTP utilise les ports 20 et 21. Le port 20 est utilisé pour le transfert de données et le port 21 pour le contrôle de la connexion.

Exercice 12.2 Serveurs DNS

Tout serveur DNS du domaine doit connaître les serveurs DNS de ses sous-domaines et éventuellement au moins un serveur de son domaine maître.

Exercice 12.3 RPC

La notion de RPC dans un environnement client/serveur consiste à définir des procédures (*stubs*) qui réaliseront des tâches spécifiques et communiqueront avec le programme principal par passage de paramètres.

Exercice 12.4 Arbre de nommage

La hiérarchie décrite par le nommage du DNS autorise l'emploi de noms identiques lorsque ceux-ci n'appartiennent pas au même domaine, ainsi dans l'exemple développé figure 12.31 : le nom cnam peut être utilisé indifféremment par la Caisse nationale d'assurance maladie (cnam.sante.gouv.fr) et par le Conservatoire national des Arts et Métiers (cnam.education.gouv.fr).

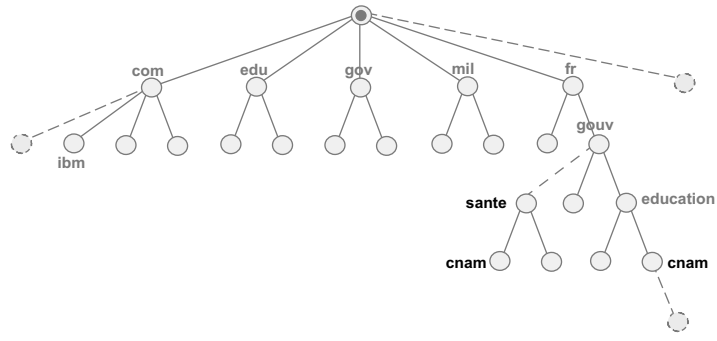


Figure 12.31 L'arbre de nommage.

© Dunod – La photocopie non autorisée est un délit

Exercice 12.5 Commande Ping

La commande Ping sur Renault.fr, a donné la réponse suivante :

```
Envoi d'une requête 'ping' sur www.renault.fr [160.92.111.2] avec 32 octets de
données :

Réponse de 160.92.111.2 : octets=32 temps=2082 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=155 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=156 ms TTL=246
Réponse de 160.92.111.2 : octets=32 temps=156 ms TTL=246
Statistiques Ping pour 160.92.111.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 155ms, Maximum = 2082ms, Moyenne = 637ms
```

1) Classe d'adresses : les classes d'adresses sont distinguées par les bits de poids fort de l'octet de poids fort de l'adresse :

0, adresse de classe A
10, adresse de classe B
110, adresses de classe C

Le premier octet (160) s'écrit en binaire : 10100000, c'est donc une adresse de classe B.

Où encore :

– La classe A, s'étend de 1.0.0.0 à 126.255.255.255
– La classe B s'étend de 128.0.0.0 à 191.255.255.255
– La classe C s'étend de 192.0.0.0 à 223.255.255.255

2) Protocoles : la commande Ping utilise deux protocoles ICMP (*Internet Control Message Protocol*) et le « transport » IP.

3) Valeur du RTT – La valeur élevée de la première requête Ping correspond vraisemblablement à la consultation du **DNS** pour la résolution de renault.fr (nom du serveur) en 160.92.111.2 (adresse du serveur).

CHAPITRE 13

Exercice 13.1 SDH/PDH

Les principaux avantages s'expriment en termes de facilités d'exploitation, de fiabilisation des liaisons (autocicatrisation), de débit et de facilité à insérer ou à extraire un débit inférieur d'un lien.

Exercice 13.2 Rendement protocolaire

Débit théorique du système

1. Largeur de bande occupée par une tonalité : 120 Hz (100+20).
2. Nombre de tonalités pouvant être utilisées simultanément :

- Bande passante du système :3 800 – 200 = 3 600 Hz
- Nombre de tonalités :3 600/120 = 30 tonalités

3. Débit maximal du système 30 × 128 × 8 = 30 720 bit/s.

Débit pratique du système

4. Puissance maximale de la tonalité reçue : la lecture de la figure 13.52 indique 9 mW.
5. Puissance minimale acceptée par le système, –3 dB correspond à une tonalité de demi-puissance soit = 4,5 mW.
6. Nombre de tonalités validées par le système : la lecture du tableau fait apparaître 25 tonalités > 4,5 mW.
7. Débit binaire effectif du modem 25 × 128 × 8 = 25 600 bit/s.

Rendement du système

8. Le nombre d'octets de bourrage que la couche AAL5 est susceptible d'introduire varie de 0 à 47 octets.
9. Nombre de cellules ATM qui seront constituées :
   - Taille des données AAL5 avant bourrage 1 500 + 8 = 1 508 octets.
   - Nombre de cellules ATM 1 508/48 = 31,4 cellules, soit 32 cellules entières.
10. Valeur des différents champs de la figure 13.53 :
    - Taille des données AAL5 après bourrage 48 × 32 = 1 536 octets
    - Données de bourrage 1 536 – 1 508 = 28 octets
    - Soit le schéma d'encapsulation suivant (figure 13.54) :

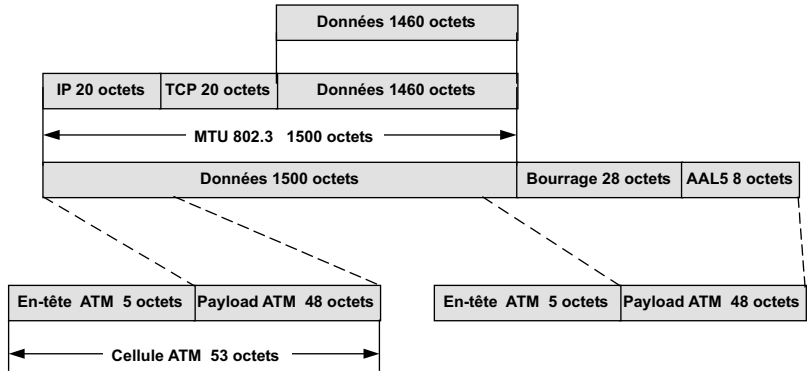


Figure 13.54 Encapsulation des données.

11. Rendement du protocole :

    Données utiles : 1 460 octets.
    Données transmises : 32 × 53 = 1 696 octets.
    Rendement du protocole : 1 460/1 696 = 86 %.

© Dunod – La photocopie non autorisée est un délit

12. Taux de transfert d'information :

    Débit réel du modem × Rendement du protocole = 25 600 × 0,86 = 22 016 bit/s

13. Taux de transfert d'information réel en tenant compte du taux d'erreur :

    Probabilité de recevoir l'ensemble des informations non erronées (p)
    p = (1–0,000001) 1 696 × 8 = 0,987.
    TTI = 22 016 × 0,987 = 21 730 bit/s.

14. Rendement global du système :

    R = TTI/Débit potentiel du modem = 21 730/30 720 = 0,707 soit environ 71 %.

CHAPITRE 14

Exercice 14.1 Reconstitution d'un paquet d'appel

Pour reconstituer le paquet d'appel il faut d'abord coder tous les éléments le constituant :

– **Codage de l'adresse** : au format X.121, l'adresse est codée selon le format < Type d'accès, Département, Commutateur de rattachement, Numéro de la liaison >. L'accès se faisant sur une LS, le type d'accès identifié par la valeur 1. Avec un chiffre par quartet, l'adresse de l'appelé est :

1 75 01 0089

L'adresse est codée en DCB, premier chiffre dans le quartet de poids fort du premier octet du champ adresse.

– **Codage des facilités**
  – Facturation à l'appelé 01, 01
  – GFA valeur locale 3 03,03
  – Taille paquet : 64 = 2^6, 128 = 2^7 soit 42,06,07
  – Négociation taille fenêtre 2, 7 43,02,07

  Dans ces conditions, la longueur du champ facilité est 10 soit 0x0A
  Détermination du CV : pour un appel sortant, le NVL affecté à la voie logique est le NVL de plus grande valeur disponible. Ici, il s'agit de la première connexion soit 19 ou, en hexadécimal : 13.

– **Format du paquet d'appel** (figure 14.70, ci-contre)

Exercice 14.2 Dialogue X.25

Rappels : la trace de niveau physique représente, codés en hexadécimal, tous les octets circulant sur la liaison. Avant d'entreprendre le décodage de ces valeurs, rappelons la structure générale de la trame LAP-B émise sur le niveau physique (figure 14.71).

Paquet		Binaire		Hexadécimal
GFI		0001	0000	10
NVL		0001	0011	13
Type paquet		0000	1011	0B
L. appelant	**L. Appelé**	0000	1001	09
Adresse appelé		0001	0111	17
		0101	0000	50
		0001	0000	10
		0000	1000	08
	0 0 0 0	1001	0000	90
Longueur champ facilités		0000	1010	0A
Facturation à l'appelé		0000	0001	01
Oui		0000	0001	01
GFA		0000	0011	03
3		0000	0011	03
Taille paquet		0100	0010	42
Émission		0000	0110	06
Réception		0000	0111	07
Taille fenêtre		0100	0011	43
Émission		0000	0010	02
Réception		0000	0111	07

Figure 14.70 Le codage d'un paquet d'appel.

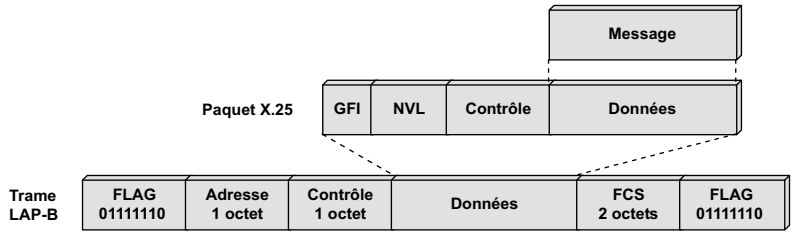


Figure 14.71 La trame LAP-B et paquet X.25

Examen de la trace ligne par ligne

Ligne 1 à 3 ETCD 7E 01 0F 68 B9 7E

Hex	Binaire	Commentaires
7E	0111 1110	Fanion de début de trame, caractérisé par six uns consécutifs. Cette combinaison binaire ne devant pas se retrouver dans le champ d'information, tous les 5 bits à 1, un zéro est inséré, il est retiré à la réception (transparence binaire de la trame HDLC). Les fanions ne seront plus analysés dans la suite du décodage.
01	0000 0001	Champ Adresse, valeur @1. Le champ Adresse présente une difficulté d'interprétation, pour en comprendre la valeur rappelons que l'adresse indiquée est celle de celui qui est ou qui se considère comme l'esclave dans l'échange.
0F	0000 1111	Trame de DM (***Disconnect Mode***), cette trame est émise par le réseau lors de la détection d'une rupture du lien physique. DM est répétée tous les T1. La rupture de la liaison est due à l'insertion de l'analyseur dans le circuit.
68		FCS
B9		FCS, les octets de FCS ne seront plus précisés dans la suite du décodage.

© Dunod – La photocopie non autorisée est un délit

7E	0111 1110	Fanion de fin, ignoré dans la suite.

Ligne 4 ETTD 7E 01 3F EB 7F 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
3F	0011 1111	L'ETTD à la réception d'un état de déconnexion tente le rétablissement de la liaison en émettant la trame (U) ***SABM***.

Ligne 5 ETCD 7E 01 73 83 5E 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
73	0111 0011	ETCD acquitte cette trame par la trame (U) ***UA***, la liaison est rétablie.

Ligne 6 ETCD 7E 03 00 10 00 FB 07 A4 EA 6F 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
00	0000 0000	***Trame d'information***, P/F = 0, Ns = 0, Nr = 0
10	0001 0000 GFI GVL	Le champ d'information contient le paquet X.25-3, le premier quartet correspond au GFI, la valeur 0001 correspond à une utilisation du format normal (numérotation modulo 8). Le N° de groupe de VL est le 0. Cet octet, identique dans le reste de la trace, ne sera plus commenté.
00	0000 0000	Les 8 bits suivants correspondent au Numéro de voie logique, soit le NVL 0. Rappelons que ce NVL est utilisé à des fins de servitude, sauf convention contraire à l'abonnement.
FB	1111 1011	Le troisième octet indique le type de paquet, FB correspond à un paquet de ***demande de reprise***. En effet, la rupture du lien est considérée comme un incident grave, il est nécessaire de rétablir un état propre. Tous les circuits virtuels précédemment établis et maintenus par le réseau vont être détruits, les compteurs Ps et Pr sont réinitialisés à zéro. Le paquet de demande de reprise a été émis sur la VL 0, ce qui est conforme aux spécifications d'X.25.
07	0000 0111	Cet octet précise la cause de la demande de reprise, 7 correspond à une fin d'incident sur le réseau.
A4	1010 0100	Le diagnostic A4 indiqué signifie que l'incident a été détecté suite à une non-réponse à N2 (compteur de retransmission).

Ligne 7 ETTD 7E 03 21 A4 56 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
21	0010 0001	Cette trame est une trame de supervision ***RR***, elle acquitte la trame précédente, Nr = 1 (Compteur Nr, les trois bits de poids fort).

Ligne 8 ETTD 7E 01 20 10 00 FF 8D 06 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
20	0010 0000	Il s'agit d'une ***trame d'information*** (premi er bit à 0), les compteurs valent Ns = 0 (première trame d'information émise), Nr = 1 (1 trame reçue).
10	0001 0000	GFI et Groupe de voies logiques.
00	0000 0000	NVL = 0
FF	1111 1111	Ce paquet est le paquet de ***confirmation de reprise***. La reprise étant acceptée par l'ETTD.

Ligne 9 ETCD 7E 01 21 14 98 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
21	0010 0001	Trame de supervision *RR*, Nr = 1.

Ligne 10 ETTD 7E 01 22 10 03 0B 09 19 20 20 59 30 02 01 01 C4 01 00 67 89 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
22	0010 0010	***Trame d'information*** (I), Nr = 1, Ns = 1.
10	0001 0000	GFI et numéro de groupe de VL.
03	0000 0011	Le paquet a été émis sur le CV 3. Le paquet est sortant.
0B	0000 1011	Il s'agit d'un ***paquet d'appel sortant***. Les données relatives à cet appel suivent.
09	0000 1001	Longueur adresse appelant = 0 ; longueur adresse appelé : 9 quartets.
19	0001 1001	L'adresse est codée en DCB avec un chiffre par quartet, de ce fait :
20	0010 0000	L'adresse est directement lue, il s'agit de :
20	0010 0000	1 92 02 0593
59	0101 1001	
30	0011 0000	Le dernier quartet est un quartet de bourrage.
02	0000 0010	Longueur du champ Facilités
01	0000 0001	Facilité de taxation au demandé ou (et) sélection rapide suivant la position des bits de l'octet suivant.
01	0000 0001	Taxation au demandé.
C4	1100 0100	Données utilisateur
01	0000 0001	idem.
00	0000 0000	idem.

© Dunod – La photocopie non autorisée est un délit

Ligne 11 ETCD 7E 01 41 12 14 7E

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
41	0100 0001	Trame de supervision ***RR***, Nr = 2.

Ligne 12 ETCD 7E 03 42 10 03 0F 70 A9 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
42	0100 0010	***Trame d'information***, Ns = 1, Nr = 2.
10	0001 0000	GFI ...
03	0000 0011	NVL = 3
0F	0000 1111	***Paquet d'acceptation d'appel***, le paquet d'appel a été accepté par l'ETTD distant, le niveau 3 est établi.

Ligne 13 ETTD 7E 03 41 A2 DA 7E

Hex	Binaire	Commentaires
03	0000 0011	Adresse, @3
41	0100 0001	Trame de supervision ***RR***, Nr = 2

Ligne 14 ETTD

```
7E 01 44 10 03 00 E0 00 00 01 00 20 08 00 10 00
C2 00 50 49 00 08 08 00 00 00 50 52 00 08 00 00
0E 60 50 6B 00 14 02 00 00 23 01 00 10 01 18 50
C9 05 00 00 00 00 01 24 7E
```

Hex	Binaire	Commentaires
01	0000 0001	Adresse, @1
44	0100 0100	***Trame d'information***, Ns = 2, Nr = 2.
10	0001 0000	GFI ...
03	0000 0011	NVL = 3.
00	0000 0000	Type de paquet, ***paquet de données*** Ps = 0, Pr = 0.
E0	1110 0000	Champ de données, il correspond à un rétablissement de la connexion de transport en environnement propriétaire DSA (BULL).

...

Le schéma de la figure 14.72 représente le diagramme des échanges.

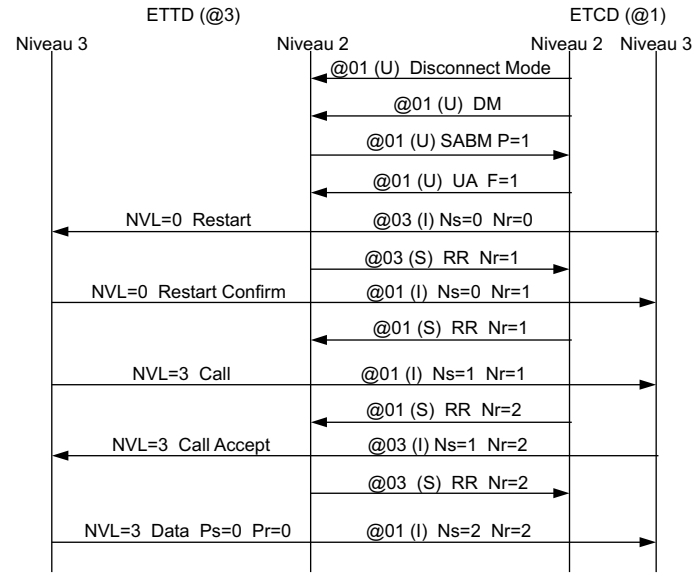


Figure 14.72 Le dialogue ETTD/ETCD suite à une rupture du lien physique.

Exercice 14.3 Définition d'un protocole

1) Valeur optimale de la taille de l'unité de données :cette valeur correspond au minimum de la fonction *Tp*. Il convient donc de rechercher la valeur de *p* qui annule la dérivée première :

$$Tp = \frac{L + pH}{D}\left(1 + \frac{N}{p}\right) \qquad \text{soit} \qquad Tp = \frac{L}{D} + \frac{LN}{Dp} + \frac{pH}{D} + \frac{HN}{D}$$

$$T'(p) = -\frac{LN}{Dp^2} + \frac{H}{D}$$

La valeur qui annule cette fonction est :

$$p = \sqrt{\frac{LN}{H}} = \sqrt{\frac{1500 \times 3{,}25}{5}} = 31{,}225 \text{ paquets (seule la solution positive est retenue !)}$$

L'étude des variations de la fonction ou du signe de la dérivée seconde montre qu'il s'agit bien d'un minimum. Ce qui correspond à une longueur de paquets de :

$$Lp = \frac{1500}{31{,}225} = 48 \text{ octets}$$

2) Contrôle de flux : pour déterminer l'efficacité de contrôle de flux, il convient de définir l'inertie du système. C'est-à-dire combien de paquets seront envoyés entre le paquet saturant et la réception du message de demande d'arrêt.

Si on tient compte du temps de transfert sur le réseau, cette valeur correspond au nombre de paquets (W) émis pendant le trajet aller et retour entre deux nœuds d'un message (Ta) soit :

$W = Ta/tb$ où *tb* correspond au temps d'émission d'un paquet

© Dunod – La photocopie non autorisée est un délit

En interne au réseau

$Ta = 2 \cdot 10^5/2 \cdot 10^8 = 1$ ms
$tb = (53 \times 8) / 622 \cdot 10^6 = 0{,}68 \cdot 10^{-6}$ s
$W = 10^3/0{,}68 \cdot 10^{-6} = 1470$

Soit 1 470 paquets de 53 octets qui auront été émis inutilement. Ce mode de contrôle de flux est inefficace (temps de réaction) sans compter que ces paquets devront être mémorisés pour être retransmis !

À l'interface usager

$Ta = 4 \cdot 10^4/2 \cdot 10^8 = 2 \cdot 10^{-4}$
$tb = (53 \times 8) / 2{,}048 \cdot 10^6 = 0{,}207 \cdot 10^{-3}$
$W < 1$

Dans ce cas, le contrôle de flux peut être très efficace, l'émission cesse immédiatement.

Dans ce réseau on pourrait donc envisager un contrôle de flux à l'interface usager/réseau, et aucun contrôle en interne au réseau.

3) Nombre de connexions simultanées (nombre de CV) : si *n* en bits est la capacité de numérotation des CV, le nombre de CV est 2^n. Dans notre cas $N = 2^{28} = 268\,435\,456$.

4) Taux d'erreur dans le réseau

a) Probabilité qu'un paquet transite sans erreur sur 1 lien

Si *Teb* est la probabilité qu'un bit soit erroné, la probabilité qu'un bit ne le soit pas est de $1 - Teb$
pour un bloc de *N* bits : $P_a = (1 - Teb)^N$
avec $Teb = 10^{-9}$, $N = 53 \times 8 = 424$ bits

b) Pour l'ensemble des 3,25 nœuds soit 4,25 liens traversés par un paquet :

$P_b = P_a{}^9 = (1 - Teb)^{4{,}25\,N} = (1 - 0{,}000000001)^{1802} = 0{,}999998198$

c) Taux d'erreur pour l'ensemble du réseau

$Teb' = 1 - 0{,}999998198 = 0{,}000001801$ soit $1{,}8 \cdot 10^{-6}$

5) Temps de traversée du réseau et gigue : il n'est pas possible de borner le temps de transit dans le réseau. Le temps minimal correspond au cas où aucune erreur ne se produirait (*Tmin*), dans tous les autres cas, le temps dépend du nombre de reprises sur erreur réalisées, suite aux erreurs, dans le réseau, la gigue ne peut donc être estimée.

6) Modem d'accès distant

Débit maximal envisageable sur le lien :

$$C = BP \log_2\left(1 + \frac{S}{N}\right) = 3100 \log_2(1001) \approx 3100 \times 10 = 31000 \text{ bit/s}$$

Valence du signal :

Le modem envisagé utilise une modulation de phase et d'amplitude à 16 états (MAQ16). Est-ce réalisable ? La valence maximale compte tenu du rapport signal à bruit est :

$$v = \sqrt{1 + \frac{S}{N}} = \sqrt{1001} = 31{,}6$$

Rien ne s'oppose donc à l'utilisation d'une modulation MAQ16

Débit du modem :

$$D = 2BP \log_2 v = 2(3400 - 300) \log_2 16 = 2 \times 3100 \times 4 = 24\,800 \text{ bit/s}$$

Exercice 14.4 Protocole ATM

Chaque commutateur ATM réalise la fonction d'adaptation des débits par l'insertion et l'extraction de cellules vides. Les cellules vides sont identifiées par une valeur spécifique de l'en-tête : 0x00-00-00-01 ou seul le bit CLP (priorité à l'écartement est positionné). L'utilisation de cellules vides interdit donc l'emploi de la liaison virtuelle de VPI/VCI 0/0.

Exercice 14.5 Priorité ou réservation de ressources

Si l'implémentation des protocoles à niveaux de priorité est plus simple que celle des protocoles à réservation de ressource, ils nécessitent un surdimensionnement des réseaux or, si le réseau est largement surdimensionné la notion de priorité n'a plus d'utilité.

Cependant, aucune prévision sur les trafics soumis ne peut être réalisée, une surcharge du réseau peut toujours se produire et dans ces conditions tous les flux sont pénalisés y compris les flux prioritaires.

Enfin, si tous les flux sont prioritaires, la notion de priorité n'a aucune utilité.

Seuls, les systèmes à réservation de ressources sont susceptibles de satisfaire pleinement les exigences des flux isochrones. Cependant, ces systèmes nécessitent un système de signalisation beaucoup plus complexe et un trafic de gestion du réseau plus important.

Exercice 14.6 Évolution de l'encapsulation d'IP

Type d'encapsulation	Mise en œuvre	Caractéristiques
IP/ATM/SDH/WDM	Solution actuelle la plus utilisée par les opérateurs pour transporter IP.	L'avantage essentiel est l'utilisation de l'existant. Le flux IP peut bénéficier de la qualité de service d'ATM (transport de la voix et de la vidéo).
IP/SDH/WDM	Utilisation directe des boucles SDH existantes	Gain d'« *overhead* », mais IP directement sur une couche de multiplexage n'assure pas l'utilisation optimale de la bande passante.
IP/WDM	Réalisation de réseau intégralement IP par liaison optique directement entre les routeurs IP.	Permet de garantir l'homogénéité du traitement de la qualité de service (IP de bout en bout). L'optimisation de la bande passante peut être obtenue par l'utilisation de MPLS (G-MPLS)

Figure 14.73 L'encapsulation IP.

© Dunod – La photocopie non autorisée est un délit

CHAPITRE 15

Exercice 15.1 Routage et commutation

La figure 15.31 illustre succinctement les différences entre les deux modes d'acheminement.

Critères	Mode orienté connexion	Mode non connecté
Mise en relation nécessaire	Obligatoire.	Non.
Délai de connexion Délai de déconnexion	Oui, pouvant être important.	Non, puisque pas de connexion.
Type de circuit offert	Permanent durant tout l'échange.	Pas de circuit réservé, mode datagramme.
Allocation de ressources	Oui, statique (à la connexion).	Non.
Contrôle de flux possible	Oui.	Non.
Séquencement des informations	Oui (garanti par le réseau).	Non (à charge du destinataire).
Reprise sur incident	Oui.	Non.
Complexité	Couche réseau	Couche transport
Optimisation des réseaux	Non, circuits et ressources réservés durant toute la relation.	Oui, pas de ressource réservée, optimisation lors du routage.
Résistance à la défaillance	Non, en cas de défaillance, il faut reconstituer un circuit virtuel.	Oui, pas de chemin préétabli, en cas de défaillance d'un lien ou d'un nœud reroutage sur une autre voie.
Adressage	Simplifié, label attribué à la connexion.	Complet, chaque bloc de données (paquet) contient l'adresse complète source et destination.

Figure 15.31 Le routage et la commutation.

D'une manière générale, les réseaux à commutation nécessitent l'établissement de routes par un protocole plus ou moins complexe. En utilisant les protocoles de routage traditionnels du monde IP, MPLS facilite la construction des routes et apporte à la commutation la robustesse des réseaux datagrammes sans les inconvénients (déséquencement des informations...). Synthèse entre les deux modes de fonctionnement des réseaux (figure 15.32), MPLS est promis à un avenir certain dans les réseaux d'opérateurs.



Figure 15.32 MPLS, synthèse entre routage et commutation.

CHAPITRE 16

Exercice 16.1 Adressage MAC, type d'adresse

1) Format de l'adresse MAC (figure 16.51)

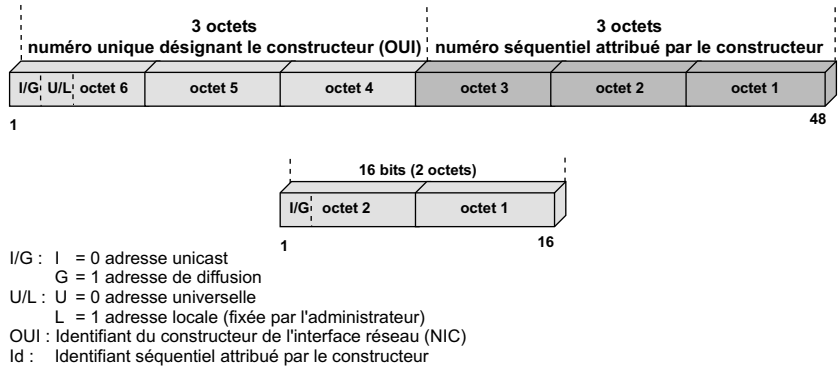


Figure 16.51 L'adressage MAC.

2) Adresses de réponse : un coupleur réseau doit pouvoir répondre aux adresses : *unicast*, *multicast* et *broadcast*.

3) Type d'adresse correspondant à l'adresse MAC 01-00-5E-AB-CD-EF : sachant que pour l'IEEE, les bits de poids faible sont émis devant (numérotation des bits de 0 à 31 de gauche à droite, format canonique), l'adresse 01-00-5E-AB-CD-EF est une adresse de type *multicast*. Le premier octet 0x01, noté selon l'IEEE, donne en binaire 10000000. Il s'agit donc d'une adresse de diffusion.

Une adresse source peut-elle être une adresse de diffusion ? Une adresse de diffusion adresse toutes les machines présentes sur le réseau, un message ne peut avoir pour origine toutes les machines ! Par conséquent, une adresse source ne peut être une adresse de diffusion. Cette évidence est utilisée dans les réseaux 802.5 (Token Ring), où le bit G=1 du champ adresse source est utilisé pour indiquer que le champ données contient des informations de routage par la source (Champ RI).

4) Type d'application : l'application peut être de la diffusion vidéo.

Exercice 16.2 Notation canonique et non canonique

Le format IEEE, dit canonique, correspond à l'écriture des octets bits de poids faible devant, le format non canonique à l'écriture naturelle. Ainsi, la valeur non canonique 1 vaut en écriture canonique 128. Passer de la forme canonique à la forme non canonique, ou l'inverse, correspond donc à inverser l'ordre des bits. Les écritures sont différenciées par les séparateurs, le tiret « - » pour la forme non canonique et deux points « : » pour la forme canonique.
Aussi, l'adresse de diffusion générale s'écrit :
FF-FF-FF-FF-FF-FF en format non canonique et FF:FF:FF:FF:FF:FF en format canonique.

© Dunod – La photocopie non autorisée est un délit

Exercice 16.3 Comparaison des topologies et méthodes d'accès

La figure 16.52 présente une comparaison succincte des topologies, en ne retenant que les topologies de base : bus, étoile et anneau.

Topologie	Avantages	Inconvénients
Bus	Diffusion aisée de messages. Insertion de stations sans interrompre le trafic.	Collision de messages. Limitation des distances (atténuation)
Étoile	Diffusion aisée par le concentrateur. Conflit d'accès réglé par le concentrateur. Insertion de stations sans interrompre le trafic, mais nécessite généralement une reconfiguration du concentrateur.	Sensibilité à la défaillance du concentrateur. Nombre de stations limité par le nombre de ports disponibles. Performances liées à la puissance de calcul du nœud.
Anneau	Liaison point à point, ce qui facilite l'utilisation de la fibre optique. Régénération du signal par chaque station, ce qui augmente la portée du réseau.	Diffusion difficile. L'insertion de stations rompt l'anneau. Complexité du coupleur (retrait et insertion d'information).

Figure 16.52 Comparaison des topologies de base.

La figure 16.53 présente une brève comparaison des principales méthodes d'accès.

Méthode d'accès	Avantages	Inconvénients
CSMA/CD	Simplicité de l'algorithme. Excellente performance à faible charge.	Les collisions pénalisent rapidement les performances dès que la charge augmente. Accès non équitable et non déterminé (accès probabiliste).
Jeton adressé	Accès déterministe et équitable. Mécanisme de priorité. Synchronisation des horloges (circulation permanente d'un message). Pas d'effondrement à forte charge.	Reconfiguration de l'anneau logique à chaque ajout ou retrait de station. Complexité de l'algorithme d'accès.
Jeton non adressé	Accès déterministe et équitable. Mécanisme de priorité.	Difficulté de gestion de l'anneau (station de surveillance). Insertion et retrait des données.

Figure 16.53 Comparaison des principaux algorithmes d'accès.

Exercice 16.4 Longueur virtuelle de l'anneau 802.5

Insérer une station revient à allonger le temps de parcours d'un temps bit, donc à augmenter la longueur virtuelle de l'anneau de la taille d'un bit. La taille d'un bit (L) est donnée par :

$$L = \text{durée d'un bit} \times \text{vitesse de propagation} = t \times V$$

avec V vitesse de propagation égale à $V = \nu \times c$,
où ν est le coefficient de vélocité du câble,
c est la vitesse de la lumière.

$$V = (2/3) \times 3 \cdot 10^8 = 2 \cdot 10^8 \text{ m/s} \Rightarrow 200 \text{ m/}\mu\text{s}$$
$$t = 1/\text{ Débit} = 1 / (4 \cdot 10^{-4}) = 0{,}25\ \mu\text{s}$$
$$L = 0{,}25 \times 200 = 50 \text{ m}$$

L'insertion d'une station accroît la longueur virtuelle de l'anneau de 50 m.

Exercice 16.5 Efficacité du protocole 802.5 à 100 Mbit/s

Le débit du réseau réel peut être mesuré par le rapport entre la longueur en bits du message à émettre et le temps d'occupation du réseau (laps de temps avant l'émission suivante).

Temps d'occupation du support

– Temps d'occupation du support = T de transmission + T de rotation + T de retard
– Temps de transmission = $(L \times 8) / 100 \cdot 10^6 = 0{,}36$ ms
– Temps de rotation = (Distance / vitesse) = 200 / 200 000 = 1 ms
– Temps de retard = Retard une station × Nombre de stations
– Temps de retard d'une station = 1 temps bit = $1 / 100 \cdot 10^6 = 10^{-8}$ s
– Temps d'occupation (en ms) = $0{,}36 + 1 + 10^{-5} = 0{,}36 + 1 + 0{,}01 = 1{,}37$ ms

Efficacité du réseau

Débit = Longueur du message / Temps d'occupation
= $(4\ 500 \times 8) / 1{,}37 \cdot 10^{-3} = 26{,}3$ Mbit/s

L'efficacité de ce réseau n'est que d'environ 25 %.

Les réseaux à jeton à haut débit implémentent un protocole similaire au 802.5 mais autorisent plusieurs jetons sur le réseau, c'est le cas notamment du réseau Token Ring à 16 Mbit/s d'IBM, et du FDDI.

Exercice 16.6 Détermination du temps d'accès

1) Temps d'attente du jeton : le cas le plus défavorable correspond à l'attente active du jeton par une station (la station désire émettre) alors que le jeton est détenu par la station qui la suit dans l'anneau et que toutes les stations sont aussi en attente active et utilisent leurs temps de parole au maximum.

Temps d'occupation de l'anneau par chaque station :

Temps d'émission + temps de rotation + retard apporté par les stations traversées

avec :

Temps d'émission = 10 ms
Temps de rotation (longueur de l'anneau / vitesse) soit $(50 \times 50) / 200 = 12{,}5\ \mu$s
Temps de retard vaut :

$$\text{Temps bit} \times \text{NB stations} = (1/4 \cdot 10^{-6}) \times 50 = 0{,}25\ \mu\text{s} \times 50 = 12{,}5\ \mu\text{s}$$
$$T = 10 + 0{,}0125 + 0{,}0125 = 10{,}025 \text{ ms}$$

© Dunod – La photocopie non autorisée est un délit

Pour les $N - 1$ stations du réseau qui vont émettre avant :

$$\text{Temps d'attente du jeton} = 49 \times 10{,}025 = 491{,}225 \text{ ms soit} \approx 1/2 \text{ seconde}$$

2) Débit utile pour cette station

Efficacité = Temps d'émission / Temps total = 10 / 491 = 0,02 soit 2 %
le débit effectif pour cette station est de : 4 Mbit $\times$ 0,02 = 80 000 bit/s

Notons que ce débit correspond à la bande passante totale du réseau divisé par le nombre de stations !

3) Réseaux CSMA/CD : ce calcul n'est pas réalisable pour un réseau Ethernet, on ne peut que calculer la probabilité d'accès au média pendant un intervalle de temps. Le CSMA/CD est dit probabiliste alors que le 802.5 est dit déterministe puisque l'on peut déterminer une borne maximum au droit à parole.

Exercice 16.7 Adresses auxquelles répond une station

1) Adresses de réponse des stations 10.75.18.30 et 10.203.125.7

Adresses	Type d'adresse	Sous-réseau 1	Sous-réseau 2
	Unicast	10.75.18.30/16	10.203.125.7/16
I	Groupe *Multicast*	224.75.161.12	224.203.161.12
P	Diffusion limitée	255.255.255.255	255.255.255.255
	Diffusion dirigée	10.75.255.255	10.203.255.255
M	*Unicast*	00-01-02-03-05	00-01-02-04-06
A	*Broadcast*	FF-FF-FF-FF-FF-FF	FF-FF-FF-FF-FF-FF
C	*Multicast*	01-00-5E-46-A1-0C	01-00-5E-46-A1-0C

Figure 16.54 Les différentes adresses d'une station.

- **Adressage IP** : l'adressage de diffusion limitée est utilisé par une station pour envoyer un message à toutes les machines situées sur le même segment qu'elle. Dans l'adresse de diffusion limitée ou *broadcast,* tous les bits sont positionnés à 1.
  L'adressage de diffusion dirigée adresse toutes les stations d'un sous-réseau. Seuls les bits du champ Net-ID sont à 1.
- **Adressage MAC** :
  - L'adressage de *broadcast* est aussi défini par tous les bits à 1.
  - L'adresse MAC *multicast* est obtenue par addition de : 01-00-5E-00-00-00 et des 23 derniers bits de l'adresse IP du groupe multicast.

2) Performances des stations : lorsque les adresses IP ne diffèrent que des 23 derniers bits, les adresses MAC résultantes sont identiques. Dans cet exercice, les deux stations ont la même adresse MAC *multicast*, c'est-à-dire qu'elles reçoivent les données de l'autre groupe *multicast*, ce qui pénalise les performances des stations. L'affectation d'adresses *multicasts* doit tenir compte de cette possibilité afin de créer des groupes indépendants au niveau MAC.

Exercice 16.8 FDDI et Token Ring

	Token Ring	FDDI
Débit	4 ou 16 Mbit/s	100 Mbit/s
Technique d'accès	Jeton non adressé et technique de l'ERT (version 16 Mbit/s)	Jeton non adressé, temporisé et technique de l'ERT
Codage	Manchester différentiel	4B/5B et NRZI
Unité de données	4 500 octets (4 Mbit/s) 18 000 octets (16 Mbit/s)	4 500 octets
Priorité	8 niveaux	8 niveaux
Topologie	Simple anneau (version IBM, double anneau)	Double anneau
Distance	300 m entre stations Portée quelques km	2 km entre stations 100 km

Figure 16.55 Comparaison FDDI/Token Ring.

Exercice 16.9 Données de la classe Isochrone

Traditionnellement, le transport de la voix nécessite de garantir la délivrance des échantillons (valeur) à un rythme précis, soit un échantillon toutes les 125 μs. Ceci nécessiterait dans FDDI-I que le TTRT (*Target Token Rotation Time*) soit de 125 μs. Ce qui compte tenu du diamètre envisageable pour le réseau est inconcevable (100 km à $2 \cdot 10^8$ m/s correspond à un temps de 0,5 ms). C'est pour cette raison que les réseaux FDDI-II et DQDB ont organisé le transfert de données à partir de trames dont la fréquence de récurrence est de 8 000 Hz (période de 125 μs).

Cependant, la technique du jeton temporisé est tout à fait à même d'assurer un transfert de la voix en mode paquet, les contraintes temporelles étant alors moins strictes. Un paquet voix de 20 octets requiert un TTRT de 2,5 ms (20×125 μs).

Exercice 16.10 Rotation des données sur le réseau FDDI

La circulation des données est illustrée figure 16.56. Dans le schéma 1, la station A a acquis le jeton et émet sa trame. En 2, après l'émission de sa trame elle génère un jeton sur le réseau. En 3, C reconnaît son adresse, il recopie la trame. Pendant ce temps, en 4, B acquiert le jeton et émet ses données. À l'instar de A, à la fin de son émission, il insère un jeton. En 5, A reçoit les données qu'il a émises, il les retire de l'anneau. Il n'a pas besoin de régénérer un jeton puisqu'il l'a déjà fait après son émission de données (**ETR**, *Early Token Release*). En 6, D a reconnu son adresse, il recopie les données. Il n'y a plus que les données de B sur le réseau que ce dernier retirera lorsqu'elles lui arriveront.

© Dunod – La photocopie non autorisée est un délit

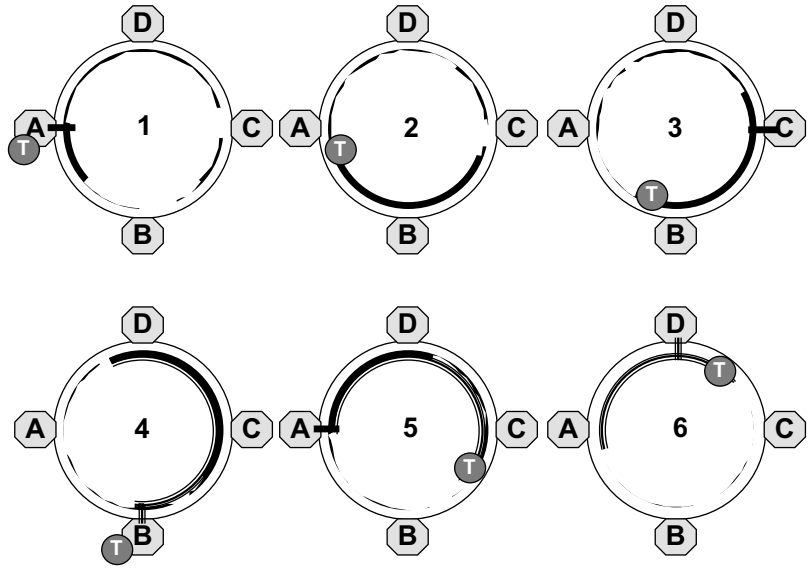


Figure 16.56 La circulation des données dans le réseau FDDI.

CHAPITRE 17

Exercice 17.1 Distinction entre CSMA/CD IEEE 802.3 et Ethernet

La figure 17.65 rappelle le format de la trame IEEE 802.3. Ethernet et 802.3 se distinguent par l'octet « longueur des données ». Le champ Longueur des données exprime, en 802.3, la longueur des données utiles de la trame MAC. En Ethernet ce champ identifie le protocole de niveau supérieur, charge à ce dernier de distinguer les données utiles d'éventuelles données de bourrage.

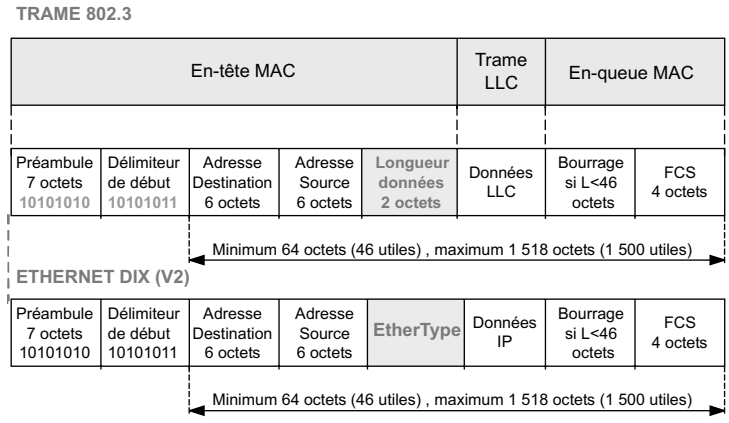


Figure 17.65 Le format de la trame Ethernet/IEEE 802.3.

La longueur des données utiles est, au maximum, de 1 500 octets (0x05DC). Toute valeur de ce champ supérieure à 1 500 identifie un protocole et non une longueur de données. Par exemple, la valeur 2 048 (0x0800) identifie le protocole IP de la pile TCP/IP.

Exercice 17.2 Séquence de synchronisation bit en 802.3 et 802.5

Un réseau 802.3 est caractérisé par l'asynchronisme des émissions, il peut y avoir de longs temps de silence entre deux messages. La dérive des horloges peut être importante (réseau plésiochrone), ce qui justifie la longue séquence de resynchronisation.

En 802.5, même en l'absence de communication entre les stations, le jeton circule. Les stations sont donc périodiquement resynchronisées (réseau synchrone) ; la séquence de synchronisation peut être supprimée.

Exercice 17.3 Transmission synchrone et protocole 802.3

Non, il est inconcevable sur un support partagé à canal unique de maintenir, à des fins de synchronisation, une activité. Plusieurs raisons peuvent être évoquées :

– La raison essentielle est le protocole d'accès au support lui-même. En effet, une station qui désire acquérir le support doit attendre le silence sur celui-ci, ce qui interdit tout trafic en dehors du trafic utile.
– Pour maintenir une synchronisation permanente des stations, il conviendrait de modifier le protocole d'accès. Une station dite maître assurerait un *polling* des autres stations, ce *polling* maintiendrait une activité sur le bus. Il serait alors nécessaire de définir un ordonnancement du *polling* et, pour respecter le principe de la décentralisation de la politique d'accès des réseaux locaux, d'admettre que chaque station puisse être maître, le maître serait désigné par un processus électif et le *polling* remplacé par un jeton. Ce ne serait plus du 802.3 mais du 802.4 (Token Bus).

Exercice 17.4 Rapidité de modulation

Le réseau 802.3 utilise le codage Manchester (biphase), ce type de codage se caractérise par une transition au milieu de chaque temps bit. La suite étant continue et de même valeur, il y a une alternance du signal par temps bit. La période du signal vaut un temps bit, il y a donc deux changements d'état par temps bit ; la rapidité de modulation est le double du débit soit 20 Mbauds.

Autre explication : le codage Manchester correspond, au niveau électrique, à un codage nB/mB. En effet un 0 correspond à l'émission de 01 (niveau électrique) et un 1 à celle de 10.

La vitesse de signalisation sur la ligne ou rapidité de modulation est bien le double du débit binaire.

Exercice 17.5 Conception d'un réseau Ethernet à 100 Mbit/s

Le fonctionnement du CSMA/CD repose sur la possibilité de détection des collisions par toute station qui émet. La **fenêtre de collision** correspond à deux fois la durée de propagation entre les deux stations les plus éloignées ce qui, ici, correspond à :

$$\textit{Time Slot} = (2 \times 200) / 200\,000 = 2 \text{ ms}$$

Le temps d'émission de la plus petite trame doit être d'au moins 2 ms.

© Dunod – La photocopie non autorisée est un délit

Temps effectif d'émission d'une trame de 4 500 octets :

$$T = \text{Longueur Trame / Débit} = (4\,500 \times 8) / 100 \cdot 10^6 = 0{,}36 \text{ ms}$$

La durée d'émission est très faible devant le *Time Slot*. Pour détecter les collisions, il sera nécessaire de compléter toutes les trames émises par du bourrage.

Le protocole CSMA/CD ne peut convenir à cette réalisation. Le message minimum devrait avoir pour longueur :

$$\text{Longueur en bits} = \textit{Time Slot} \times \text{Débit}$$

$$L = 2 \cdot 10^{-3} \times 100 \cdot 10^6 = 200 \cdot 10^3$$

$$L_{\text{octets}} = 200\,000 / 8 = 25\,000$$

Soit une trame de 25 000 octets ce qui, compte tenu du fait que la MTU du réseau est fixée à 4 500 octets, un bourrage minimal de 20 500 octets. Ce qui réduit le débit à :

$$\text{Débit nominal (taille utile/taille émise)} = 100\,(4\,500 / 25\,000) = 18 \text{ Mbit/s}$$

Pour un débit nominal de 100 Mbit/s, le débit réel effectif n'est que de 18 Mbit/s, la faiblesse de ce débit est le résultat d'opérations de bourrage importantes : au minimum 20 500 octets. Ce résultat provient d'une fenêtre de collision trop importante. Le protocole CSMA/CD est donc un mauvais choix. Les concepteurs doivent s'orienter vers un protocole plus efficace sur une telle distance comme le sont les protocoles à jeton.

Exercice 17.6 Plan d'adressage d'une entreprise

Ce problème a plusieurs solutions, celle exposée n'en est qu'une parmi d'autres.

Adressage du réseau – L'adresse privée 10.0.0.0 est une adresse de classe A, c'est-à-dire qu'elle comporte un octet d'identification du réseau (Net_ID) et 3 octets pour numéroter les stations (Host_ID).

On doit pouvoir distinguer les sites et dans chaque site 10 sous-réseaux. Une solution simple consiste à réserver le second octet à l'identification des établissements en adoptant le numéro de département. Le troisième octet peut alors être utilisé pour numéroter les sous-réseaux, le quartet de poids fort étant suffisant (2^4). Dans ces conditions, l'adresse réseau est 10.0.0.0 et le masque de sous-réseau 255.255.240.0.

Adressage des liaisons – Deux techniques peuvent être utilisées pour adresser les liaisons : soit considérer chaque LL comme un réseau (adressage point à point), soit considérer l'ensemble des LL du réseau comme appartenant au même réseau. La première technique, plus simple, sera utilisée ici. L'adressage des LL peut être quelconque, ces adresses ne sont utilisées que par les routeurs pour choisir le port de sortie (identification d'un port), dans ces conditions elles ne sont jamais vues de l'extérieur. La figure 17.66 illustre l'une des solutions possibles.

Pour identifier les liaisons nous avons adopté une numérotation significative de classe A :

– le premier octet 80 indique le réseau de LL ;
– le deuxième qu'il s'agit du réseau 10 ;
– les troisième et quatrième octets identifient les extrémités.

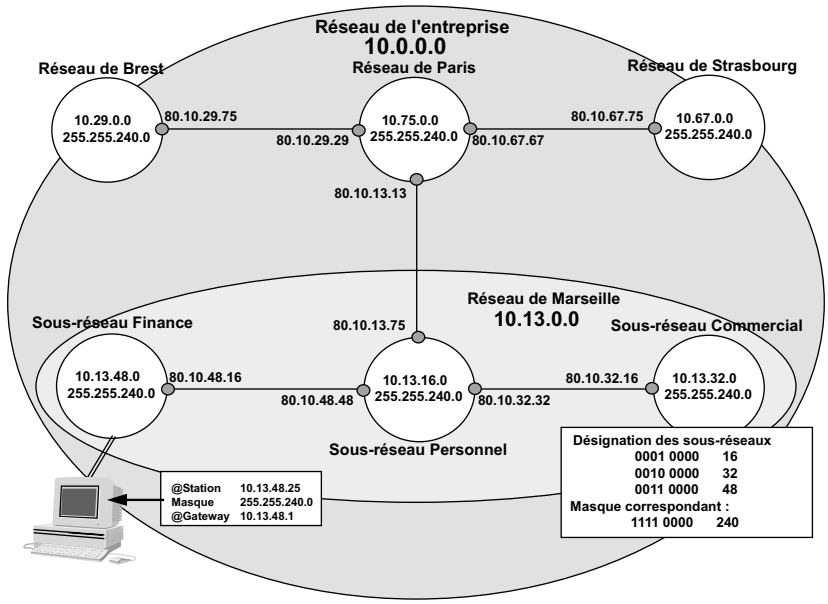
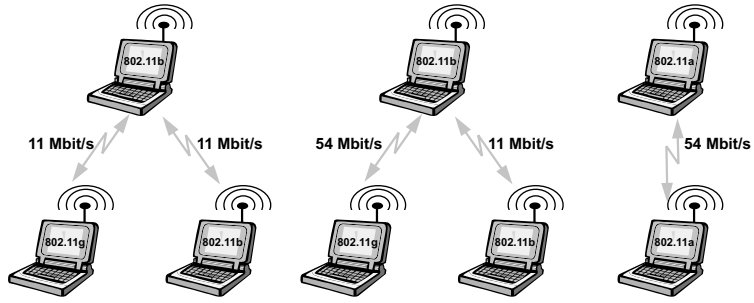


Figure 17.66 Illustration d'une solution envisageable.

Exercice 17.7 Comptabilité des systèmes 802.11b, g et a



	802.11b	802.11g	802.11a
Bande	2,4 GHz	2,4 GHz	5 GHz
Débit	1 à 11 Mbit/s	1 à 54 Mbit/s	6 à 54 Mbit/s
Codage			
1 Mbit/s	DBPSK	DBPSK	
2 Mbit/s	DQPSK	DQPSK	
5,5 Mbit/s	CCK	CCK	
11 Mbit/s	CCK	CCK	
12 – 54 Mbit/s		OFDM	
6 – 54 Mbit/s			OFDM

Figure 17.67 La compatibilité des versions 802.11.

© Dunod – La photocopie non autorisée est un délit

Pour que deux systèmes 802.11 soient compatibles il faut et il suffit qu'ils utilisent une même technique de modulation, de codage et qu'ils offrent des débits similaires (figure 17.67).

Exercice 17.8 Performance des réseaux 802.11

Le débit utile correspond au produit du débit nominal par l'efficacité du protocole. Cette efficacité est égale au rapport du temps d'utilisation du support pour émettre les données utiles au temps total du cycle de transmission.

La figure 17.68 rappelle le principe de l'accès au support, après un temps d'écoute active, si le silence persiste sur le support, l'émetteur poursuit celle-ci d'une durée comprise entre 0 et *x Time Slot* (algorithme *BackOff*) puis transmet ses données. À réception de celles-ci, le destinataire acquitte immédiatement les données reçues.

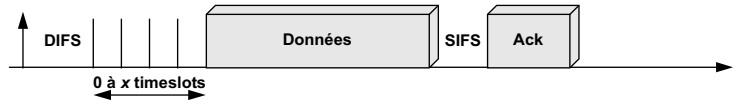


Figure 17.68 Le contrôle de l'accès en 802.11 mode DCF.

Le délai de temporisation de *backoff* est déterminé à partir de la formule :

$$\text{Délai} = \textit{Time Slot} \times \text{Rand}\,(0,\text{CW})$$

avec CW (*Contention Window*) doublant à chaque tentative et dont les valeurs limites (mini, maxi) dépendent de la version (7 à 255, 16 à 1024, 32 à 1 024). Prenons la meilleure hypothèse (7, 255) ; soit, pour la première tentative un délai variant de 0 à 140 μs.

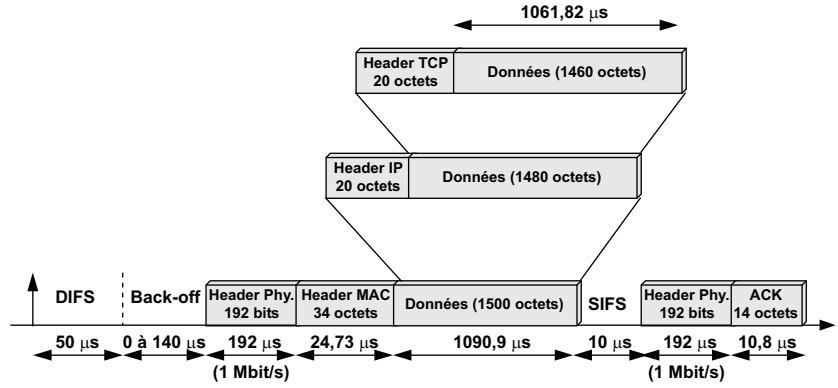


Figure 17.69 Le chronogramme de transmission 802.11b.

La figure 17.69 indique pour chaque période, d'une émission réussie à la première tentative, les différentes durées d'occupation du support. Ces durées et les résultats correspondants sont résumés dans la figure 17.70.

Le débit effectif d'une transmission est largement inférieur au débit nominal. Ceci est dû aux entêtes de message, aux délais d'attente et à l'acquittement. Cet écart entre débit nominal et débit effectif est encore plus important pour le 802.11g/a à 54 Mbit/s puisque le débit utile n'atteint qu'environ 20 Mbit/s.

Durée *backoff*		Durée utile	Durée totale	Efficacité	Débit
Mini	0	1 061,82	1 570,43	0,676	7,43 Mbit/s
Moyen	70	1 061,82	1 640,43	0,647	7,12 Mbit/s
Maxi	140	1 061,82	1 710,43	0,620	6,82 Mbit/s

Figure 17.70 Synthèse des résultats.

CHAPITRE 18

Exercice 18.1 Interconnexion d'un réseau 802.3 et 802.5

L'approche fondamentalement différente des deux réseaux impose une conversion de protocole de niveau MAC. Les différents problèmes à résoudre sont :

a) Passage du réseau 802.3 (Ethernet) au réseau 802.5 (Token Ring)

- reformatage des trames,
- inversion de l'ordre des bits,
- gestion d'une priorité fictive,
- recalcul du FCS,
- la purge de l'anneau par le pont,
- le dimensionnement des *buffers* qui devra être suffisant si le 802.5 n'est qu'à 4 Mbit/s (congestion).

b) Passage du réseau 802.5 (Token Ring) au réseau 802.3 (Ethernet)

- reformatage des trames en générant éventuellement du bourrage,
- inversion de l'ordre des bits,
- recalcul du FCS,
- supprimer les éventuelles priorités,
- acquitter la trame (bit A et C), alors que la station destinataire n'est peut-être pas à l'écoute,
- les *buffers* devront être suffisamment dimensionnés si le 802.5 est à 16 Mbit/s et que le réseau Ethernet est quelque peu chargé (congestion),
- la segmentation si la trame Token Ring est supérieure à 1 500 octets (ou l'élimination).

Exercice 18.2 *Spanning Tree Protocol* (STR)

La démarche consiste à déterminer d'abord le pont racine, puis à calculer les différents coûts à partir de la racine.

Première solution : le pont P1, de plus petit ID, est désigné comme pont *root* (racine). Sur chaque branche, il est très aisé de déterminer le pont élu, c'est celui de moindre coût. La seule difficulté qui subsiste concerne le pont P7. La figure 18.38 représente cet état intermédiaire.

La figure 18.39 cumule les coûts des différentes branches par lesquelles il est possible d'atteindre le port *non-root* du pont P3. Le coût en sortie de P3 est de 15, alors que ce port P3 reçoit une BPDU

© Dunod – La photocopie non autorisée est un délit

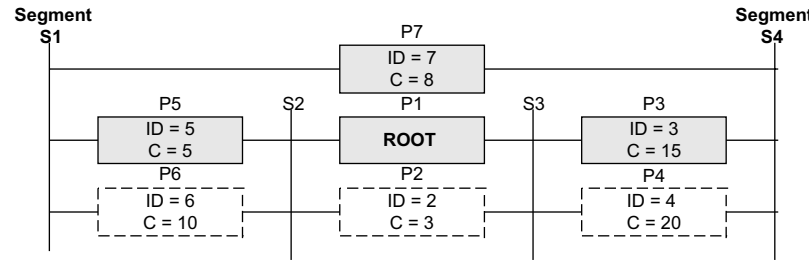


Figure 18.38 Solution intermédiaire.

qui affiche un coût de 13. P3 en déduit qu'il existe un chemin de coût plus faible pour atteindre cette direction, il se met en sommeil (pont *backup*).

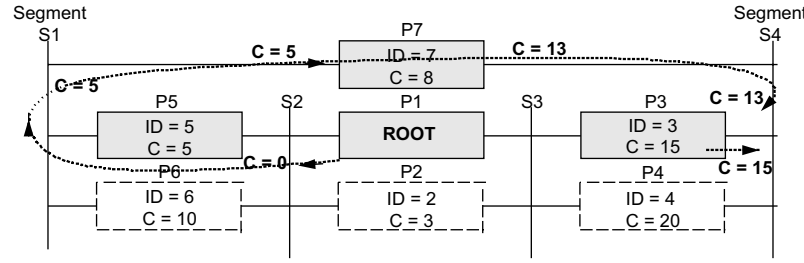


Figure 18.39 La détermination des coûts sur les branches de P7.

Le schéma final, après stabilisation, est donné par la figure 18.40. L'examen de la topologie obtenue montre que le pont P5 doit écouler tout le trafic, il constitue donc le maillon sensible du réseau (débit, fiabilité...).

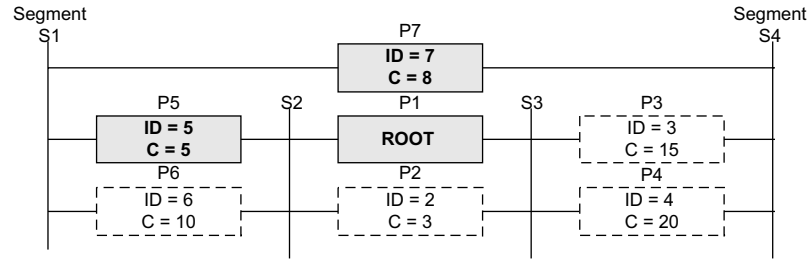


Figure 18.40 La configuration finale du réseau.

Cet état de fait, s'il n'est pas volontaire (coût des liens, conditions particulières d'exploitation, etc.), provient soit d'un mauvais choix du pont *root*, soit d'une mauvaise affectation des coûts.

Deuxième solution : la figure 18.41 propose une alternative devant conduire à une topologie équilibrée. La figure 18.42 donne la topologie finale du réseau : les trafics sont mieux répartis. La figure 18.43 fournit une représentation différente : celle-ci montre l'arborescence des différentes branches et situe les voies de secours (*backup*).

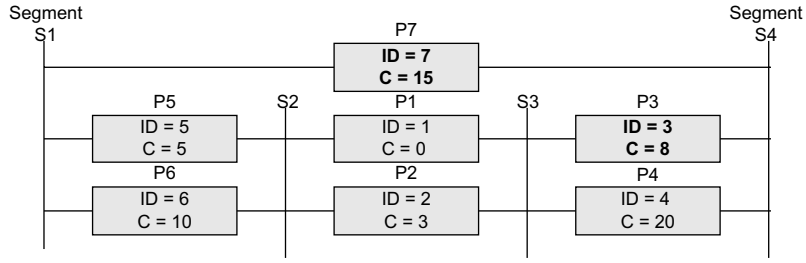


Figure 18.41 Nouvelle définition du réseau.

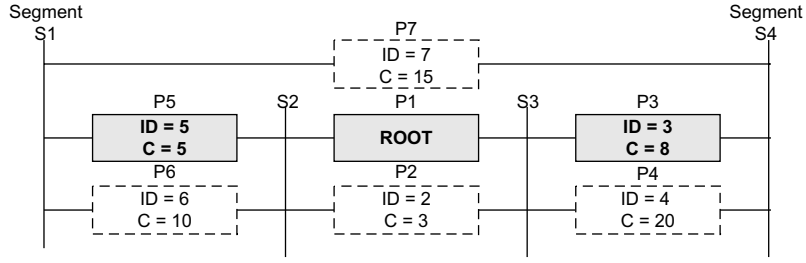


Figure 18.42 Nouvelle configuration du réseau.

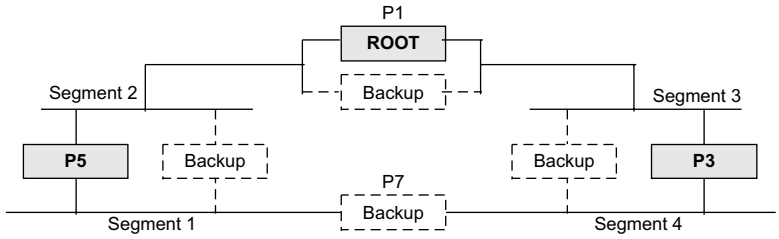


Figure 18.43 L'arbre représentatif du réseau final.

Exercice 18.3 Performances hub/commutateur

1) MTU des réseaux de type Ethernet (version 10 et 100 Mbit/s) : 1 500 octets.

2) Longueur de chaque champ en bits (figure 18.44)

La trame Ethernet varie de 64 octets à 1 518 octets, avec une MTU de 1 500 octets et 8 octets de synchronisation (préambule et délimiteur de début de trame).

L'acquittement ne contient que les en-têtes IP et TCP soit 40 octets, la charge utile minimale étant de 46 octets, il y aura donc 6 octets de bourrage.

3) Temps de latence dans chacun des équipements

– hub, équipement sans latence, retransmission dès réception ;
– commutateur *cut through*, latence égale au délai de réception du champ Source destination, soit 20 octets (40 pour un cycle, préambule 8, adresse 12) ce qui correspond à 320 bits ;

© Dunod – La photocopie non autorisée est un délit

– commutateur *store and forward*, latence égale à la réception complète de la trame, soit 1 518 + 8 pour la trame de données et 64 + 8 pour l'acquittement ce qui donne 1 598 octets ou 12 784 bits.

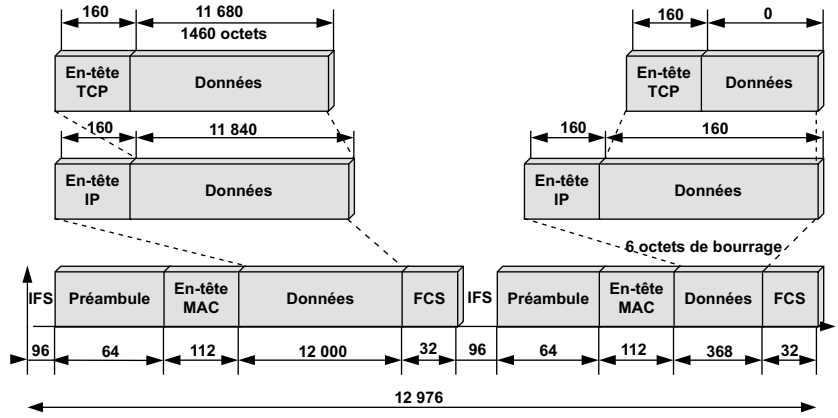


Figure 18.44 Taille des différents champs en bits.

4) Synthèse des résultats (figure 18.45)

Équipement	Volume des données utiles en bits (*1*)	Durée de l'échange en bits (hors temps de latence)	Temps de latence dans l'équipement en bits	Durée totale de l'échange exprimé en bits (*2*)	Efficacité du système Eff = (*1*)/(*2*)
Hub	11 680	12 976	0	12 976	0,9001
Commutateur *cut through*	11 680	12 976	320	13 296	0,8784
Commutateur *store and forward*	11 680	12 976	12 784	25 760	0,4534

Figure 18.45 Performance des systèmes.

5) Mode de fonctionnement du commutateur : dans le sens 10 Mbit/s vers 100 Mbit/s, le commutateur ne peut émettre plus vite qu'il ne reçoit, il doit donc mémoriser la trame avant retransmission. Dans le sens contraire, le commutateur doit aussi mémoriser les données, car il les reçoit plus vite qu'il ne les réémet. Le seul mode possible est alors le mode *store and forward*.

6) Amélioration du mode *cut through* *:* une trame corrompue par une collision est caractérisée par une taille inférieure à 64 octets (fenêtre de collision), il suffit donc de mémoriser la trame et, dès que celle-ci atteint 64 octets, la retransmettre. La latence correspond alors à la mémorisation des 64 octets soit pour un échange 128 octets (1 024 bits) d'où une efficacité de :

$$\text{Efficacité} = 11\,680 / (12\,976 + 1\,024) = 0{,}8342$$

Exercice 18.4 Choix d'un équipement

Caractéristiques du réseau	Critères de choix	Équipement/technologie complémentaire
Peu chargé, et peu de *broadcast*	Performance	Hub (peu chargé, donc pas ou peu de collisions).
Relativement chargé, peu de *broadcast* et d'erreurs	Performance et simplicité de l'administration	Beaucoup de collisions, peu de trafic de *broadcast* : commutateur *cut through.*
Relativement chargé, peu de *broadcast*, de nombreuses erreurs (câblage défectueux)	Performance et simplicité de l'administration	Commutateur *store and forward* (erreur).
Relativement chargé et de nombreux *broadcast*	Performance	Commutateur *cut through* et VLAN
Trafic voix/données	Qualité des liaisons voix	Commutateur *cut through*, VLAN et prioritisation des flux.

Figure 18.46 Choix d'un équipement.

CHAPITRE 19

Exercice 19.1 Protocoles RIP/OSPF

Les principaux éléments de comparaison entre les protocoles RIP et OSPF sont indiqués figure 19.61.

	RIP	OSPF
Caractéristiques		
Type d'algorithme	Vecteur distance	État des liens
Métrique	Nombre de sauts	Coût de la liaison
Métrique configurable	Non	Oui
Origine	IETF	IETF
Architecture du réseau		
Type	À plat	Hiérarchique
Nombre de routeurs	15	Illimité
Routeur maître	Non	Oui
Support des masques de longueur variable	Non	Oui
Performance		
Charge du réseau	Élevée	Faible
Périodicité des mises à jour	30 secondes	3 minutes
Temps de convergence	Plusieurs minutes	Quelques secondes
Mode de mise à jour	Information du voisin	*Multicast*
Support de la qualité de service	Non	Oui
Sécurité		
Authentification	RIP-2	Mot de passe dans chaque paquet

Figure 19.61 Comparaison RIP/OSPF.

Exercice 19.2 Agrégation de routes

1) Nombre d'entrées dans la table du routeur de bordure d'aires du *backbone* sans l'agrégation de routes : à chaque sous-réseau correspond une entrée, le plan d'adressage représenté figure 19.62 indique 16 sous-réseaux par aire, soit un total de 48 entrées dans la table du routeur de bordure.

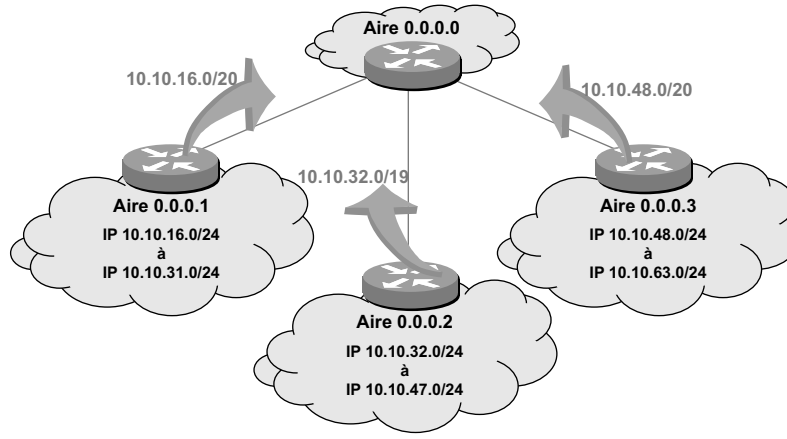


Figure 19.62 Annonces des routes OSPF.

2) Annonces des routeurs de bordure d'aires (figure 19.62) : les annonces correspondent au plus petit masque de sous-réseau commun à tous les sous-réseaux de la zone (adresses contiguës de sous-réseaux). Pour cela nous examinerons l'expression binaire de chacune des adresses réseau (dernier octet d'adresse)

– Aires 1 :

10.10.16.0/24 → 000**1** 0000
10.10.17.0/24 → 000**1** 0001
...
10.10.31.0/24 → 000**1** 1111
Soit la plus petite annonce commune 10.10.16.0/20

– Aires 2 :

10.10.32.0/24 → 00**1**0 0000
10.10.33.0/24 → 00**1**0 0001
...
10.10.47.0/24 → 00**1**0 1111
Soit la plus petite annonce commune 10.10.32.0/19

– Aires 3

10.10.48.0/24 → 00**11** 0000
10.10.49.0/24 → 00**11** 0001
...

10.10.63.0/24 → 00**11** 1111
Soit la plus petite annonce commune 10.10.48.0/20

3) Ordre des entrées dans la table : afin d'éviter toute ambiguïté les adresses, dont le masque est le plus important, sont classées en tête soit :

10.10.48.0/20
10.10.16.0/20
10.10.32.0/19

Exercice 19.3 Adresses multicast

Indépendamment de l'abonnement à un groupe *multicast,* l'adaptateur Ethernet répond aux adresses suivantes :

– son adresse *unicast* : 08-00-02-2D-75-BD ;
– l'adresse de *broadcast* : FF-FF-FF-FF-FF-FF ;

Si la station s'abonne au groupe *multicast* 224.16.21.5, l'adaptateur répondra aussi à l'adresse MAC *multicast* construite à partir de l'adresse de diffusion du groupe *multicast*. Cette adresse est la résultante de la somme de l'adresse MAC réservée 01-00-5E-00-00-00 et des 23 derniers bits de l'adresse de diffusion du groupe (figure 19.63).

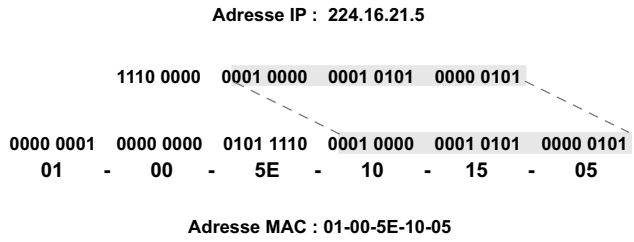


Figure 19.63 Construction de l'adresse multicast.

Exercice 19.4 Comparaison pont/routeur

Le tableau de la figure 19.64 fournit les différents critères de comparaison entre un pont et un routeur.

Indépendamment du facteur coût, ponts et routeurs diffèrent essentiellement par leur performance intrinsèque, le niveau de sécurité qu'ils autorisent et leur facilité de mise en œuvre. Les développements suivants complètent cette comparaison.

A) Comparaison en termes de performance : les ponts agissant au niveau 2 sont, de ce fait, plus efficaces (moins de temps de traitement). Essentiellement recommandés dans les environnements Ethernet en raison de leur faculté à isoler le trafic, ils sont aujourd'hui avantageusement remplacés par les commutateurs.
Cependant, tous les protocoles réseaux utilisent de nombreux messages de diffusion (*broadcast*), les ponts (commutateurs) ne peuvent filtrer ces messages, les routeurs peuvent les filtrer.

© Dunod – La photocopie non autorisée est un délit

	Pont	Routeur
Configuration	Très simple (voire sans)	Complexe
Transparence aux protocoles	Oui	Non (Protocoles routables)
Sécurité (filtre)	Sur adresse MAC	Sur adresse IP (Masque)
Extension du réseau	Aisée	Complexe si routage statique
Trafic de service	Sans, sauf *spanning tree*	Oui, pénalisant
Broadcast	Transparent	Filtre, sauf *broadcast* dirigés
Charge de travail (personnel)	Négligeable	Importante

Figure 19.64 Comparaison pont/routeur.

Dans une configuration utilisant des liens distants, donc à faible débit vis-à-vis du débit sur le LAN, la diffusion consomme une part importante de la bande passante. L'usage des ponts est donc à réserver à l'interconnexion locale.

B) **Comparaison en termes de sécurité** : la sécurité réalisée au niveau applicatif par de simples mots de passe est insuffisante au niveau d'un réseau. Il est nécessaire d'interdire les pénétrations sur le réseau lui-même. Il est évidemment possible de réaliser des filtres sur adresse MAC, mais il est alors nécessaire d'introduire soit la totalité des adresses autorisées, soit la totalité des adresses interdites !
Sur les routeurs, le filtre peut être défini par un ensemble d'adresses IP, ou, à l'aide du masque de sous-réseau, sur la totalité du trafic d'un sous-réseau, ce qui est évidemment plus facile. Certains routeurs peuvent effectuer de véritables translations d'adresse masquant ainsi au monde extérieur les adresses réelles utilisées localement.

C) **Comparaison en termes de facilité de mise en œuvre** : les ponts sont transparents aux protocoles de niveau supérieur, ils ne nécessitent aucune configuration particulière.

D) **Les *bridges* routeurs (B-routeurs)** : la plupart des constructeurs ont développé, dans un même châssis les fonctionnalités des ponts (niveau 2) et des routeurs (niveau 3). Lors de la réception d'une trame, ces équipements examinent son contenu. S'ils reconnaissent un protocole routable (IP, IPX...), la trame est traitée par l'entité routeur. Si le protocole acheminé n'est pas routable (exemple NetBIOS), la trame est alors pontée. Les ponts/routeurs ou B-routeurs sont utilisés dans les environnements multiprotocole et dans les réseaux en phase de migration d'un protocole de type NetBIOS, protocole non routable vers un protocole routable.

Exercice 19.5 Masque de sous-réseau

Les deux stations du réseau représenté figure 19.65 ne peuvent correspondre puisqu'elles sont, vis-à-vis du masque de sous-réseau, sur le même réseau.



Figure 19.65 Le réseau défaillant.

Soit il s'agit d'une erreur de configuration d'une des stations qu'il suffit alors de corriger, soit d'une erreur dans la définition du masque de sous-réseau qui, porté à 24 bits, distinguerait alors deux sous-réseaux distincts.

Exercice 19.6 Table de routage statique

1) Classe des adresses : pour déterminer la classe d'une adresse IP, il suffit d'examiner la valeur des premiers bits, ou plus simplement regarder la valeur du premier octet. Dans cet exercice, les adresses sont toutes des adresses de classe A (1er octet < 127).

2) Notation des masques : le masque de sous-réseau indique les bits de l'adresse IP à prendre en considération pour assurer l'acheminement (Net_ID et Subnet_ID). Il y a deux modes d'écriture des masques, l'écriture traditionnelle notée comme une adresse IP en notation décimale pointée ou les bits à 1 indique la profondeur d'analyse du champ adresse, et la notation issue du CDIR qui indique directement le nombre de bits à prendre en considération :

– soit la notation CIDR, X.X.X.X/16, c'est la notation utilisée dans l'exercice ;
– soit une écriture plus traditionnelle par une adresse IP ayant les bits de sous-réseau positionnés à 1, exemple X.X.X.X, 255.255.0.0 pour un masque de 16 bits.

3) Adresse de diffusion : l'adresse de diffusion dirigée correspond à l'adresse de toutes les machines d'un réseau désigné. Elle est composée du champ NET_ID éventuellement du Champ Subnet_ID et de l'adresse de diffusion dirigée du réseau 35.8.0.0/16 est 35.8.255.255.

4) Tables de routage

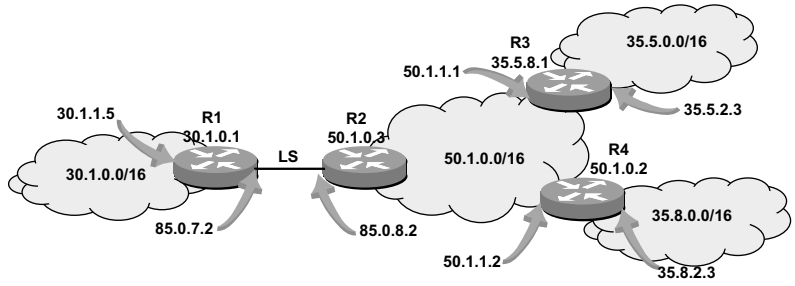


Figure 19.66 Les tables de routage.

Routeur R1 [30.1.0.0/16, locale]

[85.0.0.0/8, locale]
[35.0.0.0/8, 85.0.8.2] (cela évite deux entrées, 35.5 et 35.8)
[50.0.0.0/8. 85.0.8.2] (on aurait pu écrire 50.1.0.0/16, mais c'est moins élégant)
Les deux dernières entrées peuvent être remplacées par celles-ci :
[*,85.0.8.2] ou [0.0.0.0,85.0.8.2]

Routeur R2 [50.1.0.0.16, locale]

[85.0.0.0/8, locale]
[35.8.0.0/16, 50.1.1.2]
[35.5.0.0/16, 50.1.1.1]

© Dunod – La photocopie non autorisée est un délit

[30.1.0.0/16, 85.0.7.2]
[85.0.0.0/8, 85.0.7.2]
Les deux dernières entrées peuvent être remplacées par celles-ci :
[*,85.0.7.2] ou [0.0.0.0,85.0.7.2]

Routeur R3 [35.5.0.0/16, locale]

[50.1.0.0/16, locale]
[35.8.0.0/16, 50.1.1.2]
[30.1.0.0/16,, 50.1.0.3]
[85.0.0.0/8, 50.1.0.3]
Les deux dernières entrées peuvent être remplacées par celles-ci :
[*,85.0.7.2] ou [0.0.0.0,85.0.7.2]

Routeur R4 [35.8.0.0/16,locale]

[50.1.0.0/16, locale]
[35.5.0.0./16, 50.1.1.1]
[30.1.0.0/16, 50.1.0.3]
[85.0.0.0/8, 50.1.0.3]
Les deux dernières entrées peuvent être remplacées par celles-ci :
[*,50.1.0.3] ou [0.0.0.0,50.1.0.3]

Exercice 19.7 Réseau et qualité de service (QoS)

1) Bande passante minimale et maximale théorique

– *Bande passante maximale* : lorsqu'il n'y a pas de données à émettre dans les autres files, chaque flux peut se voir allouer l'intégralité de la bande passante soit les 2 Mbit/s.
– *Bande passante minimale* : quand les deux autres flux ont aussi des données à émettre, chaque flux voit sa bande passante réduite au minimum, ce qui correspond dans notre cas à un partage théorique de la bande passante de :

Flux voix	50 % soit 1 Mbit/s
Flux clients/serveur	30 % soit 600 kbit/s
Flux transfert de fichiers	20 % soit 400 kbit/s

2) Bande passante réelle

a) Bande passante minimale et maximale

– *Bande passante maximale* : comme précédemment la bande passante maximale est allouée à un flux lorsque les deux autres flux n'ont aucune donnée à émettre, soit 2 Mbit/s.
– *Bande passante minimale* : le mécanisme décrit ne tient pas compte de la taille des unités de données. La bande passante minimale réellement allouée dépend du nombre de blocs lus, mais aussi de la taille des blocs, ce qui modifie profondément la répartition des flux telle que l'avait imaginée notre administrateur de réseau. La figure 19.67 indique, pour chaque flux, le volume de données lu et émis à chaque lecture des files d'attente.

	Voix sur IP	Clients/serveur	Transfert de fichiers
Taille du bloc en bits	40 x 8 = 320	256 x 8 = 2 048	1 500 x 8 = 12 000
Volume transmis	320 x 5 = 1 600	2 048 x 3 = 6 144	12 000 x 2 = 24 000
Volume total transmis	1 600 + 6 144 + 24 000 = 31 744		
Ratio bande allouée sur bande totale utilisée	1 600 / 31 744 = 0,05	6 144 / 31 744 = 0,19	24 000 / 31 744 = 0,75
Bande réellement allouée	**100 000 bit/s**	**380 000 bit/s**	**1 500 000 bit/s**

Figure 19.67 Synthèse des résultats.

– *Commentaire* : l'attribution de poids sans tenir compte de la taille des unités de données fausse complètement les résultats, puisque c'est le flux que l'on désirait pénaliser le plus qui obtient le maximum de bande passante.

b) Détermination des poids pour respecter la bande minimale allouée à chaque flux *:* lors de la lecture d'une file, le système envoie au minimum un bloc de données ; les poids doivent donc être déterminés par rapport à la taille de la plus grande unité de données à émettre.

Flux	% BP	Taille	Poids théorique	Volume à émettre	Nb Blocs	Poids réel à affecter
Voix	50	40	5	1 500 x 5 = 7 500	7 500 / 40 = 187,5	187,5/ 207 = 91 %
C/S	30	256	3	1 500 x 3 = 4 500	4 500 / 256 = 17,57	17,57 / 207 = 8 %
Fichiers	20	1 500	2	1 500 x 2 = 3 000	3 000 / 1 500 = 2	2 / 207 = 1 %
Total					207,07	

Figure 19.68 Affectation des poids.

c) Autres possibilités de lecture des files d'attente *:* deux autres méthodes simples peuvent être proposées :

– Déterminer un volume maximum à lire à chaque passe.
– Diviser le temps en intervalles et affecter à chaque file un nombre d'IT en fonction de la bande passante à allouer.

CHAPITRE 20

Exercice 20.1 Capacité d'un autocommutateur

Le trafic total est la somme du trafic résidentiel et du trafic professionnel soit :

$$\text{Trafic Total } (Tt) = \text{Trafic Résidentiel } (Tr) + \text{Trafic professionnel } (Tp)$$

Si x est le nombre d'abonnés on a :

$$Tr = 0{,}1 \times 0{,}4x$$

$$Tp = 0{,}3 \times 0{,}6x$$

© Dunod – La photocopie non autorisée est un délit

Soit :

$$5\,000 = 0{,}1 \times 0{,}4x + 0{,}3 \times 0{,}6x$$

$$x = 5\,000 / 0{,}22 = 22\,727$$

Le nombre d'abonnés reliés à l'autocommutateur est de 22 727.

Exercice 20.2 Itinérance

Les causes de rupture de communication sont nombreuses, citons :

- mobile dans une zone d'ombre ;
- batterie trop faible ;
- vitesse de déplacement du mobile trop importante ;
- mobile en limite de portée d'une cellule et plus de capacité d'accueil dans la cellule qui aurait dû, compte tenu de la position du mobile, le prendre en charge.

Exercice 20.3 Système Iridium

Le système Iridium utilise 66 satellites répartis sur 6 orbites soit 11 satellites par orbite. Le temps de couverture moyen d'un satellite correspond au temps qui sépare le passage de deux satellites successifs. Durée de visibilité d'un satellite :

Période de révolution/nombre de satellites = 100/11 = 9 min.

Remarque : la durée réelle de visibilité est de 11 min.

Exercice 20.4 Schéma de réutilisation des fréquences

Le schéma minimal de réutilisation des fréquences est de trois (figure 20.49). Dans ces conditions chaque cellule peut utiliser 240/3 soit 80 fréquences.

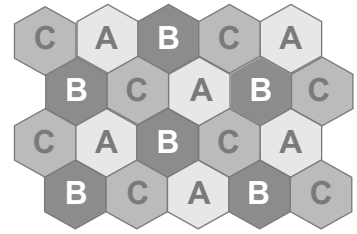


Figure 20.49 Schéma de réutilisation des fréquences (motif de 3).

Exercice 20.5 Protocole D (Q.931)

Analyse du renvoi du poste vers le 01 23 45 67 89

Diagramme des échanges (figure 20.50) : le diagramme des échanges est simple. Le plus intéressant dans cet exercice est le décodage des messages transmis que nous détaillerons complètement. Le décodage de ces messages montre la complexité et la richesse de la signalisation Q.931.

Le poste TEI 64 reçoit le message d'établissement (adresse de diffusion TEI 127) en provenance du réseau. Le poste, renvoyé sur le 01 23 45 67 89, demande l'établissement d'une connexion pour acheminer son message de renvoi (SABME). La connexion étant acceptée par le réseau (UA), le message de renvoi est adressé au réseau (Trame d'INFO).

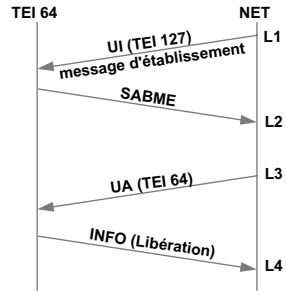


Figure 20.50 Diagramme des échanges sur renvoi d'un poste.

Analyse des éléments d'information

– **Message d'établissement** : le message d'établissement est envoyé par l'usager appelant ou le réseau pour initialiser l'établissement d'un appel. Il comprend toutes les informations nécessaires à l'établissement de la connexion et à l'exécution du service demandé.
L'élément d'information « **Mode de fonctionnement du support** » a pour objet d'indiquer le mode de fonctionnement demandé pour le support, l'ensemble des éléments d'information est transmis de bout en bout.

80H	1-------	Ce bit, dit bit d'extension, est toujours à 1 pour les éléments d'information.
	-00-----	Indique la norme de codage, ici codage CCITT (UIT), les autres valeurs ne sont pas attribuées (réservées pour une utilisation future).
	---00000	Précise le mode de fonctionnement du transfert d'information. Les valeurs suivantes sont utilisées : **00000 Parole (communication téléphonique).** 00100 Informations numériques. 01000 3,1 kHz acoustique.
90H	1-------	Extension Bit
	-00-----	Cette information précise le mode de transfert des informations, seule la valeur 00 est utilisée. Les autres valeurs sont réservées.
	---10000	Indique le débit de transfert des informations, seule la valeur 10000 est utilisée (64 kbit/s).
A3H	1-------	
	-01-----	Identifie la couche et le protocole, 01 (seule valeur utilisée) indique le protocole de la couche 1 d'information usager utilisé, précisé dans les bits suivants.
	---00011	Seule valeur utilisée, elle indique que le codage du signal suit la recommandation G.711 loi A.

© Dunod – La photocopie non autorisée est un délit

L'élément d'information « **Identification du canal** » identifie un canal à l'interface usager/réseau.

81H	1-------	Ce bit, dit bit d'extension, est toujours à 1 pour les éléments d'information.
	-0------	La valeur 0 indique que l'interface est explicitement identifiée. La valeur 0 est réservée.
	--0-----	Précise le type d'interface usager, 0 interface de base, 1 interface débit primaire.
	----0---	Non utilisé, réservé.
	-----0--	Indique si le canal spécifié est préféré ou obligatoire (exclusif). La valeur 0 indique que le canal est seulement préféré, tandis que la valeur 1 indique que seul le canal spécifié est acceptable.
	------0-	Précise si c'est le canal D qui est requis (1). 0 ce n'est pas le canal D. La valeur 1 est réservée.
	------01	Sélection de canal, précise le canal requis : 00 Pas de canal **01 Canal B1** 10 Canal B2 11 N'importe quel canal.

L'élément d'information « **Compatibilité de la couche supérieure** » permet au demandé de vérifier la compatibilité du terminal avec le téléservice demandé.

D1H	1-------	Bit d'extension, toujours à 1.
	-10-----	Précise les normes de codage utilisées. 00 Norme CCITT (UIT) **10 Norme CEPT ou national (précisé par le bit 5)**
	---100--	Interprétation 000 norme nationale **100 CCITT (UIT)/CEPT**
	------01	Présentation, 01 seule valeur attribuée, la méthode utilisée pour préciser le service est la méthode du profil.
81H	1-------	
	-0000001	Indication du téléservice demandé : Norme CCITT (UIT). **0000001 Téléphone** 0000100 Télécopie groupe 3 0100001 Télécopie groupe 4 0100100 Télétex mode mixte 0110001 Télétex mode caractère 0110010 Vidéotex alpha–mosaïque 0110101 Télex 0111000 Système de traitement de message (STM) 1000001 Application ISO

– **Message de libération** : ce message signale que l'équipement a déconnecté le canal et qu'il a libéré les références d'appel. Le récepteur doit procéder de même, et éventuellement interrompre tout appel en cours.

L'élément d'information « **Cause** » est obligatoire, il précise la raison pour laquelle a été émis le message.

87H	1-------	Bit d'extension, toujours à 1.
	-00-----	Indique les normes appliquées, seule valeur 00 (UIT). Les autres valeurs sont réservées.
	---00---	Toujours 00.
	-----111	Localisation, 111 non significatif, à mettre en relation avec la cause de la libération. Toutes les autres valeurs sont réservées.
90H	1------	Bit d'extension, toujours à 1.
	-001----	La cause est codée sur 2 champs. Le premier représente la classe de l'erreur : **001 Situation normale.** 010 Encombrement temporaire du réseau. 011 Service ou option non disponible. 100 Service ou option non mis en œuvre. 101 Message non valide (ex : paramètre, hors gamme) 110 Erreur de protocole (ex : message inconnu). 111 Interfonctionnement.
	----0000	La valeur de l'erreur est précisée ici : **0000 Libération normale**. 0001 Usager occupé. 0010 Pas de réponse de l'usager. 0011 Complément de service non enregistré. 0101 Rejet de l'appel. 0110 Numéro changé. 1000 Numéro non attribué. 1011 Destination hors service. 1100 Adresse incomplète. 1111 Normal non spécifié.

L'élément d'information « **Facilité** » indique les compléments de service demandés. Cet élément est codé sur une longueur comprise entre 4 et 24 octets.

00H	00000000	Longueur de l'identification du réseau, toujours à 0.
2AH	00101010 soit « · »	Préfixe du code service demandé, obligatoire dans le sens usager/réseau. **00101010 · Activation ou enregistrement de service**. 00100011 # Désactivation ou annulation d'un service. · # Fonction d'interrogation de l'enregistrement d'un service.
32H		Demande d'indication d'appel malveillant : « · 32# ».
23H	« # »	Fin du champ complément de service.

L'élément d'information « **Mode de fonctionnement usager** » permet aux terminaux de préciser au réseau leur mode de fonctionnement.

80H	10------	Norme de codage, seule valeur attribuée 10, norme nationale.
	--000000	Description du mode de fonctionnement, seule valeur attribuée 000000, terminal en mode de fonctionnement national.

© Dunod – La photocopie non autorisée est un délit

L'élément d'information « **Numéro appelé** » identifie la destination de l'appel.

80H `1------` Bit d'extension, toujours à 1.

`-000----` Type de numéro appelé :
000 Numérotation en bloc.
101 Envoi par chevauchement.
Les autres valeurs sont réservées.

`----0000` Indique le plan de numérotation utilisé :
0000 plan inconnu.
1001 plan de numérotation privé.
Les autres valeurs sont réservées.

3**0** 3**1** 3**2** 3**3** 3**4** 3**5** 3**6** 3**7** 3**8** 3**9** : codage du numéro appelé en format IA5 (Alphabet international N°5).
Ce qui se lit directement : 01 23 45 67 89.

CHAPITRE 21

Exercice 21.1 Utilisation de l'abaque d'Erlang

Rappelons que l'abaque à refus fournit pour un trafic à écouler de ***E*** erlang par un système de ***M*** ressources, le taux de perte de trafic. Ainsi, la figure 21.73 montre que si on soumet un trafic de 13 E à un système disposant de 18 circuits, le taux de refus est d'environ 5 %.

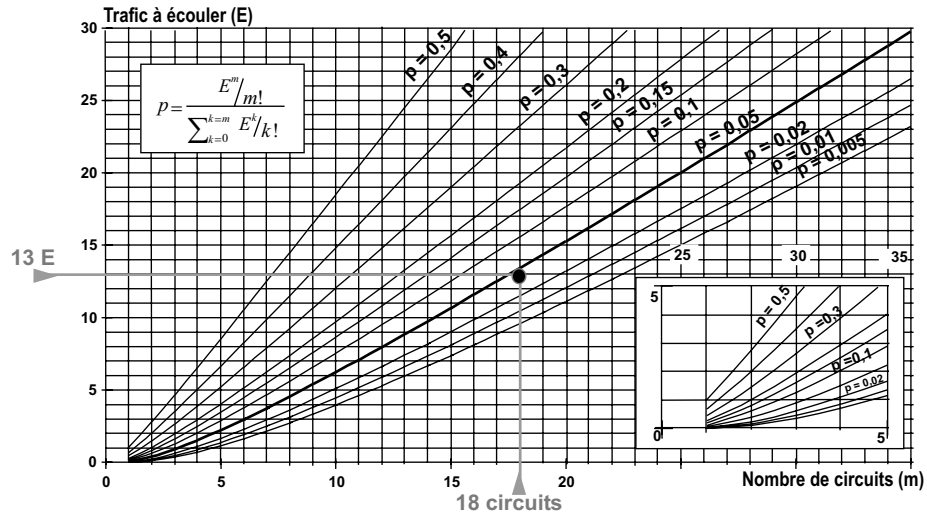


Figure 21.73 L'utilisation de l'abaque d'Erlang.

Sachant que Trafic perdu = Trafic soumis – Trafic écoulé

Probabilité de perte	1 %			10 %			50 %		
Nb circuits	Soumis	Perdu	Écoulé	Soumis	Perdu	Écoulé	Soumis	Perdu	Écoulé
5	1,25	0,02	1,23	3	0,3	2,7	9,5	4,75	4,75
10	4,5	0,05	4,45	7,5	0,75	6,75	18,5	9,25	9,25
15	8	0,08	7,92	12,5	1,25	11,25	28,5	14,25	14,25

Figure 21.74 Les différents trafics sur un faisceau.

Exercice 21.2 Trafic sur un faisceau

Un circuit pouvant écouler 1 E, le rendement d'un circuit est le rapport entre le trafic réellement écoulé par un circuit et le trafic unitaire (1 E). La lecture de l'abaque ci-dessous (figure 21.75) permet de déterminer le trafic soumis.

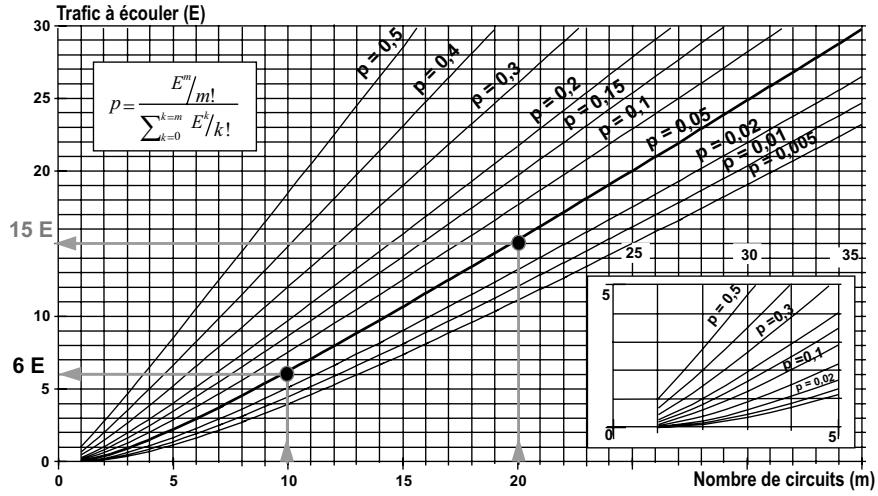


Figure 21.75 Détermination du trafic soumis.

Le trafic réellement écoulé correspond au trafic soumis diminué du trafic perdu, soit dans notre exercice 5 % du trafic soumis. La figure 21.76 fournit les résultats.

Faisceaux	Trafic soumis	Trafic écoulé	η par ligne
1 seul de 10 lignes	6 E	5,7	0,57
2 de 10 lignes	12 E	11,4	0,57
1 seul de 20 lignes	15 E	14,25	0,71

Figure 21.76 Le rendement d'un faisceau.

Conclusion : plus un faisceau est petit, plus les risques de collision d'appel sont importants, donc pour une même probabilité de refus le rendement par circuit plus petit.

© Dunod – La photocopie non autorisée est un délit

Exercice 21.3 Raccordement d'un PABX

1) Capacité de commutation du PABX : le PABX doit assurer l'écoulement de tous les types de trafic pour tous les postes qui y sont raccordés soit :

$$C = \text{Trafic d'un poste} \times \text{Nombre de postes}$$

$$C = 0{,}12\ E \times 120 = 14{,}4 \text{ erlangs}$$

Capacité du PABX : 14,4 erlangs

2) Faisceau SPA, compte tenu d'un taux de refus inférieur à 10 % : en cas d'occupation, les appels sortants sont refusés, c'est l'abaque à refus qu'il convient d'utiliser. Trafic sortant à écouler :

$$T = 0{,}04 \times 100 = 4\ E$$

La lecture de l'abaque d'Erlang à refus (en annexe) indique que sept circuits sont nécessaires.

3) Faisceau SPB, compte tenu d'une mise en attente inférieure à 2 % : en cas d'indisponibilité du correspondant, aucun trafic n'est écoulé pendant que le demandeur occupe un circuit (musique d'attente). Dans ces conditions, c'est l'abaque à attente qu'il convient d'utiliser (en annexe). Trafic à écouler :

$$T = 0{,}004 \times 100 = 4\ E$$

La lecture de l'abaque d'Erlang à attente (en annexe) indique que neuf circuits sont nécessaires.

Exercice 21.4 Trafic d'un centre d'appel

Le traitement d'une communication dure 30 secondes (25+5) soit une capacité de traitement de deux appels/minute. Une ligne (1 erlang) est donc capable de recevoir 120 appels/heure.

Sachant que le trafic à écouler est de 360 000 appels/heure (720 000/2), le nombre de lignes nécessaires est de :

360 000/120 = 3 000 lignes soit aussi 3 000 erlangs.

Cette solution émet l'hypothèse qu'il n'y a pas de collision d'appel. Il s'agit du trafic écoulé et non soumis.

Exercice 21.5 Réseau voix/données

1) Nombre de canaux voix utilisables : au-dessus d'une charge supérieure à 50 %, le temps de transit dans les files d'attente augmente rapidement. Afin de garantir une gigue de paquets minimale, la file d'attente voix ne doit pas être chargée à plus de 50 %. Compte tenu de l'utilisation d'un algorithme de compression à 16 kbit/s, un lien à 64 kbit/s ne pourra supporter plus de deux canaux voix.

2) Bande passante disponible : la bande occupée par un canal voix est égale au produit de la taille de la trame Frame Relay par le nombre de trames/s. La taille de la trame voix est égale à la taille du paquet voix à laquelle il convient d'ajouter les données protocolaires.

– *Taille d'un paquet voix :* les systèmes utilisant la compression ADPCM à 16 kbit/s émettent une trame toutes les 20 ms (50 trames/s), ce qui correspond au transport de :

Débit nominal/fréquence de récurrence = 16 000/ 50 = 320 bit/trame

Taille d'un paquet sans en-tête = 320 / 8 = 40 octets

– *Débit disponible pour les données :* l'encapsulation FRF11 ajoute 2 octets (voir figure 21.46), le protocole Frame Relay ajoute 6 octets (2 fanions, 2 DLCI, 2 FCS), la trame voix est de :

40 + 2 + 6 = 48 octets

Bande nécessaire pour un canal voix (1 trame toutes les 20 ms, soit 50 trames/s) :

$48 \times 8 \times 50 = 19\,200$ bit/s

Pour deux canaux voix : $19\,200 \times 2 = 38\,400$ bit/s
Bande disponible pour les données : $64\,000 - 37\,600 = 25\,600$ bit/s
Remarque : ce résultat ne tient pas compte des bits de transparence.

3) Taille maximale des paquets de données : le débit maximal utilisable étant de 25 600 bit/s, ce débit pouvant être écoulé à raison de 50 trames/seconde, la taille d'une trame est de :

25 600/50 = 512 octets soit 64 octets

Cette valeur correspond à une valeur couramment utilisée dans les systèmes, elle sera retenue comme taille de charge utile. Compte tenu des données d'en-tête, il convient d'ajouter les 8 octets (6 + 2) d'encapsulation soit 72 octets.

La figure 21.77 représente la « trame multiplexée » sur le support WAN.



Figure 21.77 L'entrelacement voix/données.

Notons que le débit maximal soumis au lien peut être de :

$(48 + 48 + 72) \times 8 \times 50 = 67\,200$ kbit/s (lien à 64 kbit/s) !

4) Gigue d'insertion : la gigue est maximale quand un paquet de données est émis juste avant l'arrivée d'un paquet voix. Ce dernier devra attendre la fin d'émission du paquet de données, ce qui correspond au temps d'émission d'un paquet de données :

Volume/Débit = $72 \times 8 / 64\,000 = 9$ ms par lien traversé

Si le bilan temps du réseau montre que cette gigue est trop importante, il conviendra, alors, de réduire la taille des paquets de données ou, plus logiquement, d'augmenter le débit du lien !

© Dunod – La photocopie non autorisée est un délit

Exercice 21.6 Dimensionnement d'un réseau Frame Relay/voix/données

DLCI voix : la compression ADPCM à 16 kbit/s émet une trame toutes les 20 ms (50 trames/s), ce qui correspond au transport de :

– Débit nominal / fréquence de récurrence = 16 000 / 50 = 320 bit/trame
– Taille d'un paquet sans en-tête = 320 / 8 = 40 octets

L'encapsulation FRF11 ajoute 2 octets (voir figure 16.46), le protocole Frame Relay ajoute 6 octets (2 fanions, 2 DLCI, 2 FCS), la trame voix est de :

$$40 + 2 + 6 = 48 \text{ octets}$$

Le débit minimal (CIR) nécessaire à 1 canal voix est de :

$$48 \times 8 \times 50 = 19\,200 \text{ bit/s}$$

Les paquets voix doivent être transportés sans être rejetés, le calcul précédent ne tient pas compte des bits de transparence. Il est malheureusement impossible de déterminer le volume supplémentaire introduit par la transparence. Arbitrairement nous arrondirons le débit requis au kbit supérieur, soit un CIR pour le DLCI voix de :

$$19\,200 \times 2 = 38\,400 \text{ bit/s arrondi à } 40 \text{ kbit/s}$$

Par contre, il n'est nullement besoin de définir un trafic excédentaire (EIR=0). Les caractéristiques du DLCI voix seront :

– CIR = 40 000 bit/s (sur réseau public 48 000 bit/s)
– EIR = 0

DLCI signalisation : la signalisation est fournie par le PABX, quand des informations de signalisation sont émises, elles le sont au débit du lien PABX/VFRAD ; en conséquence seul un CIR est à déterminer. De même pour tenir compte des bits de transparence, on arrondira au kbit supérieur soit :

– CIR = 10 000 bit/s
– EIR = 0

En l'absence d'information de signalisation, toute la bande passante pourra être récupérée par l'EIR du DLCI données.

DLCI Données : la donnée pourra utiliser toute la bande restante soit :

$$128\,000 - 40\,000 - 10\,000 = 78\,000 \text{ bit/s}$$

Les caractéristiques du DLCI données seront fixées à :

– CIR = 78 kbit/s
– EIR = 128 – 78 = 50 kbit/s

Le débit réel de la donnée sera largement supérieur au CIR, le canal données pouvant profiter de la récupération des silences (50 à 60 % de la bande) et de l'absence d'information de signalisation.

Exercice 21.7 Comparaison H.323 et SIP

Critères	H.323	SIP
Normalisation	UIT H.323 v5	IETF RFC 3261
Transport de la signalisation	TCP	TCP/UDP
Transport des flux multimédia	UDP	TCP/UDP
Établissement de canaux logiques	Oui, un par sens	Non
Signalisation *multicast*	Non	Oui
Prioritisation des appels	Non	Oui
Codage des primitives	Binaire Interopérabilité facilitée	Texte Décodage simplifié
Évolutivité	Faible, beaucoup d'extensions propriétaires	Protocole ouvert
Détection des boucles	Non, pas dans la v1	Oui
Gestion des conférences	Centralisée (MCU)	Distribuée

Figure 21.78 Comparaison H.323 et SIP.

CHAPITRE 22

Exercice 22.1 Analyse de la trace SNMP

La figure 22.14 rappelle la structure de la trame Ethernet. Nous n'allons nous intéresser qu'aux champs significatifs.

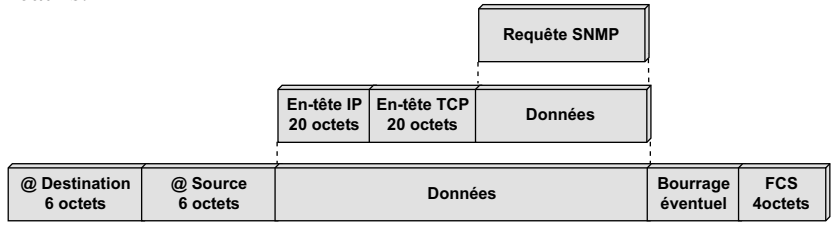


Figure 22.14 La structure de la trame Ethernet.

– **Décodage de l'en-tête MAC**

```
0000: 00 A0 24 BD 75 DB|08 00 02 05 2D FE|08 00
```

Les délimiteurs verticaux marquent les différents champs. Ne retenons que le champ protocole (valeur en gras) qui nous indique bien que le protocole supérieur est IP du DoD (type de protocole 0x08 00).

– **Décodage de l'en-tête TCP/IP**

```
0000:                                           45 00                E.
0010: 00 52 3C EF 00 00 1C 06 A4 FF 80 00 64 00 D0 80  .'<.........d...
0020: 08 29|0A CF 00 A1 47 A8 BA 20 01 A3 96 14 50 18  .)...+G.. ....P.
0030: 20 00 72 D4 00 00
```

L'en-tête IP est en italique, le protocole correspond bien à IP v4 et la longueur d'en-tête est standard (premier octet 45).

Le seul élément intéressant de l'en-tête TCP est le port source (valeur en gras) qui correspond au port 161 (0x 00 A1), c'est-à-dire le port SNMP pour les PDU *GetRequest*, *GetNextRequest* et *GetResponse*.

– Décodage du champ Données

```
0030:                    30 28 02 01 00 04 06 70 75 62   .r...0c.....pub
0040: 6C 69 63 A0 1B 02 04 03 05 52 AE 02 01 00 02 01  lic.............
0050: 00 30 0D 30 0B 06 07 2B 06 01 02 01 01 03 05 00  .0.0...+........
```

Compte tenu de l'apparente complexité des PDU SNMP, due à la succession de structures, nous avons tenté, dans la représentation suivante, de matérialiser cette imbrication (figure 22.15).

```
30 28
  | 02 01 00
  | 04 06 70 75 62 6C 69 63
  | A0 1B
  |   | 02 04 03 05 52 AE
  |   | 02 01 00
  |   | 02 01 00
  |   | 30 0D
  |   |   | 30 0B
  |   |   |   | 06 07 2B 06 01 02 01 01 03
  |   |   |   | 05 00
```

Champ	Commentaire
30 28	Le premier octet indique le type 0x30 soit 0011 0000B, il s'agit d'un type de la famille *universal*, (les deux premiers bits à 0) construit (troisième bit à 1) et type séquence (1 000). La longueur de la séquence étant de 0x28 soit 40D.
02 01 00	Le type suivant est un entier (0x02) de longueur 1. L'octet suivant indique la version de SNMP, la valeur 0 identifie SNPM v1.
04 06 70 75 62 6C 69 63	Le champ suivant est de type *string* (0x04) de longueur 6. Il s'agit du champ *Commity*, correspondant au mot de passe : *public*. Les champs suivants contiennent les données de la PDU.
A0 1B	Le premier champ indique le type et la longueur totale. Le type 0xA0 ou 1010 000B indique qu'il s'agit d'un type dépendant du contexte (10) construit (bit 3 à 1), la valeur 0 des autres éléments binaires identifie la PDU *GetRequest,* la longueur totale de cette dernière étant de 27 octets (0x1B).
02 04 03 05 52 AE	Ce champ contient le numéro d'identification de la demande. Le type est entier (0x02) de longueur 4 et le contenu 0x03, 0x05, 0x52, 0xAE. La réponse à cette demande contiendra le même identifiant.
02 01 00	Le champ *Error_Status* est à 0 (ce champ est toujours à 0 dans une PDU de type *Get*. Type entier 0x02, de longueur 1 (0x01) et de valeur 0 (0x00).
02 01 00	Ce champ est de structure identique au précédent, il s'agit du champ *Error_Index*, toujours à 0 dans une PDU *Get*.
30 0D	La valeur 0x30 annonce une nouvelle séquence (*universal*, construit) de longueur 0x0D soit 13.
30 0B	Le premier champ de cette séquence est lui-même une séquence de longueur 0x0B soit 12.
06 07 2B 06 01 02 01 01 03	Le type de cette séquence est 0x06, c'est un type *universal*, il s'agit du type ID (OID) identifiant l'objet interrogé par la PDU. La longueur de l'OID est de 7. La valeur 0x2B (43D) représente les deux premiers entiers de l'OID selon un codage particulier (A $\times$ 40 + B) soit 1 $\times$ 40 + 3, l'objet est donc identifié dans l'arbre de nommage par le chemin : 1.3.6.1.2.1.1.3, il s'agit de l'OID de *SysUpTime*.
05 00	La valeur 0x05 indique le type NIL (NULL). Ce champ indique la fin de la description et des valeurs relatives à l'objet précédemment identifié. Ici, puisqu'il s'agit du PDU de type *Get*, les champs Valeurs sont absents.

Figure 22.15 La structure de la PDU SNMP.

Exercice 22.2 SNMP et charge du réseau

Le nombre de sollicitations est de 100 toutes les 10 secondes, ce qui correspond à 10 sollicitations par seconde. Dans ces conditions, le volume à transférer est de :

$$(100 \times 8) \times 10 = 8\,000 \text{ bit/s}$$

Ce qui correspond pour une ligne à 64 kbit/s à 12,5 % de ses capacités de transfert. Le protocole SNMP est un protocole « bavard ». L'administration de sites locaux à distance est limitée. Il convient de sélectionner avec la plus grande attention les objets gérés et d'augmenter au maximum la période de *polling*.

CHAPITRE 23

Exercice 23.1 MTTR/MTBF

Calcul de la disponibilité

Étape 1 : pour calculer la disponibilité et l'indisponibilité de l'ensemble, il faut déterminer la disponibilité et l'indisponibilité de chacun de ses composants.

	MTBF	MTTR	Disponibilité (*A*)	Indisponibilité (*I*)
Système 1 & 2	4 mois	8 heures	(4 x 200) / (4 x 200 + 8) = 0,99	1– 0,99 = 0,01
Modem	2 ans	5 heures	(2 400 x 2) / (2 400 x 2 + 5) = 0,9989	1– 0,9989 = 0,0011
RTC	2 ans	24 heures	(2 400 x 2) / (2 400 x 2 + 24) = 0,9950	1– 0,9950 = 0,005
Telcos	2 ans	2 heures	(2 400 x 2) / (2 400 x 2 + 2) = 0,9995	1 – 0,9995 =0,0005

Figure 23.43 La disponibilité et l'indisponibilité.

Étape 2 : établissement du diagramme de fiabilité du système.

À chaque élément du système, on substitue une représentation quantifiée de sa disponibilité et de son indisponibilité. En remplaçant la représentation fonctionnelle par une représentation basée sur les structures élémentaires, on obtient un diagramme qu'il suffit de simplifier, en y appliquant les règles de regroupement des structures élémentaires, pour déterminer la disponibilité et l'indisponibilité globales du système étudié.

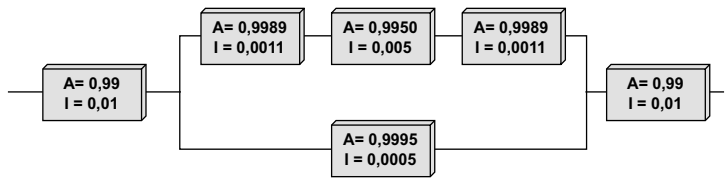


Figure 23.44 Le diagramme de fiabilité.

© Dunod – La photocopie non autorisée est un délit

Étape 3 : on formalise par branche.

– Branche 1 : Modem-RTC-Modem,

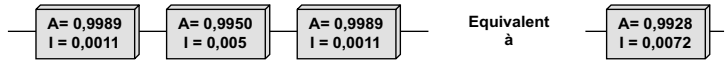


Figure 23.45 L'étude de la branche Modem-RTC-Modem.

– $A_t = A_1 \times A_2 \times \ldots \times A_n = 0{,}9989 \times 0{,}9950 \times 0{,}9989 = 0{,}9928$
– $I_t = 1 - A_n = 0{,}0072$
– Où $I_t = \Sigma\, I = 0{,}0072$

– Branche 2 : Branche 1 en parallèle avec le réseau de l'opérateur,

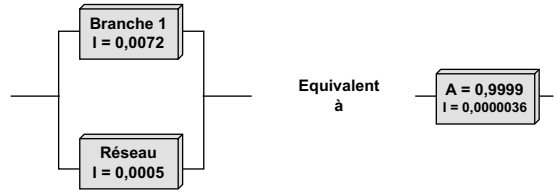


Figure 23.46 La branche 1 et réseau de l'opérateur.

– $I_t = I_1 \cdot I_2 \ldots I_n = 0{,}0072 \times 0{,}0005 = 0{,}0000036$
– $A_t = 1 - I_n = 0{,}9999$

– Branche 3 : Système 1 - Branche 2 - Système 1 (structure finale),

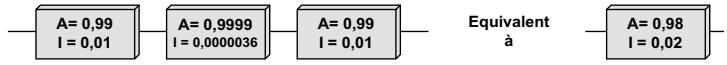


Figure 23.47 La structure finale.

– $A_t = A_1 \times A_2 \ldots A_n = 0{,}99 \times 0{,}9999 \times 0{,}99 = 0{,}98$
– $I_t = 1 - A_n = 0{,}02$
– $I_t = \Sigma\, I = 0{,}0072$

Interprétation des résultats : la disponibilité du système est de 98 %, c'est-à-dire qu'il y aura 98 heures de bon fonctionnement et 2 heures de panne en moyenne pour 100 heures de mise à disposition des équipements, mais cette valeur globale n'indique nullement l'espérance de bon fonctionnement entre deux pannes. Pour cela, il nous faut déterminer la MTBF et la MTTR résultante.

Calcul de la MTBF/MTTR : le calcul est équivalent, reprenons à partir de l'étape 3.

Étape 3 : on formalise par branche,

– Branche 1 : Modem-RTC-Modem

– MTBF =1 / $\Sigma_{i=1 \text{ à } n}$ (1/MTBF$_i$)

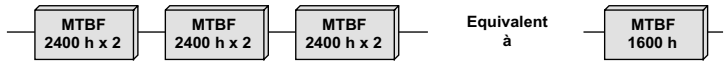


Figure 23.48 La branche Modem-RTC-Modem.

- MTBF = 1/ (1/4 800 + 1/4 800 + 1/ 4 800) = 4 800 / 3 = 1 600 h
- *I*/*A* = MTTR/MTBF soit MTTR = (*I*/*A*) × MTBF
- MTTR = (0,0072 × 1 600) / 0,9928 = 11,60 h

– Branche 2 : Branche 1 en parallèle avec le réseau opérateur,

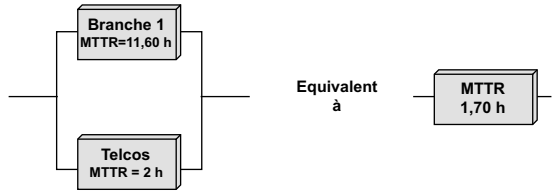


Figure 23.49 La branche 1 et réseau de l'opérateur.

- MTTR =1 / $\Sigma_{i=1 \text{ à } n}$ (1/MTTR$_i$)
- MTTR = 1 / (1/11,60 + 1/2) = 1,70 h
- *I*/*A* = MTTR / MTBF soit MTBF = (*A*/*I*) × MTTR
- MTBF = (0,9999 × 1,70) / 0,0000036 = 472 175 h

– Branche 3 : Système 1- Branche 2 - Système 1 (structure finale),

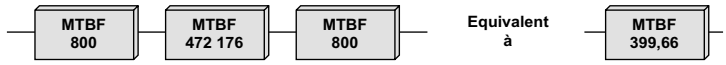


Figure 23.50 La structure finale.

- MTBF = 1 / $\Sigma_{i=1 \text{ à } n}$ (1/MTBF$_i$)
- MTBF = 1/ (1/800 + 1/472 175 + 1/800) = 399,66 h
- *I*/*A* = MTTR/MTBF soit MTTR = (*I*/*A*) × MTBF
- MTTR = (0,02 × 399,66) / 0,98 = 8,15 h

Ce qui correspond à une immobilisation d'une journée environ tous les deux mois. Vérification :

$$A = MTBF / (MTBF + MTTR) = 399 / (399 + 8,15) = 0,98$$

Exercice 23.2 Systèmes à clés symétriques ou secrètes

Dans un système à clés secrètes comportant *N* utilisateurs, chaque utilisateur doit connaître sa clé et celle de ses *N* – 1 correspondants potentiels. Ce qui correspond pour un utilisateur à *N* clés soit pour le système N^2 clés à gérer.

© Dunod – La photocopie non autorisée est un délit

Dans un système à clé publique, chaque utilisateur n'a à connaître que la clé publique de ses $N - 1$ correspondants potentiels et sa propre clé secrète soit N clés.

Exercice 23.3 Algorithme à translation de César

Plusieurs approches sont envisageables pour déchiffrer un crypte. En supposant connu l'algorithme de chiffrement utilisé, on peut essayer toutes les clés possibles. Cette méthode est évidemment peu efficace. On peut, connaissant l'origine du texte, tenter de retrouver un mot spécifique au contexte... La méthode la plus simple vis-à-vis de l'algorithme de César est de repérer la lettre dont l'apparition est la plus importante et de supposer successivement que cette lettre est le crypte de la lettre E, A, I, O, S... dans l'ordre de la fréquence d'apparition des lettres dans la langue considérée. En appliquant cette méthode au crypte « HTIFLJIJHJXFW », la lettre J ayant la plus grande apparition sera d'abord supposée correspondre au clair E, soit une translation de 5. Ce qui correspond à la grille suivante (figure 23.51).

Clair	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Crypte	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

Figure 23.51 La table de translation.

Soit le texte clair : « Codage de César ».

Mais la translation peut être plus complexe, par exemple prenons le chiffre :

« DA NATTUHA ATV DJEGGSA »

De même, supposons que ce soit la lettre E, la plus utilisée. Dans notre cas on établit la correspondance E → A soit une translation négative de 4. Prenons maintenant le mot ATV et appliquons la règle établie ATV devient EXZ, ce qui ne correspond à aucun mot de la langue française ! Cependant en regardant le premier mot « DA », le A correspondant à E, la première lettre ne peut alors qu'être une consonne, en appliquant une translation de 4 on obtient la lettre H, cela est donc plausible, mais ne correspond pas pour le mot ATV. Seul point que l'on peut considérer, une voyelle a été remplacée par une voyelle et une consonne par une consonne.

En partant de ce constat, on sait que la consonne la plus utilisée est le S. Dans notre exemple, le S serait donc remplacé par un T. Si on applique cela au mot ATV, on trouve ES?. La translation de S → T est une translation positive de 1, appliquons-là, le mot ES? devient alors ESW, ce qui est encore impossible. Supposons alors que cette translation de 1 n'est pas une translation de position mais de signification. La règle serait alors une consonne est remplacée par la consonne qui la suit. Le mot ATV devient alors EST, appliquée au mot DA, cette règle donne DA devient CE, ce qui est totalement acceptable.

Si on revient alors à la règle établie pour le codage d'un E, par assimilation on pourrait imaginer qu'une voyelle est remplacée par la voyelle qui la précède et une consonne par la consonne qui la suit. En appliquant cette règle on obtient le clair :

« CE MESSAGE EST CHIFFRE »

La translation de César est simple et peut donner naissance à divers types de codage, tous cependant facilement « cassables », avec de la patience !

Exercice 23.4 Algorithme de substitution de Vigenère

Méthode :

– Recopier autant de fois que nécessaire la clé. Afin d'obtenir un texte de longueur identique à celle du crypte (figure 23.52).

– Déterminer la lettre du clair en pratiquant comme suit :

  – à partir de la lettre de la clé, on recherche dans la colonne la lettre du crypte. En lisant horizontalement, on obtient la lettre du clair (figure 23.52).

  – lire et réintroduire les blancs.

Clé	S	E	C	R	E	T	S	E	C	R	E	T	S	E	C	R	E
Crypte	L	E	D	C	I	T	M	H	G	M	M	Z	W	R	G	I	I
	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Clair	T	A	B	L	E	A	U	D	E	V	I	G	E	N	E	R	E

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	↓ 19	20	21	22	23	24	25	26
	1	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	**S**	T	U	V	W	X	Y	Z
	2	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V	W	X	Y	Z	A
	3	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	4	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	5	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	6	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	7	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	B	E	F
	8	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	Y	Z	A	B	C	D	E	F	G
	9	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	10	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	11	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	12	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	13	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	14	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	15	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	16	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	17	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	18	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K
	19	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R
←	20	**T**	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	**L**	M	N	O	P	Q	R	S
	21	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	22	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	23	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	K	R	S	T	U	V
	24	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	25	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	26	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 23.52 La mise en correspondance de la clé, du crypte et du clair.

Le clair est donc « Tableau de Vigenère ».

© Dunod – La photocopie non autorisée est un délit

Exercice 23.5 Systèmes à clés asymétriques

Rappels de l'algorithme du RSA : le système de cryptographie à clé asymétrique le plus répandu, le RSA, repose sur l'arithmétique des grands nombres.

– La fonction de chiffrement est de la forme :

$$\text{Crypte} = \text{Clair}^{\text{clé C}} \text{ modulo n}$$

où Crypte est le message codé,
Clair, le message à coder,
clé C, la clé de chiffrement,
n, un produit de nombres premiers.

– La fonction de déchiffrement est identique :

$$\text{Clair} = \text{Crypte}^{\text{clé D}} \text{ modulo } n$$

où Crypte est le message codé,
Clair, le message à coder,
clé D, la clé de chiffrement,
n, un produit de nombres premiers.

– L'algorithme de détermination des clés est rappelé ci-dessous :

- Choisir deux nombres premiers p et q grands et différents ($> 10^{100}$).
- Calculer n tel que $n = p \times q$.
- Choisir les clés telles que $C \times D = 1 + M\,[(p-1) \times (q-1)]$, où M est un entier qui satisfasse l'égalité.
- Définir la longueur maximale (L) du bloc de bits sur lequel on applique l'opération de sorte que $2^L < n$.

1) Recherche des plus petites clés possibles : les nombres p, q devant être plus grands que 1, le premier couple de nombres premiers est : 2, 3. Dans ces conditions :

$$n = p \times q = 2 \times 3 = 6$$
$$z = (p-1)\,(q-1) = 2$$
$$C \times D = 1 + M \times 2$$

Soit pour les valeurs de M :

M	1 + *M* × 2	C	D	Commentaires
1	3	1	3	Une clé de 1 est absurde
2	5			5, nombre premier
2	7			7, nombre premier
4	9	3	3	Les clés sont symétriques
5	11			11, nombre premier
6	13			13, nombre premier
7	15	3	5	Valeurs acceptables

Figure 23.53 Recherche du plus petit couple de clés (p = 2, q = 3).

La longueur du crypte élémentaire est :

$$2^L < n \quad \text{soit} \quad 2^2 < 6.$$

Dans ces conditions, les différentes valeurs élémentaires (2 bits) sont 0, 1, 2, 3

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n
0	0	0		
1	1	1		
2	8	2		
3	27	3		

Figure 23.54 La table de chiffrement (C = 3, D = 7).

Ces valeurs sont trop petites, le crypte est identique au clair. Il faut choisir un autre couple. Le plus petit couple (p, q) suivant est : 2, 5

$$n = p \times q = 2 \times 5 = 10$$
$$z = (p-1)(q-1) = 4$$
$$\mathrm{C} \times \mathrm{D} = 1 + M \times 4$$

Soit les valeurs de M :

M	$1 + M \times 2$	C	D	Commentaires
1	5			5, nombre premier
2	9	3	3	Les clés sont symétriques
3	13			13, nombre premier
4	17			17, nombre premier
5	21	3	7	Valeurs acceptables

Figure 23.55 Recherche des clés suivantes (p = 2 , q = 5).

La longueur du crypte élémentaire est :

$$2^L < n \quad \text{soit} \quad 2^3 < 6$$

© Dunod – La photocopie non autorisée est un délit

Dans ces conditions, les différentes valeurs élémentaires (3 bits) sont :

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	7	823 543	3
4	64	4	16 384	4
5	125	5	78 125	5
6	216	6	279 936	6
7	343	3	2 187	7

Figure 23.56 La table de chiffrement (C = 3, D = 7).

Indépendamment du fait que nombre de cryptes sont encore égaux au clair, on a pu vérifier qu'il était bien possible de coder avec une clé et de décoder avec une autre.

2) Rejet de la solution établie : le couple de clés calculé est inacceptable pour crypter un fichier. En effet, la valeur 2 est cryptée 8, c'est-à-dire codée sur 4 bits. Le déchiffrement étant réalisé par bloc de 3 bits, un décalage se produira, le message décrypté sera illisible.

En conséquence il faut, d'une part, imposer que le plus grand nombre à coder ($n - 1$, puisque l'opération est modulo n) ait pour longueur binaire L. C'est-à-dire, L doit être tel que :

$$2^L + 1 = n$$

Et, d'autre part que L doit être différent de 8, car le codage d'un même octet donnerait toujours la même valeur.

3) Détermination des plus petites clés possibles et utilisables

a) Le couple p, q doit répondre à la condition : $2^L + 1 = n = p \times q$ soit :

2L + 1	p × q	Commentaires
21 + 1 = 3	1 × 3	z = 0, solution impossible
22 + 1 = 5	1 × 5	z = 0, solution impossible
23 + 1 = 9	3 × 3	Nombres identiques
24 + 1 = 17	Nombre premier	
25 + 1 = 33	3 × 11	Solution acceptable

Figure 23.57 Recherche du couple p, q.

b) Détermination des clés

$$n = p \times q = 3 \times 11 = 33$$
$$z = (p - 1) \times (q - 1) = 2 \times 10 = 20$$
$$\mathrm{C} \times \mathrm{D} = 1 + M \times 20$$

Les plus petites valeurs possibles sont pour $M = 1$: $C = 3$, $D = 7$

Les paramètres du logiciel de cryptographie seront donc :

$$C = 3, D = 7, L = 5, n = 33$$

c) Matrice de chiffrement

Clair	N = Clair ^{C}	Crypte = N mod n	N = Crypte ^{D}	Clair = N mod n
0	0	0	0	0
1	1	1	1	1
2	8	8	2 097 152	2
3	27	27	10 460 353 203	3
4	64	31	27 512 614 111	4
5	125	26	8 031 810 176	5
6	216	18	6 122 20 032	6
7	343	13	62 748 517	7
8	512	17	4 103 38 673	8
9	729	3	2 187	9
10	1 000	10	10 000 000	10
11	1 331	11	194 87 171	11
12	1 728	12	35 831 808	12
13	2 197	19	893 871 739	13
14	2 744	5	78 125	14
15	3 375	9	4 782 969	15
16	4 096	4	16 384	16
17	4 913	29	17 249 876 309	17
18	5 832	24	4 586 471 424	18
19	6 859	28	13 492 928 512	19
20	8 000	14	105 413 504	20
21	9 261	21	180 108 8541	21
22	10 648	22	2 494 357 888	22
23	12 167	23	3 404 825 447	23
24	13 824	30	21 870 000 000	24
25	15 625	16	268 435 456	25
26	17 576	20	1 280 000 000	26
27	19 683	15	170 859 375	27
28	21 952	7	823 543	28
29	24 389	2	128	29
30	27 000	6	279 936	30
31	297 918	25	6 103 515 625	31

Figure 23.58 La table de codage (C = 3, D = 7).

© Dunod – La photocopie non autorisée est un délit

4) Crypte du mot « MODEM »

Clair	M	O	D	E	M
Hex (8 bits)	4D	4F	44	45	4D
Binaire 8 bits	01001 101	01 00111 1	0100 0100	0 10001 01	010 01101
Blocs de 5 bits	01001	101 01	00111	1 0100	0100 0	10001	01 010	01101
Clair Décimal	9	21	7	20	8	17	10	13
Crypte Décimal	3	21	23	14	17	27	10	19
Blocs de 5 bits	00011	10101	10111	01110	10001	11011	01010	10011
Binaire 8 bits	00011 101	01 10111 0	11110 1000	1 11011 01	010 10011
Décimal	29	110	232	237	83
Hex (8 bits)	1D	6E	E8	ED	53

Figure 23.59 Le chiffrement du mot « MODEM ».

Soit le clair : 0x4D, 0x4F, 0x44, 0x45, 0x4D

Et le cryptogramme : 0x1D, 0x6E, 0xE8, 0xED, 0x53

Exercice 23.6 Système de Diffie-Hellman

Compte tenu des données communes (G = 3, N = 32) et des tirages d'Alice (A = 5) et de Bob (B = 7). La figure 23.60 illustre la méthode de calcul.

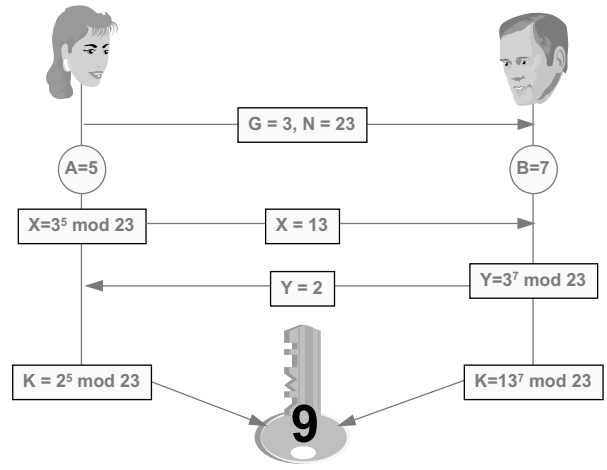


Figure 23.60 Le calcul de la clé de session.

CHAPITRE 24

Exercice 24.1 Service de vidéotex

La résolution d'un tel problème est simple, il faut d'abord déterminer le trafic à écouler, puis à l'aide de l'abaque d'Erlang définir le nombre de lignes utiles.

1) Nombre de circuits virtuels

a) Trafic à écouler

$$E = NT \,/\, 3\,600 = 600 \times 2 \times 60 \,/\, 3\,600 = 20 \text{ E}$$

b) Nombre de lignes pour une qualité de service meilleure que 1 %. La lecture de l'abaque (figure 24.20, repère 1) donne directement 30 circuits

2) Nombre de demandes satisfaites : nombre de demandes de connexion pour un taux de refus de 2 %. La lecture de l'abaque (figure 24.20, repère 2) indique que pour 30 circuits et un taux de refus de 2 % un trafic écoulé est de 22 E soit un nombre de demande de connexions de :

$$E = NT/3\,600 \text{ soit } N = 3\,600\,E/T = 3\,600 \times 22 \,/\, 2 \times 60 = 660 \text{ connexions}$$

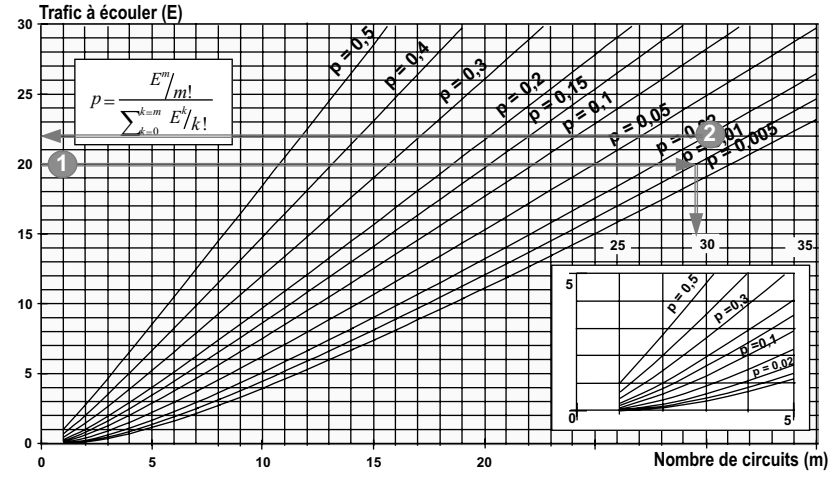


Figure 24.20 L'abaque d'Erlang à refus.

Exercice 24.2 Informatisation d'un magasin

1) Détermination du nombre de terminaux de caisse : en partant du temps d'attente (t_a) devant les caisses (10 minutes), on déterminera la charge maximale supportable (ρ). De cette charge, compte tenu du temps d'encaissement (temps de service ou t_s) on définira le nombre de clients traités par un terminal de caisse.

$$\text{de } t_a = \frac{\rho}{1-\rho}\, t_s \qquad \text{on déduit} \qquad \rho = \frac{t_a}{t_a + t_s} = \frac{10}{10+3} = 0{,}76$$

© Dunod – La photocopie non autorisée est un délit

Une charge maximale de 0,76 correspond à un taux d'arrivée devant le terminal de :

$$\text{de } \rho = \lambda\, t_s \text{ on déduit } \lambda = \frac{\rho}{t_s} = \frac{0{,}76 \times 60}{3} = 15 \text{ clients/heure}$$

Le nombre de clients dans la file sera :

$$N = \lambda t_a = \frac{15 \times 10}{60} = 3 \text{ clients}$$

Ce qui répond au cahier des charges ; dans ces conditions, il est nécessaire de disposer de quatre terminaux de caisse pour écouler les 60 clients/heure.

2) Nombre de terminaux au point d'enlèvement : les terminaux « point d'enlèvement » doivent être accessibles dans 80 % des cas, c'est-à-dire qu'un magasinier ne doit pas se voir refuser l'accès au terminal dans plus de 20 % des cas. Le nombre de terminaux se définit alors à partir des courbes d'Erlang (abaque à refus). Sachant qu'une consultation mobilise le terminal pendant une minute et que 60 clients se présentent dans l'heure :

$$\text{Le trafic à écouler est de } E = \frac{Nt}{60} = \frac{60 \times 1}{60} = 1 \text{ E}$$

La lecture de l'abaque indique deux terminaux.

3) Nombre de terminaux de point de vente : le raisonnement est identique. Compte tenu qu'il y a 100 consultations de 1 minute et 60 prises de commande de 3 minutes, le trafic à écouler est de :

$$E = \frac{NT}{60} = \frac{100 \times 1 + 60 \times 3}{60} = 4{,}66\, E$$

La lecture de l'abaque, pour un taux de refus de 5 %, donne 8 terminaux.

Le nombre de terminaux à installer est donc de :

Terminaux	Vente	Caisse	Enlèvement	Comptable
Nombre	8	4	2	2

Figure 24.21 Nombre de terminaux.

4) Temps de réponse : le temps de réponse exprime le temps d'attente de l'opérateur entre le moment où il valide une requête et celui où la réponse est affichée. La figure 24.22 matérialise les composantes de ce temps.

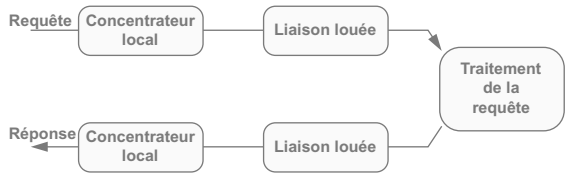


Figure 24.22 Définition du temps de réponse.

Le temps de transport des données sera déterminé à partir de la transaction moyenne. Rappelons qu'il a 100 transactions/heure point de vente, 60 transactions/heure caisse et enlèvement et 40 transactions/jour (soit 5 transactions/heure) pour les terminaux de comptabilité.

La transaction moyenne doit être définie dans le sens Host/Succursale (L_{HS}) et dans le sens Succursale/Host (L_{SH}), la longueur moyenne sera multipliée par 1,2 pour tenir compte des données de service :

$$L_{HS} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \times 800 + 60 \times 600 + 60 \times 500 + 5 \times 800}{100 + 60 + 60 + 5} \times 1{,}2 = 800 \text{ octets}$$

$$L_{SH} = \frac{\Sigma \lambda L}{\Sigma L} = \frac{100 \times 20 + 60 \times 100 + 60 \times 20 + 5 \times 200}{100 + 60 + 60 + 5} \times 1{,}2 = 54{,}4 \text{ octets}$$

Nombre de transactions ou taux d'arrivée :

$$\lambda = \sum \lambda = 100 + 60 + 60 + 5 = 225 \text{ transactions/heure}$$
$$\text{soit } 0{,}0625 \text{ transaction/seconde}$$

Temps de réponse du concentrateur local (t_{rc}), considéré comme le temps de transfert des données du concentrateur aux terminaux (requête et réponse) :

$$t_{rc} = \frac{L_{HS}}{Dc - \lambda L_{HS}} + \frac{L_{SH}}{Dc - \lambda L_{SH}}$$
$$= \frac{800 \times 8}{9600 - 0{,}0625 \times 800 \times 8} + \frac{54{,}4 \times 8}{9600 - 0{,}0625 \times 54{,}4 \times 8} = 0{,}74 \text{ s}$$

Temps de réponse de la liaison louée (t_{rt}) :

$$t_{rt} = \frac{L_{HS}}{Dt - \lambda L_{HS}} + \frac{L_{SH}}{D_t - \lambda L_{SH}}$$
$$= \frac{800 \times 8}{64000 - 0{,}0625 \times 800 \times 8} + \frac{54{,}4 \times 8}{64000 - 0{,}0625 \times 54{,}4 \times 8} = 0{,}10 \text{ s}$$

Temps de réponse de la transaction :

$$Tr = t_{rc} + t_{rl} + \text{temps de traitement de la requête}$$

$$Tr = 0{,}74 + 0{,}1 + 0{,}2 = 1{,}04 \text{ s}$$

Remarque : rappelons que lorsque le système est peu chargé, ce qui est fréquemment le cas dans les systèmes conversationnels, on peut admettre plus simplement :

$$Tr = \frac{L}{D}$$

© Dunod – La photocopie non autorisée est un délit

Exercice 24.3 Réalisation d'un réseau privé d'entreprise

1) Graphe du réseau sans contrainte

a) Matrice des coûts (Kruskal) : la première étape consiste à établir la matrice des coûts, les liens ayant tous un débit identique, cette matrice ne tiendra compte que des distances inter-sites (figure 24.23).

	Amiens	Lille	Metz	Nancy	Strasbourg	Rennes	Nantes	La Rochelle	Bordeaux	Toulouse	Clermont	Dijon	Lyon	Marseille	Nice
Paris	115	203	283	282	400	310	344	400	500	590	348	264	393	662	687
Amiens		98	296	313	424	353	412	489	603	703	462	351	497	771	786
Lille			283	313	410	444	508	587	699	792	540	396	557	835	834
Metz				47	130	591	613	642	700	713	438	217	386	650	607
Nancy					118	586	600	620	670	674	400	175	341	603	561
Strasbourg						702	713	725	761	738	472	247	384	617	544
Rennes							100	221	373	557	446	512	561	767	849
Nantes								122	275	466	391	499	517	697	792
La Rochelle									154	352	332	491	467	607	718
Bordeaux										213	306	514	437	507	639
Toulouse											275	500	361	320	470
Clermont												228	137	331	404
Dijon													174	449	439
Lyon														278	300
Marseille															160

Figure 24.23 Matrice des coûts.

b) Liste ordonnée des liens

Ordre	Lien	Distance	Ordre	Lien	Distance
1	Metz Nancy	47	61	Amiens Clermont	462
2	Amiens Lille	98	62	Nantes Toulouse	466
3	Rennes Nantes	100	63	La Rochelle Lyon	467
4	Paris Amiens	115	64	Toulouse Nice	470
5	Nancy Strasbourg	118	64	Strasbourg Clermont	472
6	Nantes La Rochelle	122	66	Amiens La Rochelle	489
7	Metz Strasbourg	130	67	La Rochelle Dijon	491
8	Clermont Lyon	137	68	Amiens Lyon	497
9	La Rochelle Bordeaux	154	69	Nantes Dijon	499
10	Marseille Nice	160	70	Paris Bordeaux	500
11	Dijon Lyon	174	71	Toulouse Dijon	500
12	Nancy Dijon	175	72	Bordeaux Marseille	507
13	Paris Lille	203	73	Lille Nantes	508

Figure 24.24 Liste ordonnée des coûts.

Ordre	Lien	Distance	Ordre	Lien	Distance
14	Bordeaux Toulouse	213	74	Rennes Dijon	512
15	Metz Dijon	217	75	Bordeaux Dijon	514
16	Rennes La Rochelle	221	76	Nantes Lyon	517
17	Clermont Dijon	228	77	Lille Clermont	540
18	Strasbourg Dijon	247	78	Strasbourg Nice	544
19	Paris Dijon	264	79	Lille Lyon	557
20	Nantes Bordeaux	275	80	Rennes Toulouse	557
21	Toulouse Clermont	275	81	Nancy Nice	561
22	Lyon Marseille	278	82	Rennes Lyon	561
23	Paris Nancy	282	83	Nancy Rennes	586
24	Paris Metz	283	84	Lille La Rochelle	587
25	Lille Metz	283	85	Paris Toulouse	590
26	Amiens Metz	296	86	Metz Rennes	591
27	Lyon Nice	300	87	Nancy Nantes	600
28	Bordeaux Clermont	306	88	Amiens Bordeaux	603
29	Paris Rennes	310	89	Nancy Marseille	603
30	Amiens Nancy	313	90	Metz Nice	607
31	Lille Nancy	313	91	La Rochelle Marseille	607
32	Toulouse Marseille	320	92	Metz Nantes	613
33	Clermont Marseille	331	93	Strasbourg Marseille	617
34	La Rochelle Clermont	332	94	Nancy La Rochelle	620
35	Nancy Lyon	341	95	Bordeaux Nice	639
36	Paris Nantes	344	96	Metz La Rochelle	642
37	Paris Clermont	348	97	Metz Marseille	650
38	Amiens Dijon	351	98	Paris Marseille	662
39	La Rochelle Toulouse	352	99	Nancy Bordeaux	670
40	Amiens Rennes	353	100	Nancy Toulouse	674
41	Toulouse Lyon	361	101	Paris Nice	687
42	Rennes Bordeaux	373	102	Nantes Marseille	697
43	Strasbourg Lyon	384	103	Lille Bordeaux	699
44	Metz Lyon	386	104	Metz Bordeaux	700
45	Nantes Clermont	391	105	Strasbourg Rennes	702
46	Paris Lyon	393	106	Amiens Toulouse	703
47	Lille Dijon	396	107	Metz Toulouse	713
48	Paris Strasbourg	400	108	Strasbourg Nantes	713
49	Paris La Rochelle	400	109	La Rochelle Nice	718
50	Nancy Clermont	400	110	Strasbourg La Rochelle	725
51	Clermont Nice	404	111	Strasbourg Toulouse	738
52	Lille Strasbourg	410	112	Strasbourg Bordeaux	761
53	Amiens Nantes	412	113	Rennes Marseille	767

Figure 24.24 Liste ordonnée des coûts. (suite)

Ordre	Lien	Distance	Ordre	Lien	Distance
54	Amiens Strasbourg	424	114	Amiens Marseille	771
55	Bordeaux Lyon	437	115	Amiens Nice	786
56	Metz Clermont	438	116	Lille Toulouse	792
57	Dijon Nice	439	117	Nantes Nice	792
58	Lille Rennes	444	118	Lille Nice	834
59	Rennes Clermont	446	119	Lille Marseille	835
60	Dijon Marseille	449	120	Rennes Nice	849

Figure 24.24 Liste ordonnée des coûts. (suite)

c) Constitution du réseau de premier niveau (sans contrainte) : la figure 24.25 synthétise la démarche permettant de retenir les liens constituant le réseau de premier niveau. La figure 24.26 illustre ce réseau, tandis que la figure 24.27 en indique le coût total.

Ordre	Lien	Distance	Ordre	Lien	Distance
1	Metz Nancy	47	12	Nancy Dijon	175
2	Amiens Lille	98	13	Paris Lille	*Boucle*
3	Rennes Nantes	100	14	Bordeaux Toulouse	213
4	Paris Amiens	115	15	Metz Dijon	*Boucle*
5	Nancy Strasbourg	118	16	Rennes La Rochelle	*Boucle*
6	Nantes La Rochelle	122	17	Clermont Dijon	*Boucle*
7	Metz Strasbourg	*Boucle*	18	Strasbourg Dijon	*Boucle*
8	Clermont Lyon	137	19	Paris Dijon	264
9	La Rochelle Bordeaux	154	20	Nantes Bordeaux	*Boucle*
10	Marseille Nice	160	21	Toulouse Clermont	275
11	Dijon Lyon	174	22	Lyon Marseille	278

Figure 24.25 Détermination des liens du réseau de premier niveau.

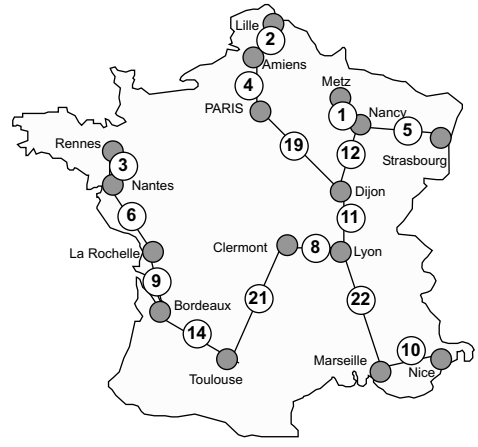


Figure 24.26 La topologie du réseau de premier niveau.

Coût total :

Ordre	Lien	Distance
1	Metz Nancy	47
2	Amiens Lille	98
3	Rennes Nantes	100
4	Paris Amiens	115
5	Nancy Strasbourg	118
6	Nantes La Rochelle	122
8	Clermont Lyon	137
9	La Rochelle Bordeaux	154
10	Marseille Nice	160
11	Dijon Lyon	174
12	Nancy Dijon	175
14	Bordeaux Toulouse	213
19	Paris Dijon	264
21	Toulouse Clermont	275
22	Lyon Marseille	278
Coût total (km)		**2 430**

Figure 24.27 Détermination du coût du réseau.

2) Constitution du réseau sous contrainte : la démarche est identique, si ce n'est que l'on refuse les liens ne respectant pas les contraintes imposées. La contrainte de débit impose un maximum de trois sites sur un lien concentré (deux nœuds et le site lui-même) et celle du nombre de bonds n'admet qu'un seul site derrière un nœud (figure 24.28).

Remarquons que du fait de la sporadicité des transferts, le débit réel offert à chaque site pourra atteindre, par instant, les 64 000 bit/s de débit nominal de la liaison.

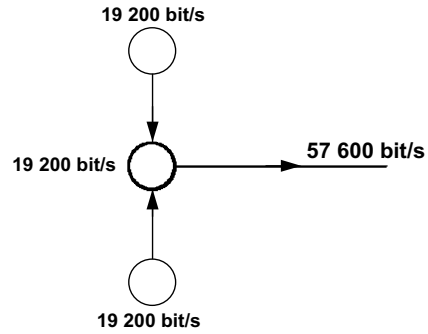


Figure 24.28 Concentration des nœuds.

En respectant les contraintes énoncées, on définit le réseau dont la topologie est représentée figure 24.29.

© Dunod – La photocopie non autorisée est un délit

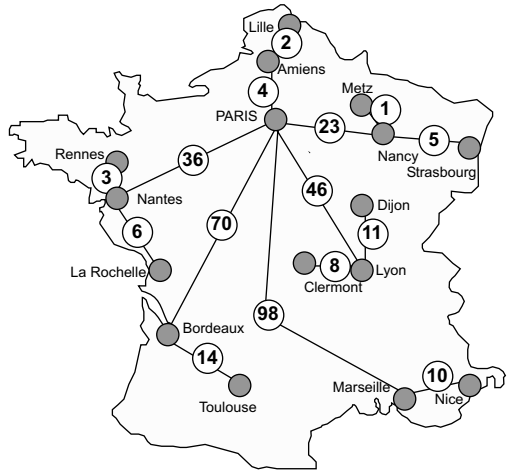


Figure 24.29 La topologie du réseau sous contrainte.

Coût du réseau sous contrainte :

Ordre	Lien	Distance
1	Metz Nancy	47
2	Amiens Lille	98
3	Rennes Nantes	100
4	Paris Amiens	115
5	Nancy Strasbourg	118
6	Nantes La Rochelle	122
8	Clermont Lyon	137
10	Marseille Nice	160
11	Dijon Lyon	174
14	Bordeaux Toulouse	213
23	Paris Nancy	282
36	Paris Nantes	344
46	Paris Lyon	393
70	Paris Bordeaux	500
98	Paris Marseille	662
Coût total (km)		**3 465**

Figure 24.30 Le coût du réseau sous contrainte.

3) Comparatif : le coût du réseau sans contraintes est de 2 430 (figure 24.27) quant à celui du réseau sous contrainte il s'élève à 3 465 (figure 24.30) soit un surcoût de 42,5%.

Exercice 24.4 Caractéristique mémoire d'un routeur

1) Taux d'arrivée des paquets (λ) : le taux d'arrivée des paquets se détermine en appliquant le principe de la superposition des flux, soit :

$$\lambda = 2 \times 4 + 2 \times 2 + 3 \times 6 + 5 \times 5 = 55 \text{ paquets/seconde}$$

2) Taux de service (μ) : le taux de service représente le nombre de paquets traités par seconde. Il est donné par la relation :

$$\mu = 1 / t_s \text{ où ts représente le temps de service soit,}$$

$$t_s = (128 \times 8 / 64\,000) = 16 \text{ ms}$$

$$\mu = 1 / 16\ 10^{-3} = 62{,}5 \text{ paquets/seconde}$$

3) Charge du système (ρ) : la charge du système ou intensité de trafic est le rapport entre la charge soumise et la charge admissible.

$$\rho = 55 / 62{,}5 = 0{,}88$$

Notons que le système est stable ($\rho < 1$), mais proche de la saturation.

4) Nombre de paquets dans le routeur (*N*) : le nombre de paquets dans le routeur est donné par la relation $N = \rho / (1 - \rho)$, soit :

$$N = \rho /(1 - \rho) = 0{,}88 / (1 - 0{,}88) = 7{,}3 \text{ paquets}$$

5) Temps moyen d'attente (t_a) : le temps moyen d'attente correspond au produit du nombre de paquets dans le routeur par le temps de traitement d'un paquet (temps de service) soit :

$$t_a = N \times t_s = 7{,}3 \times [(128 \times 8) / 64\,000] = 7{,}3 \times 0{,}016 = 0,\ 1\ 168 \text{ seconde}$$

6) Nombre de paquets dans la file d'attente (paquets en attente, *Na*)

$$Na = \lambda \times t_a = 55 \times 0{,}1168 = 6{,}424 \text{ paquets}$$

7) Temps de réponse ou temps de queue (t_q)

$$t_q = \mu / \lambda = 7{,}3 / 55 = 0{,}1327 \text{ s}$$

8) Taille du buffer (*T*)

$$T = \text{Nombre d'items en attente} \times \text{taille d'un item}$$

$$T = 6{,}424 \times 128 = 822 \text{ octets}$$

On retiendra une taille buffer de 1 ko soit une contenance de 8 paquets, la file d'attente est donc du type M/M/1/8.

9) Probabilité de perte d'un item

Nombre moyen de paquets dans le système : 7,3 paquets

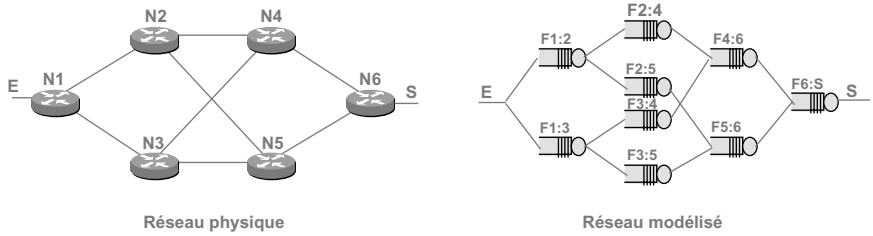
$$\text{si } \rho \neq 1\ p_n = \frac{\rho^n(1-\rho)}{1-\rho^{K+1}} = \frac{0{,}88^{\,7{,}3}\,(1-0{,}88)}{1-0{,}88^{8+1}} = 0{,}075$$

Notons que pour une charge de 50 %, la probabilité de perte serait encore de 2 %, c'est là que réside la difficulté du dimensionnement des mémoires tampons dans les éléments actifs.

© Dunod – La photocopie non autorisée est un délit

Exercice 24.5 Temps de transit dans un réseau

La méthode consiste à considérer le réseau comme une seule file d'attente et à appliquer la relation de Little pour déterminer le temps de transit. Pour cela, il convient, à partir du trafic écoulé par chaque nœud, de déterminer le nombre de paquets en transit dans le réseau et d'appliquer ensuite la relation de Little.



Réseau physique — Réseau modélisé

Lien	Proportion du trafic écoulé
N1-N2	75 %
N2-N4	50 %
N3-N5	25 %

Figure 24.31 Le réseau modélisé.

Rappelons les conditions :

- Longueur moyenne d'un paquet 128 octets
- Débit des liens 64 kbit/s
- Taux d'arrivée en E : $\lambda = 30$ paquets/s
- Temps de service : $t_s = 128 \times 8 / 64\,000 = 16$ ms
- Taux de service : $\mu = 1/t_s = 1/16\ 10^{-3} = 62{,}5$ paquet/s

D'où le tableau de synthèse suivant (figure 24.32) :

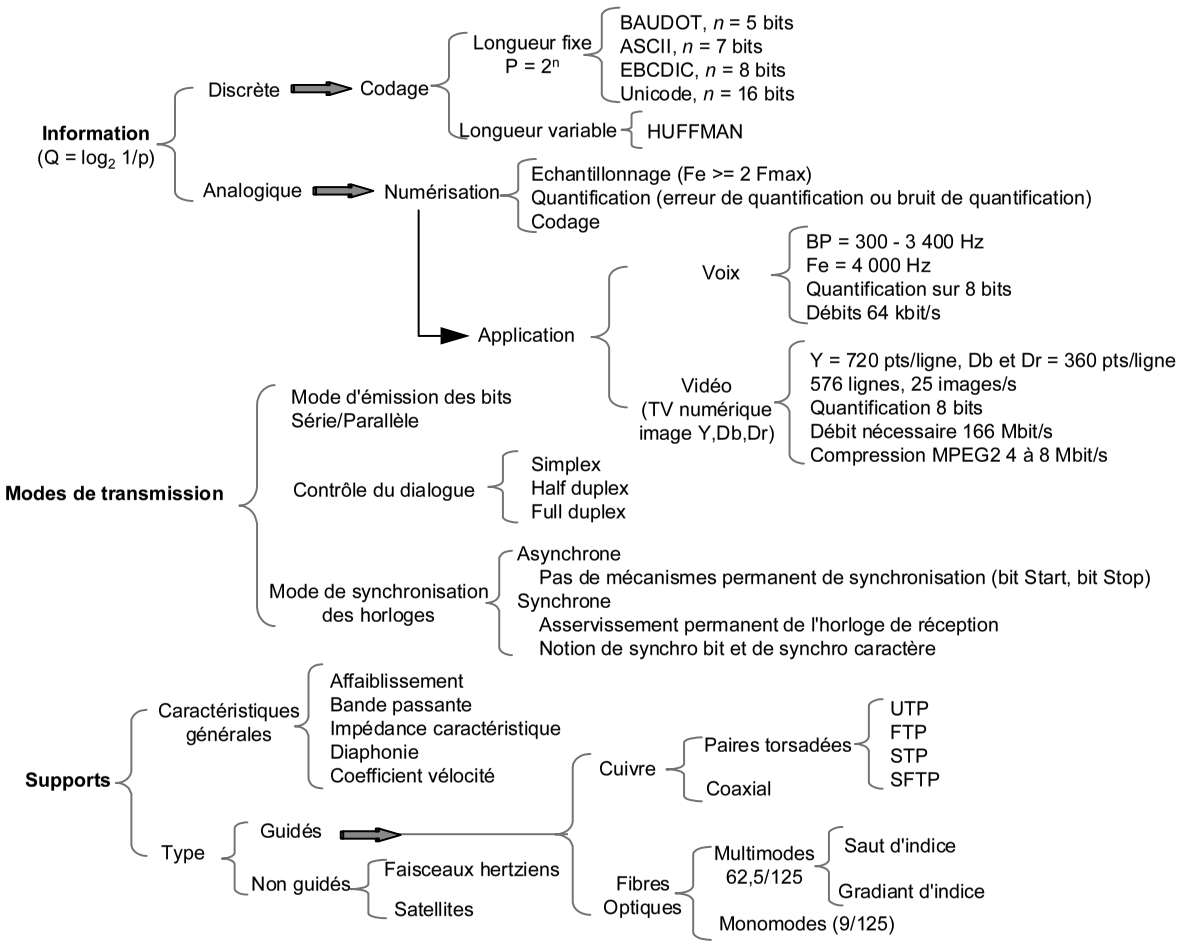
File	Trafic %	Taux d'arrivée λ	Charge $\rho = \lambda / \mu$	Nb items dans le nœud $\mu = \rho / (1-\rho)$
F1:2	0,75	22,5	0,36	0,5625
F1:3	0,25	7,5	0,12	0,1363
F2:4	0,375	11,25	0,18	0,2195
F2:5	0,375	11,25	0,18	0,2195
F3:4	0,1875	5,625	0,09	0,098
F3:5	0,0625	1,875	0,03	0,0309
F4:6	0,5625	16,875	0,27	0,3698
F5:6	0,4375	13,125	0,21	0,2658
F6:S	1	30	0,48	0,9230
Nombre de paquets dans le réseau :				2,8253

Figure 24.32 Les paquets en transit dans le réseau.

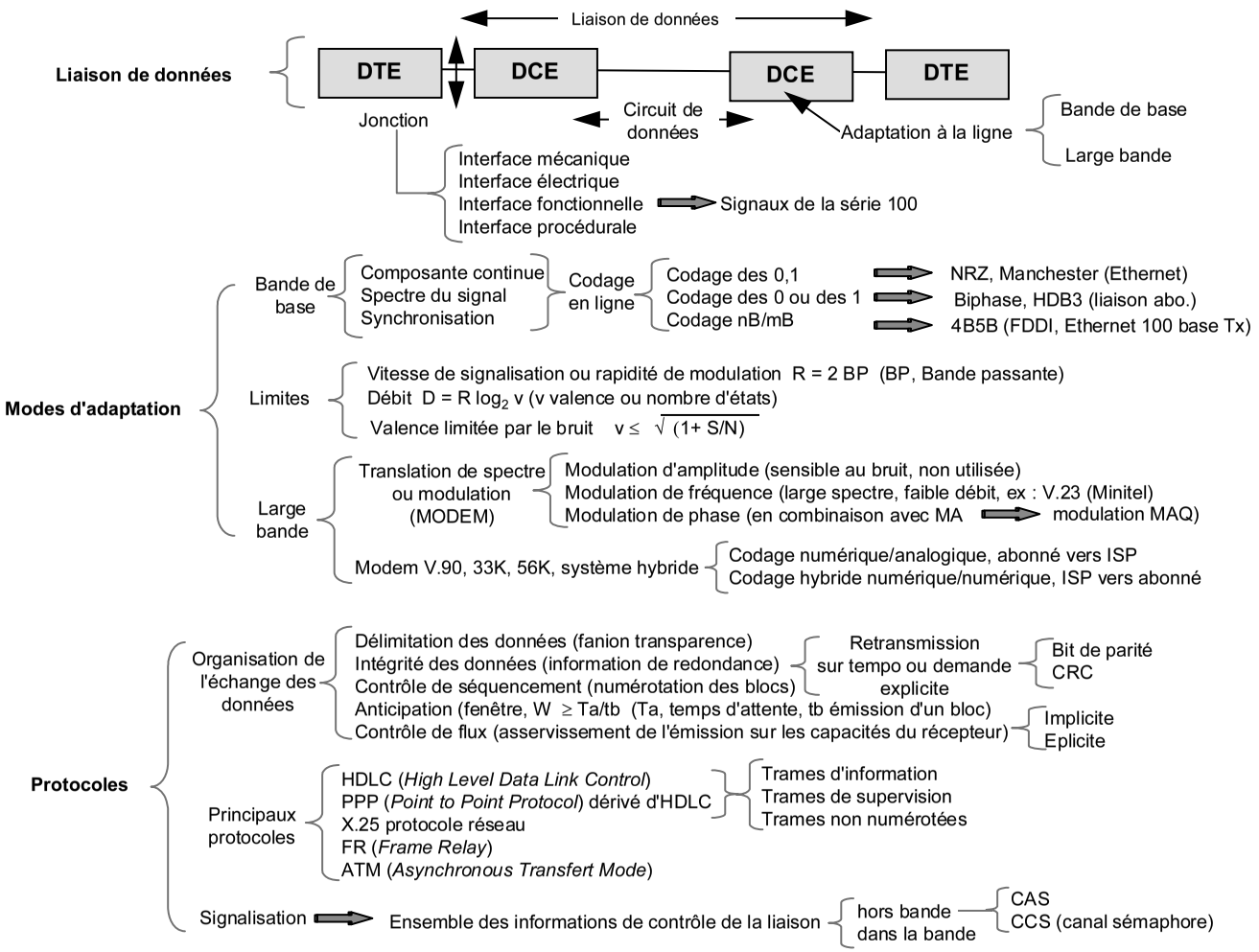
Temps de transit dans le réseau :

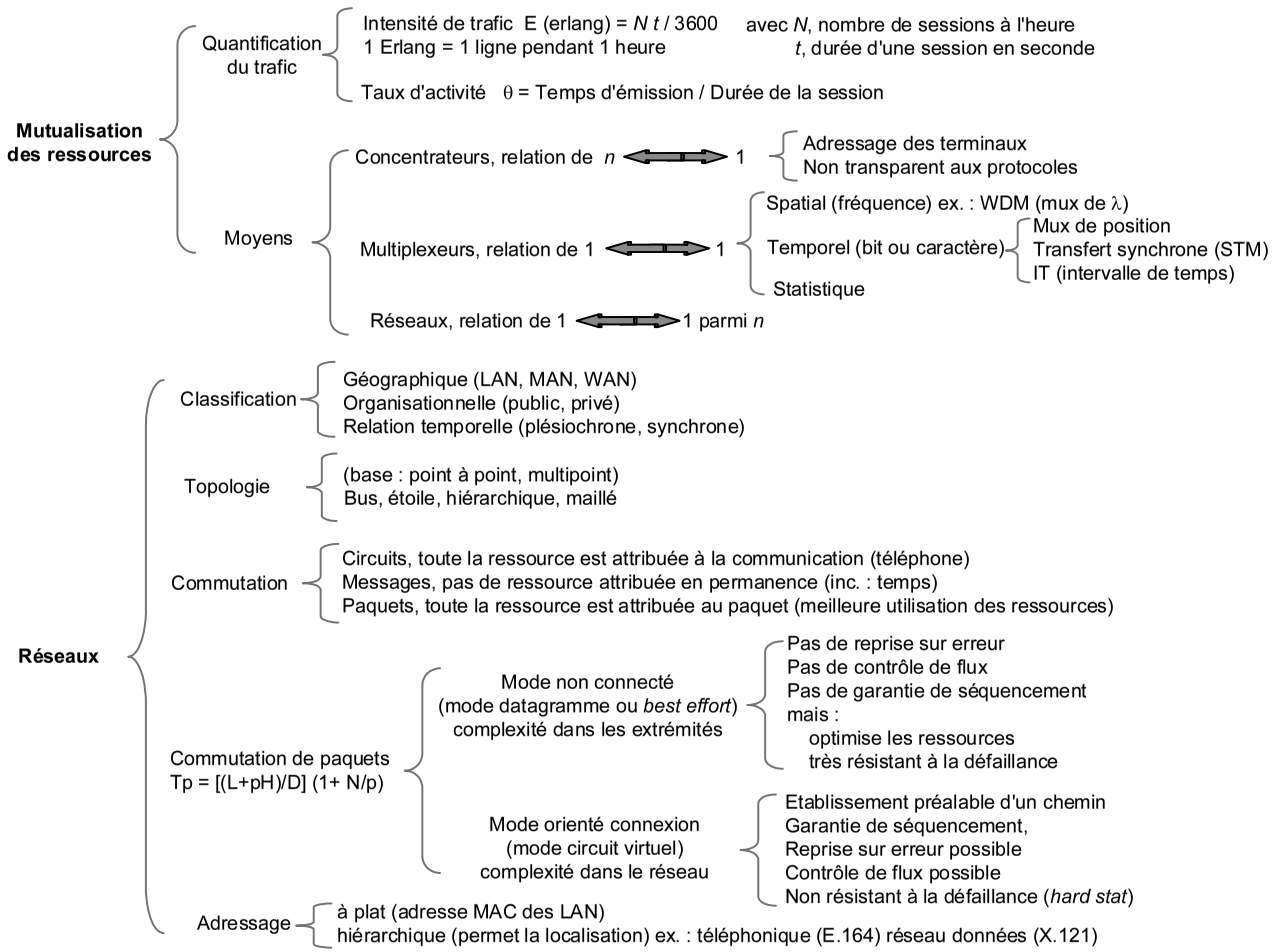
$$N = \lambda \times t_q \quad \text{soit} \quad t_q = N / \lambda = 2{,}8253/30 = 94 \text{ ms}$$

Synthèse des fondamentaux

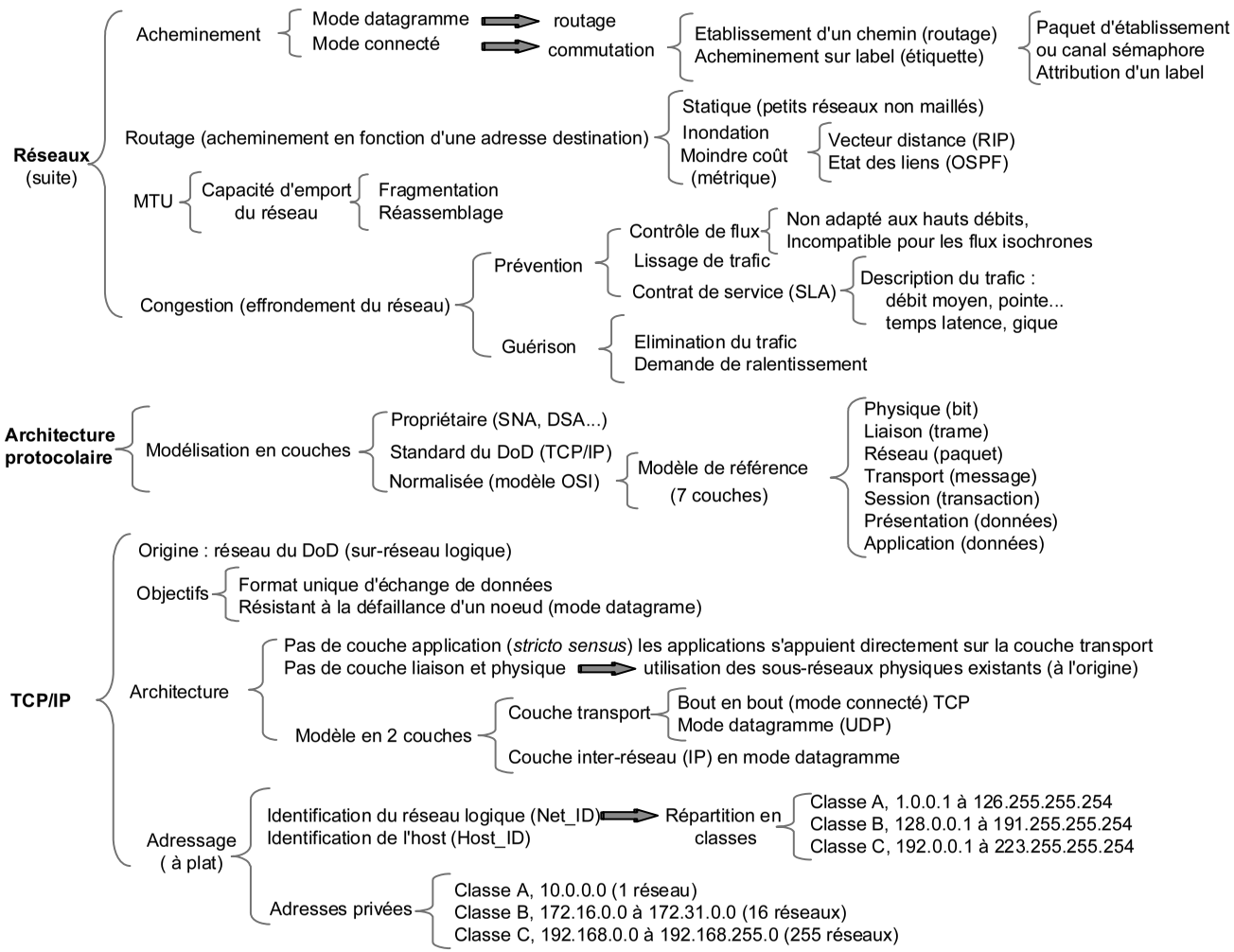

Information
(Q = log2 1/p)
Discrète
Codage
Longueur fixe
P = 2n
BAUDOT, n = 5 bits
ASCII, n = 7 bits
EBCDIC, n = 8 bits
Unicode, n = 16 bits
Longueur variable
HUFFMAN
Analogique
Numérisation
Echantillonnage (Fe >= 2 Fmax)
Quantification (erreur de quantification ou bruit de quantification)
Codage
Application
Voix
BP = 300 - 3 400 Hz
Fe = 4 000 Hz
Quantification sur 8 bits
Débits 64 kbit/s
Vidéo
(TV numérique
image Y,Db,Dr)
Y = 720 pts/ligne, Db et Dr = 360 pts/ligne
576 lignes, 25 images/s
Quantification 8 bits
Débit nécessaire 166 Mbit/s
Compression MPEG2 4 à 8 Mbit/s
Modes de transmission
Mode d'émission des bits
Série/Parallèle
Contrôle du dialogue
Simplex
Half duplex
Full duplex
Mode de synchronisation
des horloges
Asynchrone
Pas de mécanismes permanent de synchronisation (bit Start, bit Stop)
Synchrone
Asservissement permanent de l'horloge de réception
Notion de synchro bit et de synchro caractère
Supports
Caractéristiques
générales
Affaiblissement
Bande passante
Impédance caractéristique
Diaphonie
Coefficient vélocité
Type
Guidés
Non guidés
Faisceaux hertziens
Satellites
Cuivre
Paires torsadées
UTP
FTP
STP
SFTP
Coaxial
Fibres
Optiques
Multimodes
62,5/125
Saut d'indice
Gradiant d'indice
Monomodes (9/125)

© Dunod – La photocopie non autorisée est un délit



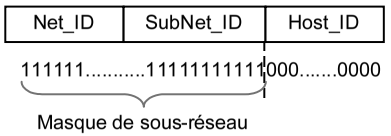

Mutualisation des ressources
Quantification du trafic
Intensité de trafic E (erlang) = N t / 3600 avec N, nombre de sessions à l'heure
1 Erlang = 1 ligne pendant 1 heure t, durée d'une session en seconde
Taux d'activité θ = Temps d'émission / Durée de la session
Moyens
Concentrateurs, relation de n 1
Adressage des terminaux
Non transparent aux protocoles
Multiplexeurs, relation de 1 1
Spatial (fréquence) ex. : WDM (mux de λ)
Temporel (bit ou caractère)
Mux de position
Transfert synchrone (STM)
IT (intervalle de temps)
Statistique
Réseaux, relation de 1 1 parmi n
Réseaux
Classification
Géographique (LAN, MAN, WAN)
Organisationnelle (public, privé)
Relation temporelle (plésiochrone, synchrone)
Topologie
(base : point à point, multipoint)
Bus, étoile, hiérarchique, maillé
Commutation
Circuits, toute la ressource est attribuée à la communication (téléphone)
Messages, pas de ressource attribuée en permanence (inc. : temps)
Paquets, toute la ressource est attribuée au paquet (meilleure utilisation des ressources)
Commutation de paquets
Tp = [(L+pH)/D] (1+ N/p)
Mode non connecté
(mode datagramme ou best effort)
complexité dans les extrémités
Pas de reprise sur erreur
Pas de contrôle de flux
Pas de garantie de séquencement
mais :
optimise les ressources
très résistant à la défaillance
Mode orienté connexion
(mode circuit virtuel)
complexité dans le réseau
Etablissement préalable d'un chemin
Garantie de séquencement,
Reprise sur erreur possible
Contrôle de flux possible
Non résistant à la défaillance (hard stat)
Adressage
à plat (adresse MAC des LAN)
hiérarchique (permet la localisation) ex. : téléphonique (E.164) réseau données (X.121)

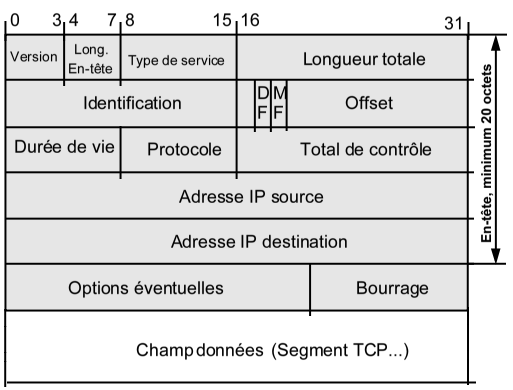
© Dunod – La photocopie non autorisée est un délit



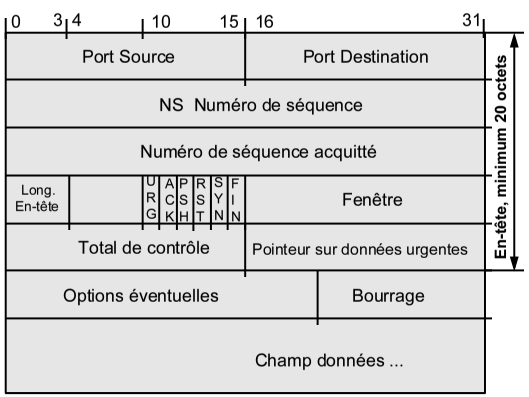
TCP/IP

- **Masque de sous-réseau**
  - Optimise l'utilisation de l'espace d'adressage
  - Facilite le routage
  - Champ de bits à 1 pour espace adresse du sous-réseau
- **Capacité de numérotation**
  - Avec *n* bits on numérote : $2^n - 2$ sous-réseaux ou machines
  - Le champ Host_ID à zéro identifie le réseau ou le sous-réseau
  - Le champ Host_ID à 1 correspond à l'adresse de *broadcast*
- **Identification des protocoles**
  - Ethertype identifie le protocole de niveau 3
  - Protocole identifie le protocole de niveau 3
  - Port identifie l'application
- **Port**
  - La notion de port autorise le multiplexage des connexions de transport
  - L'association N°Port/Adresse/Protocole (source et destination) forme un socket
- **Contrôle de flux et de congestion**
  - **Contrôle de flux** de bout en bout, asservit l'émetteur sur les capacités du récepteur (contrôle de flux dynamique)
  - IP mode *best effort* : contrôle de flux de bout en bout réalisé par TCP
  - **Contrôle de congestion** non fait par le réseau (*best effort*) TCP lors de la perte d'un ACK
  - (perte ou réception hors délai) suppose le réseau congestionné, il augmente la temporisation (RTO)
  - et diminue la fenêtre (mesure permanente du RTT pour ajuster le RTO)
- **UDP**
  - Transport en mode datagramme
  - Utilisé pour le temps réel (pas de reprise sur erreur, contrôle de flux et de congestion)





Datagramme IP



Segment TCP

Glossaire[1]

A

AAL (*ATM Adaptation Layer*) Dans l'architecture ATM, la couche AAL est chargée de l'adaptation des unités de données des protocoles supérieurs en fonction des caractéristiques retenues pour le transfert (isochronisme...). Les services de la couche AAL se déclinent en AAL1 (Service à débit constant), AAL2 (Service sur connexion à débit variable), AAL3/4 (Service à débit variable pour le transfert de données) et AAL5 (Service sur connexion à débit variable). Voir *ATM*.

ABM (*Asynchronous Balanced Mode*) Mode de communication supporté par HDLC (et par d'autres protocoles dérivés) concernant les communications point à point orientées poste à poste, dans lequel chaque station peut déclencher la transmission.

ABR (*Available Bit Rate*) Classe de service dans ATM qui autorise une source à modifier son débit disponible en fonction d'information en provenance des commutateurs internes du réseau. Voir *CBR, UBR* et *VBR*.

Accès de base ou BRI *(Basic Rate Interface*) Accès RNIS à 144 kbit/s, composé de deux canaux B à 64 kbit/s pour la transmission de la voix, de données et éventuellement d'images et d'un canal D à 16 kbit/s pour la transmission de la signalisation et de données (X.25). Voir aussi *RNIS et RNIS large bande.*

Accès primaire ou PRI *(Primaire Rate Interface*) Accès RNIS composé de 30 canaux B à 64 kbit/s (voix, données, images) et d'un canal D à 64 kbit/s (signalisation). Voir aussi *RNIS et RNIS large bande.*

Accusé de réception de bout en bout Méthode d'acquittement et de reprise sur erreur dans laquelle ce sont les organes d'extrémité qui assurent le contrôle et la reprise sur erreur. Cette méthode d'acquittement simplifie la réalisation du sous-réseau physique de transport. En environnement faiblement perturbé, l'accusé de réception de bout en bout améliore les performances du réseau (diminution de la charge de traitement des nœuds intermédiaires). Voir *Accusé de réception local*.

Accusé de réception local Méthode d'acquittement et de reprise sur erreur utilisée entre deux nœuds adjacents d'un réseau. Ce mode d'acquittement permet la reprise sur erreur au plus vite, elle minimise les délais de transmission de bout en bout en environnement perturbé. Voir *Accusé de réception de bout en bout*.

ACD (*Automatic Call Distributor*) Système de distribution des appels téléphoniques entrants ou sortants.

Acheminement Processus qui consiste à envoyer un bloc d'information (cellule, trame ou paquet) à sa destination finale *via* une ou plusieurs stations du réseau.

1. Certaines définitions de ce glossaire sont extraites du dictionnaire Cisco des termes et acronymes réseaux, et reproduits ici avec l'aimable autorisation de Cisco Systems France.

ACK (*Abréviation de acknowledgment*) Message généralement envoyé par une unité du réseau à une autre pour accuser réception d'un événement (réception d'un message, par exemple). Voir *Accusé de réception local et de bout en bout, NACK*.

ACL (*Access Control List*) Liste de contrôle des droits sur des fichiers, des accès réseau...

Adaptateur Carte PC qui assure les communications du réseau à destination et en provenance d'une station. Synonyme NIC (*Network Interface Card*).

Adaptateur d'impédance Voir *Balun.*

ADCCP (*Advanced Data Communication Control Protocol*) Protocole standard ANSI de liaison de données orienté bit.

ADCT (*Adaptative Discrete Cosinus Transform*) Méthode de codage mis en œuvre dans le codage d'image et utilisant la transformation en cosinus discrète.

Administration de réseau Terme générique utilisé pour décrire les systèmes ou les opérations qui permettent maintenir ou de dépanner un réseau.

ADPCM (*Adaptative Differential Pulse Coded Modulation*) Méthode de compression de la voix. Chaque échantillon est codé par rapport à la valeur de l'échantillon précédent. Cette technique permet de réduire la bande à 16, 32 ou 48 kbit/s selon le nombre de bits utilisés pour coder la différence.

Adresse Ensemble de données structurées utilisé pour identifier une entité unique, par exemple une station appartenant à un réseau.

Adresse de diffusion Adresse permettant la transmission simultanée à toutes les stations d'un réseau (*broadcast*).

Adresse de groupe Adresse de diffusion limitée permettant la transmission simultanée à plusieurs stations. Synonyme adresse multidestinataire (*multicast*).

Adresse Internet Adresse sur 32 bits affectée aux interfaces réseaux utilisant le protocole IP (version 4). Cette adresse est écrite sous la forme de 4 octets séparés par des points en format décimal (*dotted decimal format*). Dans la version 6 d'IP la longueur d'adresse a été portée à 128 bits. Synonyme *adresse IP.*

Adresse IP Voir *Adresse Internet.*

Adresse MAC Également appelée *adresse physique.* Cette adresse sur 6 octets identifie de manière unique une machine sur un réseau, ces adresses sont en principe gérées par l'IEEE. L'adresse IEEE est divisée en deux champs. Le premier identifie le constructeur (attribué par l'IEEE) de l'interface matérielle, le second est un numéro séquentiel attribué par le constructeur dans une séquence déterminée par l'IEEE. L'adresse IEEE garantit l'unicité de l'adresse MAC attribuée.

Adresse multidestinataire Adresse qui fait référence à plusieurs stations d'un réseau. Synonyme adresse de groupe.

Adresse physique Voir *Adresse MAC.*

Adresse source Adresse d'une station de réseau jouant le rôle d'expéditeur. Cette adresse peut être une adresse physique (adresse MAC) ou une adresse d'accès à un réseau (adresse X.121) mais aussi la désignation d'un point d'accès à un service (*SAP*, *Service Access Point dans la terminologie* ISO).

Adresse unique Adresse spécifiant une seule station d'un réseau (*unicast*).

ADSL (*Asymetrical Data Subscriber Line*) Technologie de traitement numérique du signal autorisant des débits élevés sur une simple ligne téléphonique. Les flux sont dissymétriques (640/6 000 kbit/s). À l'origine prévu pour un service de vidéo à la demande, l'ADSL constitue aujourd'hui l'offre d'accès haut débit à Internet.

Affaiblissement du signal Mesure le rapport entre la puissance du signal à l'entrée d'un système et celle en sortie. L'affaiblissement s'exprime en db (décibel).

AFI (*Authority and Format Identifier*) L'adresse réseau (*N-SAP, Network Service Access Point*) comporte trois champs : l'AFI, l'IDI (*Initial Domain Identifier*), *DSP (Domain Specific Part*). Le champ AFI identifie l'autorité d'adressage, précise le format et la syntaxe de l'adresse. Par exemple : l'adresse X.121 est désignée par l'AFI = 38. Voir *IDI* et *DSP*.

Algorithme Ensemble de règles opératoires et de procédés permettant de résoudre un problème par l'exécution d'un nombre fini d'opérations.

Algorithme de Dijkstra Algorithme de routage par méthode de choix du plus court chemin pour déterminer l'arborescence de plus court chemin. Couramment utilisé dans les algorithmes de routage à état des liaisons. Voir aussi *Algorithmes de*

routage par vecteur de distance et *Algorithmes de routage à état des liaisons.*

Algorithme de Karn Algorithme qui améliore les estimations de temps de transmission aller-retour en permettant aux protocoles des couches transport de différencier les mesures de bonne et de mauvaise qualité.

Algorithme de Nagle Algorithme composé de deux formules de contrôle de congestion qui peuvent être utilisées dans les réseaux TCP. L'une réduit la fenêtre d'émission et l'autre limite l'envoi des petits datagrammes.

Algorithme de routage à état des liaisons Algorithme selon lequel chaque routeur transmet des informations sur le coût de la connexion à chacun de ses voisins à tous les nœuds de l'inter-réseau. Ce type d'algorithme crée une vue cohérente du réseau et diminue les risques de boucles de routage. Voir aussi *Algorithme de routage par vecteur de distance, OSPF, IS-IS (Intermediate System to Intermediate System).*

Algorithme de routage Bellman-Ford Voir *Algorithme de routage par vecteur de distance.*

Algorithme de routage par vecteur de distance Catégorie d'algorithmes de routage également appelé algorithme de routage Bellman-Ford qui itère sur le nombre de sauts d'une route pour trouver l'arbre recouvrant de plus court chemin. Ce type d'algorithme implique que chaque routeur envoie toute sa table de routage à chaque mise à jour, mais uniquement à ses voisins. Ces algorithmes peuvent générer des boucles de routage mais sont, au niveau calcul, plus simples que les algorithmes de routage d'état de liaison. Voir *Algorithme de routage d'état de liaison* et *Algorithme de Dijkstra.*

Algorithme du Lempel Ziv Algorithme de compression de données.

Algorithme du spanning tree (ou arbre recouvrant) Méthode d'acheminement utilisée dans les ponts entre réseaux locaux afin d'éviter la formation de boucles.

Alias Nom de substitution utilisé pour identifier un objet en lieu et place de son nom complet.

ALOHA Technique de transmission utilisée pour assurer le partage d'un support commun. La station qui a des données à transmettre les transmet sans se préoccuper de l'état du support. Si le message émis est brouillé par la présence d'un autre signal sur le support, il ne sera pas acquitté et sera retransmis ultérieurement. La technique ALOHA a été utilisée pour réaliser des communications entre différentes îles d'Hawaii.

Alternat Voir *Half duplex.*

Amplitude Valeur de crête d'un signal analogique ou numérique.

AMRC (*Accès multiple à répartition de code ou CDMA, Code Division Multiple Access*), une seule fréquence est utilisée et un code est attribué à chaque utilisateur. Cette technique est complexe mais accroît la capacité d'accueil des bases en simplifiant la gestion des fréquences.

AMRF (*Accès multiple à répartition de fréquence* ou *FDMA*, *Frequency Division Multiple Access*) Technique de multiplexage fréquentiel dans laquelle une fréquence est allouée à chaque utilisateur.

AMRT (*Accès multiple à répartition dans le temps* ou *TDMA*, *Time Division Multiple Access*) Technique de multiplexage temporel dans laquelle un intervalle de temps (IT) est alloué à chaque station. Plus souple que la précédente, cette technique nécessite une parfaite synchronisation des stations.

Analyseur de réseau Équipement matériel/logiciel qui offre diverses fonctionnalités (décodage de paquets spécifiques, tests de dépannage préprogrammés spécifiques, filtrages de paquets, transmissions de paquets, etc.).

Annuaire Base de données mettant en correspondance une adresse réseau et un nom (résolution de nom).

Annulateur de modem Voir *Éliminateur de modem.*

Anticipation Voir *Fenêtre d'anticipation*.

AnyLAN Voir *IEEE 802.12*.

API (*Application Programming Interface*) Interface de programmation qui met à disposition des programmeurs des primitives d'accès aux programmes systèmes.

Appel de procédure à distance (*RPC*, *Remote Procedure Call*) Mode d'interaction par appel de procédures entre applications situées sur des machines différentes d'un réseau. Définit un cadre permettant de traduire les changements de contexte entre ces applications (sans que l'application appelante ait à gérer ce changement). Le RPC correspond à une mise en œuvre simple d'un modèle de type client/serveur.

Arbre recouvrant Voir *Algorithme du spanning tree.*

© Dunod – La photocopie non autorisée est un délit

ARCEP Voir *ART*

Area Voir *Région.*

ARP (*Address Resolution Protocol*) Protocole Internet utilisé pour associer une adresse IP à une adresse MAC. Défini dans le document Internet RFC 826.

ARPANET Premier réseau de communication par paquets, développé début des années 1970. Le réseau ARPANET a évolué pour devenir Internet, et le terme ARPANET a été officiellement retiré en 1990.

ARQ (*Automatic Repeat Request*) Technique de communication dans laquelle le récepteur détecte les erreurs et demande la répétition de la transmission.

ART (Autorité de régulation des télécommunications), créée par la loi du 27 juillet 1996, l'ART est chargée de définir le cadre de la concurrence entre les différents opérateurs. L'ART est devenue l'ARCEP (Autorité de régulation des télécommunications électroniques et des postes) en ajoutant à ses compétences le secteur postal (loi du 20 mai 2005).

Arythmique Voir *Asynchrone*.

ASCII (*American Standard Code for International Interchange*) Code utilisé pour la représentation des données. La longueur d'un mot du code est fixée à 7 bits (128 caractères, signes ou commandes représentables). Normalisé sous le nom de CCITT N°5 ou (AI5, Alphabet International N°5) le code ASCII a été étendu 8 bits pour représenter les caractères nationaux (ISO 8859-x) et dans les micro-ordinateurs des caractères semi-graphiques, on parle alors d'ASCII étendu ou encore d'ASCII IBM.

ASK (*Amplitude Shift Keying*) Voir *Modulation d'amplitude*.

ASN-1 (*Abstract Syntax Notation One*) Langage normalisé par l'ISO permettant de décrire des types de données de façon totalement indépendante des structures et des techniques de représentation informatiques utilisées. (Norme internationale ISO 8824 de décembre 1987). Voir aussi *BER.*

Asynchrone Se dit lorsque les événements gérés n'ont aucun lien temporel entre eux. Synonyme *arythmique*. Voir *Transmission asynchrone*, *Terminal asynchrone.*

ATDM (*Asynchronous Time Division Multiplexing*) Méthode de transmission d'information qui utilise le multiplexage par répartition temporelle, mais dans laquelle les tranches de temps sont, non pas pré-affectées à des émetteurs spécifiques, mais affectées le moment venu.

ATM (*Asynchronous Transfer Mode*) Norme UIT de *relais de cellules* dans laquelle les informations destinées à différents types de services (voix, vidéo, données) sont transmises en paquets (cellules) de longueur fixe.

ATM Forum Consortium de constructeurs, d'opérateurs, de consultants et d'utilisateurs chargés de définir et de promouvoir les technologies à base d'ATM.

Atténuation Perte d'amplitude du signal sur les lignes et équipements de transmission. Synonyme affaiblissement.

AUDIOTEX Système de communication vocale (kiosque téléphonique) dans lequel l'opérateur téléphonique et le fournisseur de services se partagent les revenus.

AUI (*Attachment Unit Interface*) Interface de raccordement de station. Câble IEEE 802.3 reliant le MAU (*Media Access Unit*) à la station. Le terme AUI peut également faire référence au connecteur de fond de panier de la station sur lequel un câble AUI peut être branché. Également appelé *câble émetteur-récepteur.*

Authentification Méthode de sécurisation des échanges dans lequel l'identité des correspondants est vérifiée avant tout échange de données.

Authority zone Voir *Zone d'autorité.*

Autocommutateur privé Standard téléphonique installé dans les locaux de l'utilisateur. L'autocommutateur met en relation une ligne entrante ou sortante avec un poste téléphonique local ou deux postes téléphoniques locaux entre eux. Synonymes *PABX et PBX.*

Avis Terme qui désigne une norme édictée par le CCITT (UIT).

B

B-ISDN (*Broadband Integrated Service Digital Network*) Voir *RNIS large bande*

B-Router (*Bridge Router*) Équipement assurant à la fois des fonctions de pont et de routeur entre deux réseaux. Synonymes *brouteur* et *pont-routeur.*

Backbone Voir *Réseau dorsal.*

BAL Abréviation de Boîte aux lettres, correspond à un espace de stockage dans lequel sont mémorisés les messages échangés entre deux processus ou deux correspondants (courrier électronique).

Balun (contraction de *balanced, unbalanced*) Composant utilisé pour adapter deux lignes d'impédance caractéristique (Zc) différente, généralement une ligne à paires torsadées et un coaxial. Synonyme *adaptateur d'impédance.*

Bande de base Technologie de transmission native en réseau qui n'opère aucune translation du spectre. Ce terme est l'opposé du terme large bande où les données à transmettre sont translatées en fréquence (modulation). Ethernet est un exemple de réseau à bande de base.

Bande de garde Bande de fréquences utilisée entre deux canaux de communication qui permet de séparer les canaux pour empêcher toute interférence mutuelle. Voir *Intermodulation*.

Bande étroite Voir *Bande de base.*

Bande passante Dans un système de transmission, les signaux sont transmis avec une distorsion faible dans une bande de fréquences comprise entre une fréquence basse (fréquence de coupure basse) et haute (fréquence de coupure haute). Au-delà de ces fréquences, tous les signaux sont fortement atténués. On appelle bande passante d'un système l'espace de fréquences tel que tout signal appartenant à cet intervalle ne subisse qu'un affaiblissement déterminé par rapport à un signal de référence. L'affaiblissement s'exprime en décibel. La bande passante est généralement définie pour une atténuation de 3 dB (réduction de moitié de la puissance transmise).

Baud Unité de mesure de rapidité de modulation, c'est-à-dire le nombre d'intervalles de temps élémentaires du signal numérique (nombre d'états).

Bc (*Commited Burst size*) Dans le relais de trames, le réseau ne traite pas la congestion, mais essaie de s'en protéger en limitant le débit des accès. Jusqu'à un certain volume de données (*Bc*, *Committed Burst sze*) le réseau assure le transfert de toutes les trames entrantes. Au-delà, le réseau autorise un certain débordement mais marque les trames en excès (bit DE, *Discard Eligibility*). Lorsque le volume transmis atteint une valeur prédéfinie à l'abonnement (Be*, Excess Burst size*) toutes les trames en excédent sont éliminées en commençant par les trames marquées puis, si la congestion persiste et s'aggrave (congestion sévère), les trames non marquées et enfin les trames de signalisation.

BCD (*Binary Coded Decimal*) Voir *Décimal codé binaire*.

BCS (*Bull Cabling System*) Système de câblage préconisé par le constructeur BULL.

Be (*Excess Burst size*) Voir *Bc*.

BEB (*Binary Exponentiel Backoff*), ou encore algorithme de ralentissement exponentiel, détermine, dans les réseaux IEEE 802.3, le délai aléatoire d'attente avant que la station ne retente, après collision, une émission.

BECN (*Backward Explicit Congestion Notification*) Champ de la trame du relais de trames (1 bit) utilisé pour informer une source que son flux de données traverse au moins un commutateur en état de congestion. Voir *FECN* (*Forward Explicit Congestion Notification*).

BER (*Basic Encoding Rules*) Règles de codage des unités de données décrites dans le langage ASN-1.

BER (*Bit Error Rate*) Pourcentage de bits erronés reçus par rapport à la séquence de bits envoyés.

BGP (*Border Gateway Protocol*) Protocole de routage inter-domaine qui devrait remplacer le protocole EGP (*Exterior Gateway Protocol*).

Big-endian Méthode de stockage ou de transmission de données dans laquelle le bit ou l'octet le plus significatif est présenté en premier (de gauche à droite). Voir aussi *Little-endian.*

Binaire Système de codage de données composé uniquement de 0 et de 1.

Bit (Acronyme né de la contraction des mots anglais « *binary digit* ») Le bit est le plus petit élément d'information d'un système binaire transmissible, il peut prendre la valeur 0 ou 1. En principe le terme bit est invariable, mais l'usage le considère comme une unité classique et accorde le terme bit. Cependant on écrit 4 800 bits, mais 4,8 kbit ou encore 4 800 bit/s pour désigner le débit d'une ligne qui transmet 4 800 bits par seconde.

Bit par seconde (bit/s ou bps) Unité de mesure du débit d'informations binaires. En principe l'utilisation de l'abréviation « bps » est à bannir à cause de la possible confusion avec byte par seconde.

© Dunod – La photocopie non autorisée est un délit

Blindage Tresse métallique de protection entourant un (câble coaxial) ou plusieurs conducteurs (paire coaxiale) afin de le protéger des rayonnements électromagnétiques. Le blindage est plus efficace aux basses fréquences qu'un simple écrantage du câble. Voir *Écran*.

BLU (*Bande latérale unique*) Technique de modulation d'amplitude dans laquelle on a supprimé la porteuse et l'une des deux bandes latérales. Les signaux modulés en BLU sont moins sensibles à la dispersion du spectre (*fading* sélectif).

Bluetooth Technique de communication sans fil permettant à plusieurs systèmes de communiquer par liaison radio dans un rayon de quelques mètres.

Boucle de courant (*Current loop*) Système de signalisation où les interfaces connectées sont sensibles aux variations de courant et non aux variations de tension.

Boucle locale d'abonné Ligne entre un abonné et le réseau de téléphone public.

Boucle locale radio (BLR) Technique qui permet de raccorder un abonné du réseau téléphonique par une liaison hertzienne.

Bout en bout Se dit d'une connexion ou d'un contrôle qui met directement en relation les entités communicantes. Par exemple, dans le cas d'un contrôle d'erreur de bout en bout en bout, la détection d'erreur et la reprise sont effectuées par le destinataire et non par les relais intermédiaires. La couche transport d'ISO et de TCP/IP sont des couches de bout en bout.

BPDU (*Bridge Protocol Data Unit*) Paquet hello des protocoles « *spanning-tree* ». Voir aussi *PDU*.

BRI (*Basic Rate Interface*) Voir *Accès de base*.

Bridge Voir *Pont*.

Broadband Voir *Large bande*.

Broadcast Voir *Adresse de diffusion.*

Brouteur Voir *B-Router.*

Browser Logiciel d'exploration permettant de naviguer sur Internet. Synonyme *navigateur*.

Bruit Signal parasite sur un canal de communication. On distingue deux types de bruits : le bruit blanc (bruit naturel, occupant un large spectre, peu gênant) du bruit impulsionnel signal parasite intermittent provoquant une altération d'un bloc de données. Le rapport signal à sur bruit et la bande passante sont les deux éléments essentiels qui caractérisent un canal de transmission.

Bruit de quantification La numérisation d'un signal analogique comprend les étapes d'échantillonnage, de quantification et de codage. La quantification est effectuée par rapport à une échelle (échelle de quantification) et la valeur de l'échantillon est exprimée par rapport à la valeur la plus proche de l'échelle. Cette méthode introduit une erreur de quantification dite bruit de quantification.

Buffer (mémoire tampon) terme anglo-saxon passé dans le langage courant des informaticiens pour désigner un espace mémoire dédié.

Burst Synonyme de *rafale de trafic*.

Bus à jeton Architecture LAN utilisant un accès par passage de jeton sur une topologie en bus. Cette architecture est la base de la spécification LAN IEEE 802.4.

Byte Voir *Octet.*

C

Câblage Ensemble des éléments passifs permettant de raccorder les différents usagers d'un réseau local (câble, prises murales, panneaux de répartition ou de brassage...).

Câble Support de transmission composé de fils ou de fibres optiques enveloppés sous une gaine de protection.

Câble blindé Câble comportant une enveloppe métallique (tresse ou feuillard) dite blindage et assurant une protection contre les phénomènes électromagnétiques.

Câble coaxial Câble blindé composé d'une gaine extérieure cylindrique en tresse métallique qui entoure un conducteur intérieur central (âme).

Câble croisé Voir *Éliminateur de modem.*

Câble optique Voir *Fibre optique.*

Cache de noms Méthode de stockage, par un nœud, de la correspondance entre un nom d'hôte distant et son adresse sur le réseau.

Call-back Technique d'appel vers l'étranger consistant à appeler un opérateur étranger et à raccrocher. L'opérateur étranger établira alors la liaison avec le demandé et rappellera le demandeur. La communication est facturée au coût de l'opérateur étranger.

Canal B (*Bearer*) En RNIS, canal *duplex* à 64 kbit/s utilisé pour transmettre la voix ou des données.

Canal D (*Data*) Canal de signalisation du RNIS fonctionnant en *duplex* et à 16 kbit/s (accès de base) ou 64 kbit/s (accès primaire).

Canal E (*Echo*) Canal RNIS de contrôle de l'accès au canal D (écho du canal D).

Canal H (*High speed*) Canal RNIS à débit primaire fonctionnant en *full duplex* à 384 kbit/s non disponible en France.

Canal sémaphore Canal dédié à la signalisation entre deux ou plusieurs systèmes. Ex. : le canal D du RNIS.

CAP (*Carrierless Amplitude*/Phase modulation) Technique de codage.

Carrier signal Voir *Porteuse.*

Carrier Voir *Opérateur de télécommunication*.

CAS (*Channel Associated Signaling*) Signalisation de canaux numériques par vol de bits dans un IT de données (Trame T1) ou par IT réservé (Trame MIC, IT16).

CATV (*Cable Antenna TeleVision*) Voir *Câble coaxial*.

CBDS (*Connectionless Broadband Data Service*) Service d'interconnexion de réseaux WAN à haut débit fonctionnant en mode commutation de paquets non connecté. Synonyme *SMDS.*

CBR (*Constant Bit Rate*) Dans un réseau ATM, débit négocié et garanti durant toute la durée de la connexion. Voir *ABR, UBR* et *VBR.*

CCBNT (*Circuit commuté B non transparent*) Service offert sur un réseau RNIS dans lequel une connexion numérique de bout en bout n'est pas garantie.

CCBT (*Circuit commuté B transparent*) Service offert sur un réseau RNIS dans lequel une connexion numérique de bout en bout est garantie.

CCIR (*Comité consultatif international des radiocommunications*) Organisme international de normalisation chargé d'émettre des avis sur la technique et la réglementation des radiocommunications, et notamment sur l'attribution des fréquences radio. Le CCIR a été intégré à l'UIT.

CCITT (*Comité consultatif international télégraphique et téléphonique*) Organisme international de normalisation en matière de télécommunications, qui développe des normes de communication sous forme, par exemple, d'avis en V (V.23, V.24...) pour les lignes analogiques ou en X (X.25...) pour les réseaux de données. Le CCITT est devenu l'UIT-T.

CCS (*Common Channel Signaling*) Signalisation dans laquelle les informations de signalisation sont transmises sur un canal commun à toutes les communications. Le canal D du RNIS est un exemple de signalisation CCS.

Cellulaire Voir *Radio cellulaire*.

Cellule Élément de base du multiplexage et de la communication ATM. Chaque cellule se compose d'un en-tête de 5 octets et de 48 octets de données utiles.

CGI (*Common Gateway Inteface*) protocole de communication entre un serveur Web et une application.

CHAP (*Challenge Handshake Authentication Protocol*) Fonction de sécurité qui empêche tout accès non autorisé aux unités protégées. CHAP est un sous-protocole de PPP (*Point to Point Protocol*).

Chat (bavardage) communication écrite en temps réel sur Internet entre deux ou plusieurs internautes.

Cheapernet Terme faisant référence à la norme IEEE 802.3 10 Base2 ou au câble spécifié par cette norme. Thinnet, qui est également utilisé pour décrire cette norme, spécifie une version plus fine et moins onéreuse du câble Ethernet. Synonymes *câble noir, Ethernet capillaire, câble RG-58.*

Checksum Voir *Somme de contrôle, CRC* et *FCS.*

Chiffrement Technique de codage des informations qui applique un algorithme spécifique destiné à les rendre incompréhensibles à toute personne tentant de les lire illégalement. Le décryptage applique l'algorithme inverse et restructure les données dans leur format d'origine.

Chrominance En télévision couleur, le terme chrominance désigne les informations de couleur R, V, B. Voir *Luminance*.

CIR (*Commited Information Rate*) En *Frame Relay*, débit moyen d'information garanti.

Circuit Canal de communication entre plusieurs points.

Circuit virtuel (CV) Circuit logique établi pour assurer la fiabilité des communications entre deux stations d'un réseau.

© Dunod – La photocopie non autorisée est un délit

Circuit virtuel commuté (CVC) Circuit virtuel qui peut être établi dynamiquement à la demande. Inverse de *circuit virtuel permanent ou PVC (Permanent Virtual Circuit).*

Circuit virtuel permanent (CVP ou PVC) Circuit virtuel dont l'affectation est permanente.

Classe de service Voir *CoS*.

Client serveur Modèle d'organisation et de répartition des traitements entre un poste de travail « intelligent » et un serveur.

CLP (*Cell Loss Priority*) Dans une cellule ATM, le bit CLP indique une cellule pouvant, en cas de congestion, être éliminée en priorité.

Cluster Voir *Grappe*.

CMIP/CMIS (*Common Management Information Protocol/Common Management Information Services*) interface de service/de protocole de gestion de réseaux de l'ISO créée et normalisée par l'ISO pour la gestion de réseaux hétérogènes.

CMOT (*CMIP Over TCP*) Gestion d'un réseau TCP/IP par le protocole ISO CMIP.

CNLP/CLNS (*Connectionless Network Protocol/ConnectionLess Network Services*) Protocole/service de couche réseau ISO qui ne demande pas l'établissement d'un circuit avant la transmission des données (ISO 8473). CLNP est l'équivalent ISO de IP.

CNLS (*ConnectionLess Network Service*) Voir *Mode non connecté*.

Codage à la source Technique dans laquelle à un élément d'information on fait correspondre une combinaison binaire. Voir *ASCII*.

Codage en ligne Technique électrique qui consiste à modifier la forme du signal pour l'adapter aux exigences du support de transmission. Voir *Bande de base.*

Codage 4B5B Technique de codage des informations binaires dans laquelle un groupe de 4 bits est remplacé par une combinaison binaire de 5 bits telle qu'il existe au moins deux transitions par groupe de 5 bits. Le codage 4B5B est utilisé dans les réseaux FDDI.

Codage biphase ou Manchester Système de codage bipolaire développé à l'origine pour les réseaux Ethernet. Les informations de synchronisation sont incorporées dans le flot des données synchrones, à chaque temps bit correspond une transition du signal. La composante continue du codage biphase est nulle.

Codage différentiel Technique de codage numérique selon laquelle une valeur binaire est signalée par un changement de signal, et non par un niveau de signal particulier.

Codage Manchester différentiel Technique de codage numérique selon laquelle la transition du signal est de même sens que la précédente si le bit à coder est un 0 et de sens inverse si celui-ci est un 1. C'est la technique utilisée par les réseaux IEEE 802.5 et Token Ring.

Codage Manchester Voir *Codage biphase*.

CODEC Abréviation de codeur-décodeur. Équipement ou composant qui utilise généralement la modulation par impulsions codées pour transformer les signaux analogiques vocaux en signaux numériques, et *vice versa*.

Communauté En protocole SNMP, groupe logique d'unités faisant partie du même domaine administratif.

Commutation de cellules Forme particulière de la commutation de paquets. La cellule est « un paquet » de petite taille fixe. Voir *ATM*.

Commutation de circuits Technique dans laquelle un circuit physique dédié, ou un intervalle de temps, entre l'émetteur et le récepteur est établi et maintenu durant tout l'échange.

Commutation de messages (*Messages switching*) Technique de commutation consistant à diriger un message, dans son intégralité, de commutateur en commutateur, jusqu'à son destinataire.

Commutation de paquets (*Packets switching*) Technique consistant à transmettre un message segmenté en blocs (paquets) entre commutateurs jusqu'à son destinataire. Chaque paquet pouvant être acheminé de manière indépendante (mode datagrammes) ou tous sur le même chemin (mode orienté connexion ou mode connecté). Voir aussi *Commutation de circuits* et *Commutation de messages.*

Commutation Ethernet (*Switched Ethernet*) Apparue dans le monde Ethernet, la commutation a été mise en œuvre pour résoudre les problèmes d'effondrement des réseaux (collisions) et garantir à une communication une certaine bande passante, la technique de commutation est aujourd'hui mise en œuvre dans tous les types de réseaux. Dans cette technique, le *hub* est remplacé par un commutateur rapide qui met en relation directe ses différents ports d'accès selon une table dite table de commutation.

Commutation spatiale Technique de commutation de circuits dans laquelle une mise en relation de deux abonnés par juxtaposition de circuits physique est réalisée.

Commutation temporelle Technique de mise en relation de deux abonnés par juxtaposition d'intervalle de temps (IT).

Compléments de service Ensemble de services offerts par le réseau téléphonique RNIS qui correspondent essentiellement à un enrichissement de l'offre téléphonique traditionnelle. Ils fournissent une prestation optionnelle donnant lieu à facturation (abonnement ou appel par appel). Ces prestations sont, pour la plupart, déjà offertes sur les installations privées par l'intermédiaire des PABX.

Compression Application à un ensemble de données d'un algorithme qui diminue l'espace/la largeur de bande nécessaire au stockage/à la transmission de cet ensemble.

Concentrateur Équipement qui permet le regroupement de plusieurs canaux dans un réseau à topologie en étoile. Ce terme est également utilisé pour faire référence à une unité qui contient plusieurs modules d'équipements de réseaux et d'interconnexion de réseaux.

Connecteur en T Équipement en forme de T comportant deux connecteurs femelles et un connecteur mâle BNC.

CONS (*Connection-Oriented Network Service*) Mode de transfert assurant aux protocoles des couches supérieures un fonctionnement orienté connexion. Voir *Mode orienté connexion.*

Contention Synonyme *collision.* Situation dans laquelle les unités en réseau sont en concurrence pour l'accès au support physique. Voir *Commutation de circuits.*

Contrôle d'erreur Technique permettant de garantir que les transmissions entre un émetteur et un destinataire sont exemptes d'erreur.

Contrôle de flux isarythmique Technique de contrôle de flux basée sur la circulation d'une autorisation sur le réseau (permis).

Contrôle de flux par fenêtre Méthode de contrôle de flux selon laquelle un récepteur donne à l'émetteur l'autorisation de transmettre des données jusqu'à ce qu'une fenêtre soit pleine. Lorsque la fenêtre est pleine, l'émetteur doit arrêter de transmettre jusqu'à ce que le récepteur ait déplacé la fenêtre. Cette méthode est utilisée notamment par TCP et d'autres protocoles de transport et par différents protocoles de couches de liaison.

Contrôle de flux Technique permettant d'assurer qu'une entité émettrice à trop fort débit ne submerge une entité réceptrice (asservissement de la cadence d'émission sur les capacités de réception du récepteur).

Contrôle de liaison logique (LLC, *Logical Link Control*) Sous-couche définie par l'IEEE de la couche liaison de données de l'ISO qui gère le contrôle des erreurs, le contrôle du flux et les échanges de trames.

Contrôle de parité (ou d'imparité) Technique de détection d'erreur qui consiste à ajouter au caractère transmis un bit à 1 ou à 0 (bit de parité) pour que la somme des bits à 1 transmis soit paire (contrôle de parité) ou impaire (contrôle d'imparité).

Cookie Petit fichier téléchargé et contenant des informations sur le site Web visité. Ces éléments seront réutilisés lors d'une prochaine connexion.

CoS (*Class of Service,* Classe de service) Regroupement logique de caractéristiques de transmission affectées à un type de flux. Voir *ABR, CBR, UBR, VBR.*

Couche Division fonctionnelle d'une architecture de communication. Une couche est un ensemble de services offert par une entité. Voir *OSI.*

Couche application Couche 7 du modèle de référence OSI. Cette couche met à disposition des programmes applicatifs des entités d'application (AE). Les principaux services de la couche application sont le courrier électronique (X.400), l'annuaire (X.500) et le transfert des fichiers (FTAM).

Couche liaison de données Couche 2 du modèle OSI. Ses principaux services sont la détection des erreurs et le contrôle du flux.

Couche physique Couche 1 du modèle OSI qui définit les interfaces électriques, mécaniques et physiques du réseau, et les différents aspects du support du réseau.

Couche présentation Couche 6 du modèle OSI, qui définit la représentation des données entre deux entités de la couche application.

Couche réseau Couche 3 du modèle OSI, qui concerne le routage des informations sur le réseau et les techniques d'adressage.

© Dunod – La photocopie non autorisée est un délit

Couche session Couche 5 du modèle OSI, qui coordonne l'activité des sessions entre les applications, le contrôle des dialogues.

Couche transport Couche 4 du modèle OSI, qui assure la fiabilité des transmissions entre les nœuds d'extrémité (EN). Cette couche assure également le contrôle d'erreur et le contrôle du flux des données, et utilise souvent des circuits virtuels pour garantir la fiabilité de la transmission des données.

Courant faible Se dit des câblages qui ne mettent en œuvre que des signaux dont la tension maximale n'est que de quelques volts et dont l'objet est le transport d'information et non d'énergie (téléphone, données...). Voir *Courant fort*.

Courant fort Se dit des installations dont l'objet essentiel est le transport d'énergie quel que soit les niveaux de tension transportés.

Courant porteur Voir *Modulation*.

Courrier électronique Voir *Messagerie électronique.*

Coût de routage Valeur arbitraire utilisée pour déterminer le chemin de moindre coût (débit, nombre de sauts, taille des files d'attente...) possible entre un point d'origine et un point de destination. Voir aussi *Métrique de routage.*

CRC (*Cyclic Redundancy Check*) Technique de recherche d'erreurs selon laquelle le destinataire d'une trame calcule un reste en divisant le contenu de la trame par un polynôme générateur principal, et compare le reste calculé (lui-même souvent appelé CRC) à la valeur calculée selon le même principe par l'émetteur et transmis avec l'unité de données. Si les deux valeurs sont différentes, le bloc reçu est rejeté et une retransmission est éventuellement redemandée. Synonyme c*ontrôle de redondance cyclique.* Voir *FCS*.

Critère de Nyquist Relation entre la bande passante du système et le nombre d'états significatifs. Voir *Rapidité de modulation, Baud*.

Crossbar Ancien système de commutation électromagnétique utilisé dans les réseaux téléphoniques.

CSMA/CD (*Carrier Send Multiple Access Collision Detection*) Réseau à accès multiple par détection de porteuse et détection de collisions. Procédure d'accès au canal par laquelle les stations voulant transmettre testent la présence d'un signal sur le canal. Si aucune activité électrique n'est détectée, les stations peuvent transmettre. Si deux stations transmettent simultanément, il se produit une *collision*, celle-ci est détectée par les stations concernées, qui arrêtent leur transmission et réalisent une retransmission après un temps d'attente aléatoire. L'accès CSMA/CD est utilisé par Ethernet et IEEE 802.3.

CT2 Norme de radiotéléphone numérique sans fil. Définit des petits terminaux de poche permettant d'appeler par l'intermédiaire de bornes situées à une certaine distance, mais non de recevoir.

CTI (*Computer Telephony Integrated*) Technique permettant l'interaction entre les éléments d'un appel téléphonique et une application informatique.

Current loop Voir *Boucle de courant*.

CV Voir *Circuit virtuel.*

CVC Voir *Circuit virtuel commuté.*

CVP Voir *Circuit virtuel permanent.*

Cycles par seconde Voir *Hertz.*

D

D_Channel Voir *Canal D*

Daemon Programme qui s'exécute en arrière-plan.

Datagramme (*Datagram*) Groupe logique d'information transmis sans qu'il ait été établi au préalable un circuit virtuel. La transmission n'est pas garantie, elle est dite *best effort*. Voir *Mode non connecté*.

DCB Voir *Décimal codé binaire.*

DCE (*Data Circuit Equipment*) Voir *ETCD.*

DCE (*Distributed Computing Environnement*) Ensemble de spécifications de l'OSF (Open System Fundation) organisant le traitement d'applications réparties en environnement Unix.

DCS 1800 (*Digital Cellular System* 1 800 MHz) Norme de radiotéléphonie numérique dérivée du GSM.

DE (*Discard Eligibility*) En cas de congestion, dans un réseau à relais de trames, les trames en excès sont purement et simplement éliminées par le réseau. Le bit *DE* est positionné par le réseau ou par les organes d'accès pour indiquer les trames à éliminer en priorité lors d'une congestion.

Débit binaire Mesure la vitesse de transfert des informations sur un canal, ou les caractéristiques de

transfert d'un équipement. Le débit se mesure en bit/s.

Décibel (dB) Unité logarithmique exprimant le rapport entre deux grandeurs.

Décimal codé binaire (*BCD, Binary Coded Decimal ou DCB)* Représentation binaire des nombres dans laquelle chaque chiffre est codé sur 4 bits. Le codage DCB est utilisé dans la représentation des adresses X.121.

DECT (*Digital European Cordless Telephon*) Norme de radiotéléphonie numérique généralement utilisée pour la réalisation de téléphonie mobile d'entreprise. Le DCET utilise la bande des 1 800 MHz.

Dégroupage Obligation qui est faite à l'opérateur historique (France Télécom) de mettre, moyennant redevance, à disposition des opérateurs alternatifs, une partie du câblage de la boucle locale.

Délai de file d'attente Temps pendant lequel les données doivent attendre avant d'être traitées par le système.

Délai de propagation Délai nécessaire à la circulation des données sur le réseau entre leur source et leur destination finale.

Délimiteur Voir *Fanion.*

Démodulation Opération qui rend à un signal modulé sa forme d'origine. Les modems effectuent des fonctions de démodulation en prenant un signal analogique et en lui rendant sa forme numérique d'origine.

DES (*Data Encryption Standard*) Technique de cryptographie développée par le National Bureau of Standards américain.

Détection d'erreur Voir *Contrôle de parité, CRC, FCS*.

DHCP (*Dynamic Host Configuration Protocol*) Service d'attribution dynamique d'une adresse IP à une station.

Dial-up line Se dit d'une connexion lorsque celle-ci est établie à la demande (connexion temporaire), généralement par l'intermédiaire du réseau téléphonique.

Diaphonie Défaut de transmission provoqué par l'influence d'un canal de transmission sur un autre. Voir *Paradiaphonie*.

DIB (*Directory Information Base*) Désigne l'annuaire distribué dans la norme X.500.

Diffusion (*Broadcast*) Méthode de transmission de messages ou de fichiers à tous les destinataires d'un réseau.

DISC (*DISConnect*) Trame non numérotée d'HDLC, l'un des ETTD prend l'initiative de la rupture de connexion.

Distorsion d'amplitude Déformation du signal résultant du fait qu'un système ne transmet pas identiquement toutes les composantes du signal. Voir *Bande passante*.

Distorsion de phase Problème découlant de la non-uniformité des vitesses de transmission des composants d'un signal sur un support de transmission (vitesse de groupe).

DIT (*Directory Information Tree*) Organisation de la représentation arborescente des données dans la DIB d'X.500.

DIX (*Digital Intel Xerox*) Voir *Ethernet.*

DLCI (*Data Link Connection Identifier*) Étiquette identifiant une connexion dans les réseaux relais de trames (équivalent à la notion de NVL – Numéro de voie logique – dans X.25).

DNS (*Domain Name System*) Nom du système d'annuaire distribué défini dans l'architecture TCP/IP et utilisé dans Internet.

DoD (*Department of Defense*) Ministère de la défense des États-Unis, à l'origine du protocole TCP/IP.

Domaine Entité logique de gestion définie par l'administrateur du réseau qui regroupe un ensemble d'utilisateurs et de serveurs. En architecture Internet, partie d'une arborescence de noms.

Domotique Ensemble de techniques informatiques en relation avec l'habitat privé.

Dorsal Se dit d'un réseau fédérateur, synonyme de *backbone*.

DPAM (*Demand Priority Access Method*) Technique d'accès utilisée dans les réseaux IEEE 802.12. Les stations sont raccordées à un concentrateur intelligent selon une topologie physique identique à celle du réseau 10 base T (réutilisation du câblage existant). Lorsqu'une station a des données à émettre, elle formule une requête au *hub*, qui lui alloue ou non le support.

DQDB (*Distributed Queue Dual Bus*) Protocole de communication, développé par les Télécoms Australia, normalisé par le comité IEEE 802.6 pour les réseaux de type métropolitain. DQDB utilise la notion de cellule

© Dunod – La photocopie non autorisée est un délit

Drapeau Voir *Fanion.*

Driver Ensemble de programmes constituant un tout et destiné à assurer le fonctionnement d'un élément (carte réseau, imprimante...).

DSI (*Digital Speech Interpolation*) Technique utilisée dans les réseaux voix/données pour récupérer, au profit de la donnée, les temps de silence de la voix.

DSP (*Domain Specific Part*) Partie de l'adresse ISO qui contient un identificateur de zone (domaine). Voir *AFI*, *IDI*.

DSR (*Data Set Ready*) Signal à la jonction RS-232-C activé lorsque le DCE (ou ETCD) est prêt à être utilisé.

DTE (*Data Terminal Equipment*) Voir *ETTD*

DTMF (*Dual Tone Multifrequency*) Système de numérotation téléphonique dans lequel chaque chiffre est représenté par deux fréquences, numérotation dite aussi Q.23.

Duplex Mode de transmission permettant de transférer des informations dans les deux sens sur un même canal. Synonyme *bi-directionnel.*

Durée de vie (TTL, *Time To Live*) Champ d'une unité de donnée qui contient un indicateur dit de durée de vie. Initialisé par l'émetteur, ce compteur est décrémenté par chaque nœud traversé. Quand la valeur atteint 0, le bloc de données est détruit. Cette technique évite qu'un bloc de données ne boucle dans un réseau.

E

E&M (*Earth & Mouth*) Signalisation téléphonique RON/TRON (*Earth* pour RON, *Mouth* pour TRON). Voir *RON/TRON.*

E-mail (email) Courrier électronique. Synonyme *courriel*.

EBCDIC (*Extended Binary Coded Decimal Interchange Code*). Code alphanumérique sur 8 bits développé par IBM.

Échantillonnage Technique qui consiste à prélever, à intervalles réguliers, des échantillons d'un signal analogique afin de le convertir en signal numérique.

Écho Signal parasite dû à la réflexion du signal lors d'une désadaptation d'impédance. L'écho engendre des ondes stationnaires, il génère des bits fantômes qui peuvent, dans les réseaux locaux Ethernet, provoquer des collisions.

Écran Feuille métallique entourant une ou plusieurs paires torsadées afin de les protéger des rayonnements électromagnétiques. Voir *Blindage*.

EDI (*Electronic Data Interchange*, traduit en français par *: Échange de données informatisées*). Technique permettant de remplacer, pour les échanges entre entreprises ou organismes, les documents papiers par des documents informatisés.

EFCN (*Explicit Forward Congestion Notification*) Dans un réseau ATM, ce bit est positionné par tout commutateur en état de congestion.

Égal à égal (*Peer to Peer Ressource Sharing*) Se dit d'un réseau local lorsque toutes les stations qui le composent peuvent partager des ressources et exécuter des applications locales.

Égalisation Technique utilisée pour compenser les distorsions des canaux de communication. Synonyme *compensation, correction de distorsion.*

EGP (*Exterior Gateway Protocol*) Protocole internet d'échange d'informations de routage entre systèmes autonomes. ce protocole est documenté dans le RFC 904.

EIR (*Excess Information Rate*) Correspond au trafic maximum autorisé dans un réseau Frame Relay. Toutes les données émises dans l'intervalle CIR (*Constant Bit Rate*) et EIR sont marquées, positionnement du bit DE (*Discard Eligibity*) et éliminées en cas de congestion.

Éliminateur de modem Dispositif de câblage permettant de simuler le dialogue à l'interface entre un modem et le terminal. L'éliminateur de modem permet de s'affranchir de l'utilisation d'un modem lors de transfert sur courte distance. Synonyme *câble croisé*, *null modem.*

Émulateur de modem Dispositif permettant de réaliser une liaison de terminaux ETTD sans modem. Synonyme *null modem.*

Émulation de terminaux Application réseau selon laquelle un ordinateur exploite un logiciel qui le présente à un hôte du réseau comme un terminal passif connecté directement.

En-tête Données jointes à un bloc de données comportant les informations nécessaires au traitement, à l'acheminement ou au contrôle des données transmises. Ces informations de contrôle sont ajoutées avant les données lors de leur encapsulation pour transmission sur le réseau. Synonyme *PCI*. Voir *PCI*.

Encapsulation Technique qui consiste à transporter des unités de données d'un protocole dans une unité de données d'un autre protocole. Synonyme *tunnel*.

Enregistreur Élément d'un commutateur téléphonique qui reçoit et interprète la numérotation téléphonique.

Enveloppe Voir *En-tête.*

Équilibrage de charges Fonction qui permet à un routeur de répartir le trafic sur l'ensemble de ses interfaces qui sont à la même distance de l'adresse de destination. Les algorithmes d'équilibrage de charges les plus efficaces utilisent à la fois des informations de fiabilité et des informations de débit de ligne. L'équilibrage de charges augmente l'utilisation des segments du réseau, et donc sa bande passante disponible.

ERBdB Émetteur-récepteur en bande de base. Équipement qui réalise une adaptation du signal au support (codage en ligne).

Erlang Unité de mesure d'intensité de trafic d'un trafic. Un erlang correspond à l'occupation d'une ligne pendant une heure. La notion d'erlang est essentiellement utilisée en téléphonie où l'on admet qu'un poste téléphonique a un trafic, à l'heure de pointe, de 0,12 erlang.

ERMES (*European Radio MEssaging System*) Projet d'unification des systèmes de radiomessageries unilatérales européens (*pager*).

Erreur d'alignement Dans les réseaux IEEE 802.3, erreur qui se produit lorsque le nombre total de bits d'un paquet reçu n'est pas un nombre entier d'octets. Ce type d'erreur est généralement provoqué par des problèmes de collision.

Erreur de quantification Voir *Bruit de quantification*.

ETCD (*Équipement de terminaison de circuit de données*) Appareil adaptant les signaux émis par un équipement terminal aux caractéristiques de la ligne. Un modem peut être considéré comme un ETCD. Synonyme *DCE* (*Data Circuit Equipment*).

Ethernet Réseau local à bande de base inventé par Xerox et développé conjointement par Xerox, Intel et Digital Equipment Corporation (Ethernet DIX). Les réseaux Ethernet utilisent une méthode d'accès aux média de type CSMA/CD. Ethernet est normalisé par la série de normes IEEE 802-3.

Ethernet jaune Voir *IEEE 802.3 10Base5*.

ETR (*Early Token Release*). Dans la version du réseau Token Ring à 4 Mbit/s, un seul jeton circule en permanence sur le support (système à trame unique). Dans les réseaux en anneau utilisant des débits supérieurs afin d'améliorer l'efficacité, lorsque la station maître a terminé d'émettre son message, elle régénère un jeton (système à trames multiples). De ce fait, plusieurs messages d'origines différentes et un jeton libre peuvent circuler en permanence sur le réseau. Le protocole ETR est utilisé dans les réseaux IEEE 802.5 à 16 Mbit/s et dans le réseau FDDI.

ETTD (*Équipement terminal de traitement de données*) Partie d'une station de données qui peut recevoir et/ou émettre des données, et qui assure la fonction de contrôle des communications de données selon certains protocoles. Le terme ETTD regroupe les ordinateurs, les traducteurs de protocole et les multiplexeurs. Synonyme DTE (*Data Terminal Equipment*).

Eutelsat (*European telecommunication satellite*) Organisation européenne offrant des services internationaux (notamment téléphoniques) de communication par satellite.

Extranet Réseau de communication interne à l'entreprise (Intranet) ouvert à certains éléments extérieurs à l'entreprise.

F

Fac simile Voir *Télécopieur*.

Facilities management (Externalisation) Délégation plus ou moins totale des traitements informatiques et (ou) des télécommunications d'une entreprise à un prestataire de service.

Fading En transmission radio, combinaison d'ondes directes et réfléchies qui module la réception et provoque un effet d'évanouissement.

Faisceau hertzien Système de transmission radio à très haute fréquence se substituant aux systèmes filaires, les faisceaux hertziens permettent de réaliser des liaisons sans coût de génie civil.

Fanion Information précédant et suivant une trame afin de la délimiter. Synonyme *drapeau, délimiteur.*

FCS (*Frame Check Sequence*) Terme faisant référence aux caractères qui sont ajoutés à une trame pour la détection des erreurs. Synonyme *CRC*. Voir *CRC*

© Dunod – La photocopie non autorisée est un délit

FDDI (*Fiber Distributed Data Interface*) Norme définie par l'ANSI et spécifiant un réseau à jeton à 100 Mbit/s utilisant un câble à fibre optique. Pour assurer la redondance de niveau physique, utilise une architecture à double anneau.

FDDI-II Évolution de la norme FDDI proposée par l'ANSI. FDDI garantit une bande passante minimale aux données des différentes stations (classe synchrone) mais ne garantit pas une récurrence temporelle entre les différentes émissions. De ce fait, FDDI-I n'est pas susceptible d'assurer des transferts de données de type isochrone (voix, vidéo). FDDI-II superpose sur un même support, l'anneau FDDI, une voie asynchrone et synchrone (fonctionnement en mode paquet) et une voie isochrone (fonctionnement en mode circuit).

FDM (*Frequency Division Multiplexing*) Voir *Multiplexage en fréquence.*

FECN (*Forward Explicit Congestion Notification*) Les réseaux à relais de trames ne gèrent pas la congestion. Le contrôle de celle-ci est reporté aux organes d'extrémité. Lorsque le réseau est en état de congestion, il élimine purement et simplement les trames en excès et positionne un bit pour informer les organes d'extrémité de cet état. Les bits *FECN* (notification de congestion en aval) et *BECN* (*Backward Explicit Congestion Notification,* notification de congestion en amont) sont utilisés pour signaler aux organes d'extrémité l'état de congestion du réseau.

Fédérateur Voir *Réseau dorsal.*

Fenêtre d'anticipation Technique de transmission dans laquelle les blocs de données sont émis sans attendre un accusé de réception. Le nombre de blocs pouvant être envoyés sans acquittement est désigné par fenêtre d'anticipation.

Fenêtre d'émission Voir *Fenêtre d'anticipation*.

Fenêtre de réception Nombre de blocs de données pouvant être reçus et éventuellement réordonnés par un système récepteur. Voir *Rejet sélectif*, *Rejet simple*.

Fibre monomode Fibre optique de diamètre relativement faible dans laquelle ne se propage qu'un seul faisceau de rayon lumineux. Ce type de fibre a une bande passante plus élevée que la fibre multimode, mais demande une source lumineuse ayant une plus faible largeur de spectre, par exemple LASER.

Fibre multimode Fibre optique dans laquelle la propagation des informations s'effectue selon plusieurs chemins (modes).

Fibre optique Support de verre transportant les informations binaires en modulant un faisceau lumineux. La fibre optique autorise des débits élevés et permet de couvrir des distances importantes.

FIFO (*First In, First Out*) Mode de gestion des files d'attente selon lequel le premier message arrivé est le premier transmis.

File d'attente Généralement, liste ordonnée d'éléments en attente de traitement. En routage, ensemble de paquets attendant d'être transmis sur une interface de routeur.

Firewall Voir *Pare-feu.*

Flow control Voir *Contrôle de flux*.

FM (*Frequency Modulation*) Voir *Modulation de fréquence*.

Fondamental Composante sinusoïdale de même fréquence que le signal périodique d'origine. Voir *Théorème de Fourier*.

Forwarding Voir *Acheminement.*

Frame Interval (IFG, *Inter Frame Gap*) Intervalle de temps minimal entre deux trames sur un réseau IEEE 802.3. Une station avant d'émettre doit détecter un silence d'au moins 9,6 μs (réseau à 10 Mbit/s). Ce temps minimal entre deux messages permet : d'une part, à l'électronique de bien discerner deux messages et, d'autre part, l'absorption d'éventuelles réflexions pour éviter la détection de collisions fantômes.

Frame Relay Voir *Relais de trames.*

Frame Relay Forum Consortium de constructeurs, d'opérateurs, de consultants et d'utilisateurs chargés de la définition et de la promotion des techniques et solutions basées sur le Frame Relay. Voir *Relais de Trames*.

Freeware Logiciels gratuits.

Fréquence Nombre de cycles d'un signal transmis pendant une unité de temps donnée. La fréquence se mesure en Hertz (Hz) ou cycles par seconde.

Fréquence vocale Désigne généralement la bande de fréquences nécessaire à la transmission de la voix analogique (300 à 3 400 Hz).

FSK (*Frequency Shift Keying*) Voir *Modulation de fréquence*.

FTP (*File Transfer Protocol*) Protocole de manipulation de fichiers l'environnement TCP/IP. FTP permet la création, la suppression et le transfert de fichiers.

FTP (*Folied Twister Pair*) Câble à paires torsadées écranté.

Full duplex Mode de fonctionnement d'une ligne ou d'un équipement dans lequel les informations sont transmises simultanément dans les deux sens. Synonyme *bi-directionnel simultané.*

G

Gateway Voir *Passerelle*.

GFI (*General Format Identifier* ou *IGF*, *Identificateur général de format*) Champ d'un paquet X.25 qui permet de définir certains paramètres de l'échange.

GIF (*Graphic Interchange Format)* Mode de compression d'images numérisées en 256 couleurs.

Gigue (*jitter*) Variation du temps de transmission d'un signal.

GPRS (*General Packet Radio Services*) Norme de transmission de données en mode paquet s'appuyant sur un réseau GSM.

GPS (*Global Positioning System*) Système militaire de localisation par satellite (États-Unis).

Grappe Ensemble de terminaux passifs raccordés derrière un concentrateur.

GSM (*Global System for Mobile* communication, adaptation anglo-saxonne de Groupe Spécial Mobile) Norme de radiocommunication numérique avec les mobiles. France Télécom (Orange) et SFR utilisent cette norme.

H

H.323 Norme UIT pour le transfert de flux multimédia sur réseau sans garantie de service (mode datagramme), utilisé dans la voix sur IP.

Hachage Technique de cryptographie garantissant l'intégrité des données.

Half duplex Mode de communication dans lequel les données ne circulent que dans un sens à la fois. Synonymes *alternat et semi-duplex.*

Hand Over ou **Hand Off** Fonction d'un système de radiocommunication qui permet à une station de se déplacer sans interruption de la communication.

Harmonique Composante sinusoïdale d'un signal périodique non sinusoïdal. Voir *Théorème de Fourier*.

HDBn Haute densité binaire d'ordre *n* Codage de type bipolaire dans lequel on introduit des bits fictifs (bit de viol et bit de bourrage) pour éviter une suite de plus de *n* bits consécutifs à zéro.

HDLC (*High Level Data Link Control*) Protocole ISO standard de liaison de données orienté bit, dérivé de SDLC. Spécifie une méthode d'encapsulation sur des liaisons de données séries synchrones.

Header Voir *En-tête*.

HEC (*Header Error Control*) Octet de contrôle d'erreur sur l'en-tête d'une cellule ATM. Le calcul du HEC utilise les techniques du CRC. L'HEC sert aussi au cadrage des cellules ATM.

Hertz Mesure de fréquence ou de largeur de bande. Synonyme *cycles par seconde.* Abréviation : *Hz.*

Hertzien Voir *Faisceau hertzien*.

HIPPI (*High-Performance Parallel Interface*) Interface à hautes performances définie par la norme ANSI X3T9.3/88-023.

HM (*Huffman Modified*) Codage de Huffman utilisé dans les télécopieurs. Dans ce code, le codage des suites de points blancs ou noirs est pré-établi. Voir *Huffman*.

Horloge Élément d'un système de transmission qui détermine la cadence d'émission des symboles. Le rythme de l'horloge s'exprime en Hz.

HTML (*HyperText Markup Language*) Langage de description des pages de documents hypertextes mis à disposition sur les serveurs Web.

HTTP (*HyperText Transfer Protocol*) Standard de protocole de transmission de données représentées en HTML (documents hypertextes).

Hub Généralement équipement qui sert de centre à un réseau à topologie physique en étoile. En terminologie IEEE 802.3, un *hub* est un répéteur multiport Ethernet, qui est parfois appelé concentrateur. Le terme est également utilisé pour faire référence à une unité matérielle/logicielle contenant plusieurs modules (indépendants mais reliés les uns aux autres) de matériels de réseaux et d'interconnexion de réseaux.

Huffman (codage) Méthode de compression basée sur les occurrences d'apparition d'un symbole, d'une combinaison binaire ou autre. Le symbole

© Dunod – La photocopie non autorisée est un délit

le plus fréquemment employé sera codé avec un nombre minimum de bits. Le code de Huffman est utilisé dans la télécopie. Voir *HM*.

I

ICMP (*Internet Control Message Protocol*) Protocole internet qui fournit des messages d'erreur et d'autres informations concernant le traitement des paquets IP. Documenté dans le RFC 792.

IDI (*Initial Domain Identifier*) Élément de l'adresse réseau de l'ISO, IDI identifie le domaine dans lequel s'applique l'adresse. C'est par exemple le code pays de X.121. Voir *AFI*, *DSP*.

IDP (*Initial Domain Part*) Partie d'une adresse SNPA (*SubNetwork Point of Attachement*) qui définit l'autorité de gestion de l'espace d'adressage.

IEEE (*Institute of Electrical and Electronic Engineers*) Organisation professionnelle américaine qui définit, entre autres, des normes réseau. Ses normes LAN sont actuellement les plus suivies et comprennent notamment des protocoles similaires ou pratiquement équivalant aux protocoles Ethernet et Token Ring.

IEEE 802.2 Protocole IEEE qui spécifie une implémentation de la sous-couche Contrôle de liaison logique de la couche Liaison de données (couche LLC). Ce protocole gère les erreurs, le format des données, le contrôle de flux et l'interface de service de couche 3, il est utilisé dans les normes de réseaux locaux (LAN) comme IEEE 802.3 et IEEE 802.5.

IEEE 802.3 Protocole IEEE qui spécifie une implémentation de la couche Physique et de la sous-couche MAC de la couche liaison de données, Ce protocole utilise l'accès CSMA/CD à différents débits sur différents supports physiques.

IEEE 802.3 10Base5 Norme IEEE 802.3 Ethernet. Transmission en bande de base utilisant comme support un câble coaxial épais. Débit de 10 Mbit/s et longueur maximale d'un segment limitée à 500 m.

IEEE 802.3 10Base2 Norme IEEE 802.3 Ethernet utilisant pour support un câble coaxial fin. Longueur maximale d'un segment limitée à 185 mètres. Débit de 10 Mbit/s.

IEEE 802.3 1Base5 Première version du réseau Ethernet sur paires torsadées. Le débit était limité à 1 Mbit/s. Synonyme *StarLAN*.

IEEE 802.3 10BaseT Norme IEEE 802.3 qui utilise un câblage à paires torsadées non blindées et à un débit de 10 Mbit/s. Évolution du réseau StarLAN.

IEEE 802.4 Protocole IEEE qui spécifie une implémentation de la couche physique et de la sous-couche MAC de la couche liaison de données. Ce protocole utilise la technique de passage de jeton sur une topologie en bus.

IEEE 802.5 Protocole IEEE qui spécifie une implémentation de la couche physique et de la sous-couche MAC de la couche Liaison de données. Ce protocole utilise la technique de passage de jeton à 4 ou 16 Mbit/s sur un câblage à paires torsadées blindées et est très semblable au Token Ring IBM.

IEEE 802.6 Spécification MAN (réseau métropolitain) IEEE basée sur la technologie DQDB. Ce protocole supporte des vitesses de transmission comprises entre 1,5 et 155 Mbit/s.

IEEE 802.12 (*100 VG AnyLAN*) VG Lan est un réseau local à 100 Mbit/s compatible, au niveau des formats de trames, avec Ethernet ou Token Ring (selon configuration), il implémente un nouveau protocole d'accès fondé sur la méthode du *polling*. Le terme *AnyLAN* provient de sa double compatibilité, se contentant de simples paires torsadées de qualité vocale (*VG*, *Voice Grade*), le 100 VG AnyLAN offre un débit de 100 Mbit/s et un accès déterministe.

IFG (*Inter Frame Gap*) Temps de silence entre deux trames Ethernet. Voir *Frame Interval*.

IGP (*Interior Gateway Protocol*) Protocole Internet utilisé pour échanger des informations de routage au sein d'un système autonome. Ex. : IGRP, RIP et OSPF.

IGRP (*Interior Gateway Routing Protocol*) Protocole IGP développé par Cisco Systems pour résoudre les problèmes associés au routage dans de gros réseaux hétérogènes.

Impédance Caractéristique électrique d'un système dépendant directement de sa résistance, de sa capacitance, de son inductance et de la fréquence. L'impédance s'exprime en ohms (Ω).

Impédance caractéristique (*Zc*) L'impédance caractéristique est l'impédance d'une ligne de longueur infinie. On montre que lorsqu'une ligne de longueur finie est refermée sur un récepteur, dont l'impédance *Zr* est égale à l'impédance caractéristique de la ligne, celle-ci se comporte comme une ligne de longueur infinie, on dit alors que la

ligne est adaptée. Voir *Adaptateur d'impédance, Balun.*

Infrarouge Bande d'ondes électromagnétiques dont la plage de fréquences se situe au-dessus de celle des micro-ondes, mais en dessous du spectre visible, et utilisée pour la transmission d'informations sans fil sur de très courtes distances.

Interface Connexion entre deux équipements ou systèmes. En télécommunications, connexion à un réseau. Également, frontière entre des couches adjacentes du modèle OSI. En téléphonie, frontière définie par une communauté des caractéristiques de signaux, de caractéristiques d'interconnexion physique, et de contenu des signaux échangés.

Interférences Parasites perturbant les signaux circulant sur des canaux de communication.

Intermodulation Interférence entre deux signaux l'un modulant l'autre et vice versa. Pour éviter l'intermodulation, les spectres de fréquences des deux signaux doivent être suffisamment espacés (*bande de garde*).

International Standards Organization Voir *ISO.*

Internetworking Interconnexion de réseaux.

Interopérabilité Possibilité, pour des équipements de différents constructeurs, de communiquer entre eux.

Intranet Réseau d'entreprise mettant en œuvre les mêmes technologies que le réseau Internet.

Invitation à émettre (*polling*) Dans une relation maître/esclave, l'invitation à émettre est envoyée par la station maître à la station esclave pour l'inviter à envoyer ses informations. Cette solution évite les problèmes de conflits entre machines.

Invitation à recevoir (*selecting*) Dans une relation maître/esclave, l'invitation à recevoir est envoyée par la station maître à la station esclave pour lui indiquer qu'elle a un message à lui envoyer.

IP (*Internet Protocol*) Protocole de couche 3 (couche réseau) contenant des informations d'adressage et certaines informations de contrôle permettant le routage des paquets. Documenté dans le RFC 791. Synonyme *protocole inter-réseau.*

IPNS (*ISDN PABX Networking Specification*) Système de signalisation entre PABX hétérogènes développé par Alcatel et Siemens et à l'origine de la norme Q-SIG.

IRC (*Internet Relay Chat*) Voir *Chat.*

Iridium Système de téléphonie par satellites comprenant 66 satellites développé par Motorola. Fermé trois mois après sa mise en service pour faute de client, Iridium a été racheté par Boeing, le principal client est l'US-Army.

ISDN (*Integrated Services Digital Network*) Voir *RNIS.*

ISO (*Interconnexion de systèmes ouverts*) Traduction française de OSI, ne devrait jamais être utilisée, car il y a alors confusion entre le modèle (OSI en anglais et ISO en français) et l'organisme (ISO en anglais et OSI en français). Voir *OSI.*

ISO (*International Standard Organization*) Organisme international chargé de la mise au point d'une vaste gamme de normes, dont celles concernant les réseaux. L'ISO a mis au point le modèle de référence le plus connu, appelé *modèle OSI.*

Isochrone Signaux ou réseaux utilisant une référence temporelle unique.

IS-IS Algorithme de routage IGP (*Interior Gateway Protocol*) hiérarchique à état des liaisons de l'OSI. Voir *Algorithme de routage à état des liaisons*.

IT (*Intervalle de temps*) Dans le multiplexage temporel, l'IT correspond au temps attribué à chaque source pour émettre ses données.

J

Jabber Condition d'erreur qui survient lorsqu'une unité du réseau transmet continuellement des informations parasites. En protocole IEEE 802.3, paquet de données dont la longueur dépasse celle autorisée par la norme (1 518 octets).

Jarretière Câble souple utilisé dans les panneaux de brassage (répartiteurs) pour relier un abonné à un service (téléphonique, commutateur ou *hub* Ethernet...).

Jeton Trame d'informations de contrôle dont la possession donne à une station du réseau le droit d'émettre.

Jeton adressé Technique du jeton utilisé dans les réseaux IEEE 802.4. Dans ces réseaux le jeton contient l'adresse de la station à laquelle le droit de parole est attribué. Le jeton circule de la station de plus faible adresse à celle de plus forte adresse, formant ainsi un anneau virtuel sur le bus (anneau logique/bus physique).

© Dunod – La photocopie non autorisée est un délit

Jeton non adressé Technique de distribution du droit à parole utilisée dans les réseaux IEEE 802.5. Dans un tel système, les informations (trames) transitent par toutes les stations actives. Le droit à parole est matérialisé par une trame particulière « *le jeton ou token* ». Celui-ci circule en permanence de station en station. Une station qui reçoit le jeton peut émettre une ou plusieurs trames (station maître). Si elle n'a rien à émettre, elle se contente de répéter le jeton (station répéteur).

Jitter Voir *Gigue.*

Joncteur Élément de raccordement d'une ligne ou d'un circuit à un organe de traitement.

JPEG (*Joint Photographic Experts Group*) Norme de compression très performant d'images fixes numérisées en 16,7 millions de couleurs (12 bits par pixel).

K

Kerberos Protocole d'authentification d'un utilisateur développé par le MIT (Massachussetts Institute of Technology).

Kermit Protocole de transfert de fichiers en mode asynchrone et d'émulation de terminaux. Développé par l'université de Colombia, Kermit est du domaine public.

L

LAN (*Local Area Network*) Voir *Réseau local.*

LAN émulation Technique qui permet la réalisation d'un réseau local virtuel sur une infrastructure à base d'ATM. Cette technique masque aux couches supérieures l'emploi d'un réseau ATM en lieu et place d'un LAN traditionnel (*legacy LAN*).

LAP-B (*Link Access Protocol, Balanced)* Procédure dérivée de HDLC, version UIT X.25 d'un protocole de liaison de données orienté bit.

LAP-D (*Link Access Protocol D*) Protocole de couche Liaison de données RNIS pour canal D. Ce protocole est dérivé du protocole LAP-B UIT X.25 et conçu essentiellement pour résoudre les problèmes de signalisation de l'accès de base RNIS. Défini par les avis UIT Q.920 et Q.921.

Large bande Par opposition aux transmissions en bande de base, technologie de transmission qui effectue une translation du spectre du signal (modulation).

Largeur de bande Espace de fréquence occupé par un signal (fondamental et harmoniques). Synonyme *spectre de fréquence*.

Larsen Du nom de son découvreur, l'effet Larsen correspond au couplage entre un microphone et un système amplificateur qui provoque une boucle de réaction positive et fait entrer le système en oscillation. l'effet Larsen se manifeste par un sifflement aigu.

LASER (*Light Amplification by Stimulated Emission of Radiation*) Équipement de transmission dans lequel un matériau actif est excité par un stimulant externe pour produire un faisceau étroit de lumière cohérente qui peut être modulé en impulsions pour transporter des données.

LCR (*Least Cost Routing*) Logiciel embarqué dans les PABX et destiné à choisir l'opérateur de moindre coût pour établir une communication téléphonique.

LDAP (*Lightweight Directory Access Protocol*) Protocole fédérateur d'accès aux services d'annuaire.

LED (*Light Emitting Diode*) Composant électronique qui sous l'effet d'un courant émet une radiation lumineuse.

Lempel Ziv Voir *Algorithme du Lempel Ziv.*

LIA (*Liaison inter-automatique*) Liaison établie entre deux autocommutateurs téléphoniques pour acheminer des communications téléphoniques.

Liaison Canal de communication de réseaux composé d'un circuit ou d'une voie de transmission, et comprenant tous les équipements entre l'émetteur et le récepteur. Terme souvent utilisé pour faire référence à une connexion WAN. Parfois appelée *ligne.*

Liaison analogique et liaison numérique Désigne un type de liaison. Une liaison est dite analogique lorsque l'interface usager est du type analogique (modem), elle est dite numérique quand l'interface usager est numérique (CODEC ou ERBdB).

Liaison d'abonné Liaison dédiée qui relie un abonné d'un réseau à un point d'accès de ce réseau.

Liaison de données (*data link*) Liaison affectée à une transmission numérique. Cette expression désigne surtout la couche 2 du modèle OSI de l'ISO.

Ligne commutée Circuit de communication établi par une connexion *via* un réseau à commutation de circuits utilisant l'infrastructure du réseau téléphonique.

Ligne multipoint Ligne de communication reliant physiquement plusieurs équipements.

Link status (*état de la ligne*) Signal particulier utilisé dans les réseaux 802.3 10 base T pour contrôler la continuité du lien entre le *hub* et la station.

Liste d'accès Liste tenue à jour par les routeurs afin de contrôler l'accès à un certain nombre de services (par exemple pour empêcher les paquets ayant une certaine adresse IP de sortir sur une interface particulière du routeur).

Little-endian Méthode de stockage ou de transmission des données dans laquelle le bit ou l'octet le moins significatif est présenté en premier. Voir aussi *Bigendian.*

LLC (*Logical Link Control*) Voir *Contrôle de liaison logique.*

Loi-A Norme CCITT (UIT-T) de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage. Cette norme est surtout utilisée dans les réseaux téléphoniques européens. La loi-A est incompatible avec la loi-mu en vigueur en Amérique du Nord et au Japon.

Loi-mu Norme nord-américaine de compression-extension utilisée lors de la conversion de signaux analogiques/numériques sur les systèmes à modulation par impulsion et codage.

Longueur d'IT Exprime en bits le nombre de bits transportés durant un intervalle de temps dans un système de multiplexage temporel.

Longueur de mot La longueur de mot exprime le nombre de bits qui code un symbole. Par exemple le code ASCII utilise des mots dont la longueur est de 7 bits.

Luminance En télévision couleur, le signal de luminance représente l'image monochrome ou échelle des gris. Voir *Chrominance*.

M

MAC (*Medium Access Control*) Dans les réseaux locaux, sous-couche de niveau liaison gérant l'accès au support. Voir *Contrôle d'accès au support.*

Mail Box Voir *BAL*

Maillage Définit la connectivité d'un nœud du réseau, le nœud pouvant être atteint par différents liens.

MAN (*Metropolitan Area Network*) Réseau de transmission couvrant généralement une ville et ses environs. Autorise l'interconnexion de plusieurs réseaux locaux.

Manchester Voir *Codage biphase*.

MAQ (*Modulation en amplitude et à porteuse en quadrature*) Technique de modulation qui combine la modulation d'amplitude et de phase.

Masque de sous-réseau Champ de bits qui permet d'étendre l'adresse réseau d'IP. Ce champ est utilisé pour spécifier des sous-réseaux du réseau principal.

MAU 1) *Medium Attachment Unit* Équipement de raccordement dans un réseau Ethernet. Synonyme *transceiver*. **2)** *Multiple Access Unit Hub* dans les réseaux 802.5 (Token Ring).

Média Supports physiques véhiculant les signaux de transmission : paires torsadées, câbles à fibres optiques, câbles coaxiaux et atmosphère (qui sert de support de transmission aux micro-ondes, aux rayons laser et aux transmissions infrarouges).

Mémoire-tampon (*buffer*) Zone de mémoire utilisée pour la gestion des données en transit. Les mémoires-tampons sont souvent utilisées pour compenser les différences de vitesse de traitement entre les stations du réseau. Les données transmises par rafales peuvent être stockées dans une mémoire-tampon jusqu'à ce qu'elles puissent être prises en compte par les périphériques moins rapides.

Messagerie électronique Technique permettant aux utilisateurs d'échanger des messages sur un certain nombre de types de réseau en utilisant des protocoles variés. Synonyme *courrier électronique.*

Méthode d'accès Algorithme de partage du support physique dans un réseau local. Voir *MAC*.

Métrique de routage Valeur qui permet à un algorithme de routage de déterminer qu'une route est meilleure qu'une autre. Ces informations sont stockées dans des tables de routage. Les métriques peuvent être exprimées en fonction du taux d'erreur de la liaison, du délai de transmission, de la bande passante, de la charge, du MTU, du nombre de sauts.

© Dunod – La photocopie non autorisée est un délit

Metropolitan Area Network Voir *MAN*.

MF (*Modulation de fréquence*) Voir *Modulation de fréquence*.

MHS (*Message Handling System*, ISO 10021, CCITT) Implémente un service de messagerie en mode non connecté ; en cas d'absence du destinataire, le message est délivré dans sa boîte aux lettres.

MIB (*Management Information Base*) Base de données d'information d'administration des réseaux.

MIC (*Modulation par impulsions et codage*). Technique de transmission des informations analogiques sous forme numérique par échantillonnage et codage des échantillons d'aide d'un nombre fixe de bits. Synonyme *PCM*, *Pulse Code Modulation*.

MICDA (*MIC différentielle adaptable*) Processus tirant profit de la forte corrélation statistique entre des échantillons de voix consécutifs afin de créer une échelle de quantification variable. La MICDA encode des échantillons de voix analogiques en signaux numériques de haute qualité.

Micro-ondes Ondes électromagnétiques de fréquences comprises entre 1 et 30 Ghz. Les réseaux exploitant ce type d'ondes reposent sur une technologie récente, mais de plus en plus employée en raison de son faible coût et de sa bande passante importante.

Microprogramme Instructions logicielles enregistrées de manière permanente ou semi-permanente en mémoire morte (ROM). Synonyme *firmware.*

Middleware Ensemble de logiciels situé entre le système d'exploitation et les programmes d'application.

MIME (*Multipurpose Internet Mail Extension*) Logiciel de diffusion de messages électroniques au format binaire. Permet l'encapsulation de différents formats de données dans un même message.

Minitel Terminal asynchrone défini pour l'accès au vidéotexte.

MNP (*Microcom Network Protocol*) Série de protocoles intégrés aux modems proposée par la société Microcom ayant pour objectif d'améliorer la transmission sur une liaison de données. Les plus connus sont MNP4, détection d'erreur, et MNP5, compression de données qui ont été repris par les instances de normalisation.

Mode non connecté (*CNLS*, *ConnectionLess Network Service*) Mode dans lequel les transferts de données sont effectués à la demande. Chaque bloc de données est transféré indépendamment, il n'y a aucune garantie de délivrance (mode pour le mieux ou *best effort*). Ce mode est généralement appelé mode datagramme.

Mode orienté connexion (*CONS*, *Connection-Oriented Network Service*) Mode dans lequel les transferts de données demandent l'établissement préalable d'un circuit virtuel (CV). Le mode orienté connexion est généralement désigné plus simplement par mode connecté.

Modèle OSI (*Open System Interconnection*) Modèle architectural de réseaux développé par l'ISO et le CCITT. Le modèle se compose de sept couches, dont chacune spécifie des fonctions réseau particulières comme l'adressage, le contrôle du flux, la gestion des erreurs, l'encapsulation et la fiabilité du transfert des messages. La couche la plus haute (la couche application) est la plus proche de l'utilisateur, et la couche la plus basse (la couche physique) la plus proche de la technologie des supports. Le modèle OSI est universellement utilisé pour apprendre et comprendre les fonctionnalités des réseaux.

MODEM (Modulateur-démodulateur). Boîtier qui convertit les signaux numériques en vue de leur transmission sur des installations de communication analogique, et *vice versa*.

Modulation Technique par laquelle un signal à transmettre modifie un paramètre d'un autre signal, appelé porteuse. Voir *Modulation d'amplitude, Modulation de fréquence, Modulation de phase*.

Modulation d'amplitude (*ASK, Amplitude Shift Keying*) Technique de modulation dans laquelle le signal à transmettre n'est pas transmis directement. Ce signal est utilisé pour modifier l'amplitude d'un autre, généralement sinusoïdal, appelé porteuse.

Modulation de fréquence (*FSK, Frequency Shift Keying*) Technique de modulation dans laquelle le signal modulant modifie la fréquence du signal porteur. Du fait de la grande largeur de bande du signal modulé, la modulation de fréquence n'est utilisée que dans les modems à faible débit.

Modulation de phase (*PSK, Phase Shift Keying*) Technique de modulation dans laquelle le signal modulant modifie la phase du signal porteur. Généralement, les modems utilisent une combinaison de la modulation d'amplitude et de phase appelée MAQ (Modulation en amplitude et quadrature).

Modulation par impulsions codées Voir *MIC*.

MP3 Norme de compression du son.

MPEG (*Move Picture Experts Group*) Format de compression vidéo utilisé dans la télévision numérique.

MRT (*Multiplexage à répartition temporelle*) Voir *MuItiplexage temporel.*

MRT Asynchrone (*Multiplexage à répartition temporelle asynchrone*) Voir *ATDM.*

MTA (*Message Transfer Agent*) En messagerie, entité (logiciel) qui assure la circulation des messages entre agents utilisateurs.

MTBF (*Mean Time Between Failure*) Temps moyen de bon fonctionnement d'un équipement.

MTS (*Message Transfer System*) En messagerie, ensemble des MTA appartenant à un même domaine.

MTTR (*Mean Time To Repair*) Temps moyen de remise en état d'un équipement.

MTU (*Maximum Transfer Unit*) Taille maximale des paquets, exprimée en octets, qu'un réseau peut transmettre.

Multicast Voir *Adresse de groupe.*

Multimédia Flux d'information qui associe le texte, le son, l'image et la vidéo.

Multiplexage Technique permettant de faire passer plusieurs communications sur un même canal de transmission.

Multiplexage à répartition temporelle asynchrone Voir *ATDM*.

Multiplexage de position Technique dans laquelle les différents blocs de données sont identifiés par leur position dans une trame. Le multiplexage temporel est une technique de multiplexage de position.

Multiplexage en fréquence Technique qui consiste à découper la bande passante d'un canal en plusieurs sous-bandes, chacune étant affectée à une voie. Le multiplexage en fréquence correspond à une juxtaposition fréquentielle de voies et à une superposition des signaux dans le temps.

Multiplexage par étiquette Technique dans laquelle les blocs de données ne sont pas identifiés par leur position dans une trame mais par un identificateur appelé étiquette. Cette étiquette peut, par exemple, être le numéro de voie logique utilisé dans X.25 pour identifier les paquets sur une liaison.

Multiplexage spatial Voir *Multiplexage en fréquence*.

Multiplexage temporel Technique permettant d'affecter à des informations provenant de différents canaux une largeur de bande sur un support unique, selon un système d'affectation de tranches de temps (IT, Intervalle de temps). Le multiplexage temporel correspond à une juxtaposition des voies dans le temps et à l'utilisation d'un même espace fréquentiel.

Multiplexeur statistique (*STDM, Statistical Time Division Multiplexing*) Équipement de multiplexage qui affecte de manière dynamique la capacité d'une ligne uniquement aux canaux d'entrée actifs, et permet de connecter davantage de stations qu'un multiplexeur traditionnel. Également appelé *multiplexeur statistique temporel.*

N

NACK (*Negative Acknoledge*) Acquittement négatif. Voir *ACK*.

Named pipes (*pipe nommé*) Canal virtuel de communication permettant une communication directe entre deux applications.

Navigateur Voir *Browser*.

NDI (*Numéro de désignation de l'installation*) Partie de la numérotation téléphonique qui identifie l'installation privée.

NDIS (*Network Driver Interface Specification*) Spécification Microsoft et 3-COM d'un logiciel permettant de piloter une carte d'interface réseau en s'affranchissant du protocole et des matériels utilisés. NDIS autorise l'utilisation simultanée de plusieurs protocoles réseaux sur le même adaptateur physique. Voir *ODI*.

NDS (*Numéro de désignation supplémentaire*) Partie de la numérotation téléphonique qui désigne l'abonné.

NetBEUI (*Network Bios Extended User Interface*) Interface de transport de la couche NetBIOS.

NetBIOS (*Network Basic Input/Output System*) Interface de couche Session pour réseaux de type IBM PC et Microsoft.

Newsgoups (*UseNet newsgroups*) Forum de discussion thématique sur Internet.

© Dunod – La photocopie non autorisée est un délit

NFS (*Network File System*) Ensemble de protocoles développés par Sun Microsystem pour permettre l'accès partagé des fichiers sur un réseau. Parmi les suites « NFS figurent notamment NFS, XDR (*External Data Representation*) et RPC (*Remote Procedure Call*) qui font partie d'une architecture plus importante que Sun appelle *ONC* (*Open Network Computing*).

NIC (*Network Interface Controller ou Network Interface Card*). Voir *Adaptateur.*

NLPID (*Network Level Protocol Identifier*) Élément d'information de l'encapsulation défini par la RFC 1490 qui identifie le protocole transporté.

NNI (*Network Node Interface*) Interface standard entre des commutateurs ATM. Également *Network-to-Network Interface* en relayage de trames.

Nœud Terme générique utilisé pour faire référence à une entité pouvant accéder à un réseau. Synonyme *station.* Système constituant un carrefour de lignes de communications dans un réseau : serveur, concentrateur, frontal.

Non-répudiation Mécanisme d'authentification dans lequel l'auteur d'un message ne peut nier l'avoir émis ou le destinataire l'avoir reçu.

Norme Ensemble de règles ou de procédures consacrées par la pratique ou la décision d'un organisme officiel.

NSAP (*Network Service Access Point*) Adresses réseau ISO, spécifiées par la norme ISO 8348/Ad. Point auquel les services réseaux OSI sont mis à la disposition d'une entité de transport.

Null modem Voir *Éliminateur de modem.*

Numeris Nom commercial du réseau numérique à intégration de services commercialisé par France Télécom. Voir *RNIS*.

Numérotation Système de signalisation des adresses d'abonné (numéro d'abonné) dans un réseau téléphonique (plan de numérotation). Il existe deux types de numérotation : la numérotation décimale et la numérotation à fréquence vocale. Le plan de numérotation international est défini par la norme E.164.

Numérotation à fréquence vocale Voir *Numérotation fréquentielle*.

Numérotation décimale ou analogique (33/66) Numérotation téléphonique des postes téléphoniques à cadran. La numérotation est réalisée par ouverture de la liaison d'abonné. Les numéros sont envoyés au commutateur de rattachement sous forme d'impulsions de 66 ms suivi d'un repos de 33 ms, d'où le nom de système 33/66. Il est envoyé une impulsion pour le 1, deux pour le 2, etc.

Numérotation fréquentielle ou vocale (multifréquentielle) Numérotation téléphonique normalisée (Q.23). Ce type de numéro est composé à partir du clavier à touche de téléphone. L'enfoncement d'une touche correspond à l'envoi de deux fréquences (la haute suivie de la basse) au central de rattachement (**DTMF**, *Dual-Tone MultiFrequency*). Les postes peuvent comporter 12 ou 16 touches. Certains postes téléphoniques fréquentiels ont la possibilité d'émettre une numérotation décimale. Transmise en transparence durant une conversation, la numérotation à fréquence vocale autorise un dialogue homme machine.

Numérotation numérique ou binaire Numérotation téléphonique des postes téléphoniques numériques. Ces postes émettent directement un signal binaire sur une voie dite de signalisation. La numérotation peut être propriétaire (poste numérique propriétaire) ou normalisée (RNIS).

NVL (*Numéro de voie logique*) Étiquette d'identification d'une communication dans les réseaux X.25. Le NVL n'a qu'une valeur locale (entre deux nœuds adjacents du réseau).

Nyquist (Critère) Voir *Critère de Nyquist*.

O

Objet géré En gestion de réseau, station qui peut être gérée par un protocole de gestion de réseau.

OCR (*Optical Character Recognition*) Système de reconnaissance optique de caractères convertissant un document imprimé en un document texte.

Octet Terme générique utilisé pour faire référence à une série de 8 bits consécutifs traités comme un tout. Synonyme *byte*.

ODI (*Open Data-link Interface*) Spécification Novell d'un progiciel pour cartes d'interface réseau. Voir *NDIS*.

ODIF (*Office Document Interchange Format*) Format d'échange de documents dans le cadre de la norme ODA.

OEM (*Original Equipment Manufacturer*) Constructeur ou distributeur qui revend un matériel ou un logiciel sous sa propre marque.

Opérateur de télécommunications Organisation publique ou privée offrant des services de télécommunication.

OSI (*Open System Interconnection*) Voir *Modèle OSI*.

OSPF (*Open Shortest Path First*) Algorithme de routage IGP (*Interior Gateway Protocol*) hiérarchique à état des liaisons successeur de RIP dans le monde Internet. Ces fonctionnalités comprennent le routage à moindre coût, le routage multivoie et l'équilibrage des charges. L'OSPF est dérivé d'une ancienne version du protocole IS-IS de l'OSI. Voir *Algorithme de routage à état des liaisons*.

OUI (*Organization Unit Identifier*) Premier champ de l'adresse MAC IEEE. OUI identifie le manufacturier de l'interface réseau.

Outsourcing Voir *Facilities Management*.

P

PABX (*Private Automatic Branch eXchange*) Voir *Autocommutateur privé.*

Packet Voir *Paquet*.

Packets switching Voir *Commutation de paquets.*

PAD (*Packet Assembler-Disassembler*) A pour objectif essentiel d'encapsuler les données issues du terminal asynchrone (ETTD-C) dans un paquet X.25 et de décapsuler les données à destination de ce terminal. Afin d'éviter que sur le réseau ne circule un paquet pour chaque caractère, le PAD assemble ces caractères en paquets, l'avis X.3 précise les modalités essentielles de cette fonction.

Paire torsadée Support de transmission composé de deux fils isolés disposés selon une configuration en spirales régulières. Les fils peuvent être blindés ou non blindés. La paire torsadée est très courante dans les applications téléphoniques, et de plus en plus utilisée dans les réseaux locaux.

PAM (*Pulse Amplitude Modulation*) Dans ce mode de modulation, l'amplitude d'une impulsion de durée constante est modulée en fonction de l'amplitude d'un signal analogique. Voir *Modulation d'amplitude*.

PAN (*Personnal Area Network*) Système de transmission de données à usage personnel. Voir *Bluetooth*.

PAP (*Password Authentification Protocol*) Sous-protocole d'authentification par échange de mot de passe de PPP (*Point to Point Protocole*).

Paquet (*Packet*) Unité de données du niveau 3 du modèle OSI. Voir aussi *Trame*, *Datagramme, Segment* et *Message.*

Paradiaphonie La paradiaphonie exprime l'affaiblissement du signal reçu sur une paire par rapport au signal transmis sur une autre paire. Plus la valeur est élevée meilleur est le câble.

Pare-feu Équipement réseau de sécurité qui effectue un filtrage des données. Synonyme *firewall*.

Parité Voir *Contrôle de parité*.

Passerelle (*Gateway*) Élément d'interconnexion de réseau de niveau supérieur à 3. Les passerelles applicatives sont très utilisées pour permettre l'interfonctionnement de programmes aux fonctionnalités identiques mais fonctionnant sur des systèmes incompatibles (exemple passerelle de messagerie). Ce terme a longtemps été utilisé dans le monde TCP/IP pour désigner des routeurs (Passerelles inter-réseau).

Payload Correspond au champ de données d'une unité de données. Synonyme *charge utile.*

PBX (*Private Branch eXchange*) Voir *Autocommutateur privé*.

PCI (*Protocol Control information*) Informations de contrôle ajoutées aux données de l'utilisateur pour composer un paquet OSI. Équivalent OSI du terme *en-tête.*

PCM (*Pulse Code Modulation*) Voir *MIC.*

PDH (*Plesiochronous Digital Hierarchy*) Hiérarchie de multiplexage temporel qui regroupe au premier niveau 32 IT (2 048 kbit/s) en Europe (E1) et 24 IT en Amérique du Nord et au Japon (T1).

PDU (*Protocol Data Unit*) Unité de données échangées entre des stations à un niveau spécifique du modèle OSI.

Peer to Peer Voir *Égal à égal*.

Périphérique Entité pouvant accéder à un réseau. Synonyme *nœud.*

PgP (*Pretty good Privacy*) Logiciel de cryptographie utilisé pour les échanges sur Internet.

© Dunod – La photocopie non autorisée est un délit

Phase Un des trois éléments définissant une onde, avec son amplitude et sa fréquence.

Piggyback Procédure selon laquelle l'accusé de réception d'un bloc de données est inséré dans un bloc de données émis sur une liaison *duplex*. Cette procédure optimise le débit global.

PIH (*Protocol Identifier Header*) Champ de l'encapsulation SNAP (*SubNetwork Access Protocol*) qui identifie le protocole transporté.

Pile de protocoles Ensemble des couches de logiciels dont l'interaction permet de réaliser une architecture de communication. Synonyme *stack*.

PIN (*Personnal Identification Number*) Code personnel d'authentification utilisé en GSM.

PING (*Packet INternet Groper*) Message d'écho ICMP et sa réponse, souvent utilisés pour tester l'accessibilité d'une station du réseau.

Pipe Processus qui permet la communication directe entre deux programmes que ceux-ci soient locaux ou distants. La sortie du flux d'information de l'un correspond à l'entrée de l'autre.

Pixel (*Picture Element*) Point élémentaire d'une image numérique.

Plésiochrone Caractéristique d'un réseau numérique synchronisé dans lequel chacune des stations communicantes est synchronisée sur une source d'horloge différente mais de fréquences et de stabilité identiques.

PLP (*Packet Level Protocol*) Autre désignation du protocole X.25. Voir *X.25*.

Point à point Caractéristique d'une liaison ne connectant que deux équipements. Inverse de *multipoint.*

Polling Technique de scrutation d'un terminal. Voir *Invitation à émettre.*

Pont Unité fonctionnelle qui interconnecte deux segments de réseaux, et permet le transfert de paquets entre eux. Le pont agit au niveau 2 (liaison de données) du modèle OSI et est indépendant des protocoles des couches supérieures. Dans les environnements locaux les ponts ont été remplacés par des commutateurs. Ces derniers offrent les mêmes fonctionnalités mais assurent une transmission plus rapide.

Pont distant Pont qui relie des segments de réseaux physiquement distincts par des liaisons WAN.

Pont local Pont qui relie directement des réseaux d'une même région géographique.

Pont-routeur Voir *B-Router.*

Pontage transparent Système de pontage adopté par les réseaux Ethernet et IEEE 802.3 selon lequel des ponts transmettent des trames saut par saut en fonction de tables associant des nœuds d'extrémité (adresse MAC) à des ports de ponts.

Port Interface physique entre une ligne et un équipement de réseau (routeur, par exemple). En terminologie IP, terme également utilisé pour spécifier le processus récepteur de la couche supérieure.

Porteuse (*Carrier signal*) Signal radio modulé par des données à transmettre.

POTS (*Plain Old Telephone Service*) Service standard de téléphone analogique fréquemment utilisé aux États-Unis.

PPP (*Point-to-Point Protocol*) Protocole dérivé d'HDLC, successeur de SLIP qui offre des connexions de routeur à routeur et d'hôte à réseau sur des circuits synchrones et asynchrones. Voir aussi *SLIP.*

PRI (*Primaty Rate Interface*) Interface RNIS à accès primaire. Cet accès se compose d'un unique canal D à 64 kbit/s et de 23 (aux États-Unis accès T1 à 1,544 Mbit/s) ou de 30 (en Europe accès T2 à 2,048 Mbit/s) canaux B pour la voie et/ou les données. Voir aussi *RNIS large bande et RNIS.*

Private Automatic Branch Exchange Voir *Autocommutateur privé.*

Protocole Description formelle de règles et de conventions régissant la manière dont les stations d'un réseau échangent des informations.

Protocole de routage Protocole d'échange d'information de routage et d'établissement des tables de routage. Ex. : IGRP, RIP et OSPF.

Protocole orienté bit Type de protocole de transmission sur couche Liaison de données qui peut transmettre des trames quel que soit leur contenu. Comparés aux protocoles niveau octet, les protocoles niveau bit sont plus efficaces et plus fiables, et permettent de fonctionner en *duplex*.

Protocole point-à-point Voir *PPP.*

Proxy (synonyme de *mandataire*) Technique dans laquelle une machine ou un logiciel répond aux requêtes en lieu et place d'une ou plusieurs machines. Le proxy peut ainsi réaliser des opérations que le programme d'origine n'aurait pu effectuer (incompatibilité ou autre).

PSDN (*Packet Switched Data Network*) Réseau de transmission utilisant la commutation de paquets. Désigne généralement un réseau X.25.

PSK (*Phase Shift Keying*) Voir *Modulation de phase*.

PSN (*Packet Switch Node*) Nœud de commutation de paquets. Généralement le PSN est un ETCD qui permet la connexion à un ETTD. Voir aussi *X.25.* Cet acronyme est également couramment utilisé pour *Packet Switch Network.*

Puissance lexicographique On appelle puissance lexicographique d'un code le nombre de symboles qu'il est possible de représenter à l'aide de ce code. En logique binaire avec n éléments binaires on peut représenter 2^n symboles (code à n moments).

PVC (*Permanent Virtuel Circuit*) Voir *Circuit virtuel permanent.*

Q

Q.920/Q.921 Avis du CCITT pour les interfaces réseau-utilisateurs RNIS portant sur la couche 2 du modèle ISO. Voir aussi *UNI.*

Q.931 Avis du CCITT, standard de signalisation des connexions RNIS.

Q-SIG (*Signalisation au point Q*) Norme de signalisation développée par l'ECMA et normalisé par l'ISO pour permettre un dialogue entre PABX hétérogènes.

Q.932 Avis du CCITT qui constitue le standard de la signalisation de l'établissement des circuits virtuels ATM et une évolution de l'avis CCITT Q.931.

QoS (*Quality of Service*) Voir *Qualité de service.*

Qualité de service Mesure des performances d'un système qui reflète sa qualité de transmission et la disponibilité du service.

R

Radio cellulaire Technique d'organisation des transmissions radiofréquences dans laquelle on établit une correspondance entre une fréquence et une zone géographique (cellule). Cette organisation autorise le réemploi des fréquences dans des cellules non contiguës.

RAID (*Redundant Array of Inexpensive Disk*) Système de disques à tolérance de panne.

Rapidité de modulation Voir *Baud*.

RARP (*Reverse Address Resolution Protocol*) Inverse logique de ARP qui permet à une station d'obtenir une adresse IP.

RAS (*Remote Access Service*) Système de contrôle des accès distants.

Réassemblage Reconstitution d'une unité de données après sa fragmentation par la source ou à un nœud intermédiaire.

Récupération des silences (*DSI, Digital Speech Interpolation*) Lors d'une communication téléphonique, environ 60 % du temps est inutilisé par la communication (silence). La technique de récupération des silences récupère ces instants pour effectuer des transmissions de données. Pour éviter que le correspondant distant n'ait l'impression que la communication est interrompue le DSI regénère, localement, un bruit de fond.

Redirection Partie des protocoles ICMP et ES-IS qui permet à un routeur d'indiquer à un hôte que l'utilisation d'un autre routeur serait plus efficace.

Région Ensemble logique de sous-réseaux interconnectés et constituant un domaine de routage autonome.

Reject sélectif Technique dans laquelle le récepteur ne demande la retransmission que du seul bloc reçu erroné. L'utilisation du rejet sélectif implique que le récepteur ait la capacité de mémorisation des blocs reçus ultérieurement à celui erroné et que le récepteur soit capable d'assurer le réordonnancement des blocs avant de les délivrer à la couche supérieure. Le nombre de blocs en attente s'appelle la fenêtre de réception. Voir *Rejet simple*.

Rejet simple Technique dans laquelle le récepteur demande à l'émetteur de reprendre la transmission à partir du bloc reçu erroné. Le récepteur n'a aucune capacité de stockage ni de réordonnancement, la fenêtre de réception est de 1. *Voir Rejet sélectif*, *Fenêtre de réception*.

Relais Terminologie OSI décrivant une unité qui connecte plusieurs réseaux ou systèmes de réseaux. Un relais de couche 2 est un pont, et un relais de couche 3, un routeur.

Relais de trame (*Frame Relay*) Protocole réseau issu de LAP-D et présenté comme une simplification d'X.25.

© Dunod – La photocopie non autorisée est un délit

Remise pour le mieux *(best effort)* Se dit des réseaux datagrammes dans lesquels aucune garantie de remise au destinataire n'est donnée.

RENATER Réseau national de télécommunications de la recherche.

Répéteur Équipement qui régénère le signal d'information et le signal d'horloge. Un répéteur permet d'augmenter la portée d'un système de transmission.

Réseau cellulaire Réseau de télécommunication spécialement destiné aux équipements mobiles et qui permet la communication entre ces unités mobiles, ainsi qu'avec l'ensemble des abonnés au téléphone du monde entier. Le territoire couvert est divisé en cellules, et chaque cellule est équipée d'une station fixe à laquelle est attribué un certain nombre de fréquences radio-électriques.

Réseau d'entreprise Réseau (généralement important et diversifié) connectant les principaux points d'une entreprise. À la différence du WAN, ce type de réseau est généralement privé, et ne concerne qu'une entreprise.

Réseau dorsal (*Backbone*) Réseau jouant le rôle d'artère principale pour le trafic qui circule souvent en bidirectionnel, c'est-à-dire à la fois à destination et en provenance d'autres réseaux.

Réseau local (LAN, *Local Area Network*) Réseau couvrant une surface géographique relativement peu étendue (généralement un étage ou un bâtiment). Comparés aux réseaux longue distance, les réseaux locaux ont généralement des débits de transmission élevés et des taux d'erreur faibles.

Réseau longue distance Voir *WAN*.

Réseau métropolitain Voir *MAN*.

Réseau privé Voir *Réseau d'entreprise.*

Réseau privé virtuel Ensemble de ressources de communication logiquement organisées par un service d'exploitation public et mise à la disposition du client de façon à apparaître comme son réseau privé.

Réservation de bande passante Dans les réseaux commutés, processus permettant de réserver des ressources à une communication.

Résolution d'adresses Méthode permettant de faire correspondre les adresses de niveau 3 OSI (couche Réseau) aux adresses MAC.

Résolution de noms Association d'un nom à une adresse de réseau.

Résolution dynamique d'adresses Utilisation d'un protocole de résolution d'adresses pour déterminer et stocker à la demande des informations sur les adresses.

RFC (*Request For Comments*) Documents normatifs dans l'environnement TCP/IP. Certains RFC sont déclarés par l'AB « standard Internet ». La plupart des RFC concernent des spécifications de protocole comme Telnet et FTP, mais certains sont humoristiques et/ou historiques. Les RFC sont fournis par les *Network Information Centers* d'Internet.

RHM (*Relation Homme Machine*) Terme désignant généralement le programme de gestion d'un système et par extension la console d'accès à ce système.

RIF (*Routing Information Field*) Champ de l'entête IEEE 802.5 qui est utilisé par un pont pour déterminer les anneaux Token Ring par lesquels une trame MAC doit transiter. Le RIF comporte notamment un numéro de pont et un numéro d'anneau.

RIP (*Routing Information Protocol*) Protocole de routage entre passerelles fourni avec les systèmes UNIX Berkeley. IGP le plus répandu dans l'Internet, le protocole RIP utilise le *nombre* de *sauts* comme métrique de routage. Le nombre maximal de sauts autorisés pour ce protocole est fixé à 16.

RJ-45 Connecteur glissant à 8 fils utilisé dans les réseaux locaux (IEEE 802.3 1 base5 ou StarLAN et 10 base T). Également utilisé dans certains cas pour les lignes téléphoniques (RNIS).

RLE Réseau local d'entreprise Voir *Réseau local.*

RMON (*Remote MonitOr Network*) Sonde destinée à remonter des informations d'administration.

RNIS (*Réseau numérique à intégration de services*) Ensemble de protocoles de communication proposé par les opérateurs de téléphone pour transporter, sur une même infrastructure, plusieurs services concernant la voix, les données ou les images. Ce réseau permet de connecter des équipements téléphoniques (autocommutateurs), des équipements informatiques (terminaux), la télécopie et le vidéotexte. Voir aussi *RNIS large bande.*

RNIS large bande Norme de transmission développée par le CCITT (UIT-T) pour transmettre des applications nécessitant une bande passante importante comme la vidéo. Ce standard utilise

la technologie ATM sur des circuits de transmission SONET pour offrir des vitesses de transfert de données comprises entre 155 Mbit/s et 622 Mbit/s, et au-delà.

Roaming Fonction de localisation dans un système de radiocommunication avec les mobiles.

RON/TRON (*Réception/Transmission*) Voir *E&M*.

Routage Processus de détermination du chemin d'accès vers un hôte distant. Dans les réseaux importants, ce processus est très complexe en raison du nombre de destinations intermédiaires potentielles qu'un paquet peut traverser avant d'atteindre sa destination.

Routage adaptatif Voir *Routage dynamique.*

Routage de plus court chemin Routage qui réduit au minimum les coûts de transmission par application d'un algorithme approprié.

Routage de type de service Système de routage dans lequel le choix d'une voie du réseau dépend des caractéristiques des sous-réseaux concernés, du paquet, et du plus court chemin entre le point considéré et sa destination.

Routage dynamique Routage qui s'ajuste automatiquement à la topologie ou à la charge du réseau. Synonyme *routage adaptatif.*

Routage hiérarchique Routage basé sur un système d'adressage hiérarchique. Par exemple, les algorithmes de routage IP utilisent des adresses IP, qui contiennent des numéros de réseaux, des numéros d'hôtes et (éventuellement) des numéros de sous-réseaux.

Route Synonyme de *chemin.*

Route par défaut Entrée d'une table de routage utilisée pour diriger des trames pour lesquelles un saut suivant n'est pas explicitement mentionné dans la table de routage.

Route statique Route qui est entrée manuellement dans la table de routage par défaut. Les routes statiques ont priorité sur toutes les routes choisies par tous les protocoles de routage dynamique.

Routeur Système relais de niveau 3 qui permet de choisir, parmi plusieurs chemins, celui que suivra le trafic du réseau en fonction d'une métrique optimale. (Également appelé *passerelle,* dans l'environnement TCP/IP, bien que ce terme de passerelle soit de moins en moins utilisé) le routeur transmet des paquets d'un réseau à un autre, en fonction d'informations de couche de réseau.

Routeur désigné Routeur OSPF qui génère une annonce d'état de liaison pour un réseau multi-accès. En OSPF, chaque réseau multi-accès ayant au moins deux routeurs connectés a un routeur désigné. Celui-ci, choisi par le protocole Hello OSPF, permet de réduire le nombre de contiguïtés nécessaires dans un réseau multi-accès. Ceci diminue également le trafic des protocoles de routage et la taille de la base de données topologique.

Routeurs voisins En OSPF, deux routeurs qui ont des interfaces avec un réseau commun. Dans les réseaux multi-accès, les voisins sont découverts dynamiquement par le protocole Hello de l'OSPF.

RPC (*Remote Procedure Call*) Voir *Appel de procédure à distance.*

RPIS (*Réseau privé à intégration de services*) Réseau privé de type RNIS autorisant le transfert de la voix, des données et de l'image.

RPV (*Réseau privé virtuel*) Voir *VPN*.

RS-232C Interface de couche physique, pratiquement identique à l'avis V.24.

RSA (*River Shamir et Adelman*) Algorithme de chiffrement à clés publiques et clés secrètes portant le nom de ses concepteurs.

RSVP (*Ressource ReSerVation Protocol*) Protocol de signalisation de l'environnement TCP/IP qui consiste pour un flux IP donné à « baliser » un chemin en y réservant des ressources.

RTC (*Réseau téléphonique commuté*) Réseau utilisé pour le téléphone classique.

RTT (*Round-Trip Time*) Voir *Temps de transmission aller-retour.*

S

SAR (*Segmentation and Reassembly*) Voir *Segmentation* et *Réassemblage.*

Saut Passage d'un routeur au routeur suivant (hop).

SDA (*Sélection directe à l'arrivée*) Service téléphonique permettant de joindre directement le poste demandé sans passer par le standard de l'entreprise. La SDA est un service, le nombre de numéros SDA attribué n'est pas lié au nombre de lignes de l'abonnement, mais au nombre de postes téléphoniques connectés au PABX local.

SDH (*Synchronous Digital Hierarchy*) Hiérarchie numérique synchrone destinée aux infrastructures

© Dunod – La photocopie non autorisée est un délit

des grands réseaux de télécommunication. Grâce à une technique de distribution des horloges à tous les niveaux de concentration, le SDH autorise une gigue faible. Voir *PDH.*

SDLC (*Synchronous Data Link Control*) Protocole IBM de couche de liaison de données orienté bit, qui a donné naissance à de nombreux protocoles similaires dont HDLC et LAP-B.

SDU (*Service Data Unit*) Unité de données du modèle OSI à la limite entre deux couches.

SECAM (*Sequentiel couleur à mémoire*) Système de télévison couleur français dans lequel l'information concernant une couleur est envoyée une ligne sur deux et mise en mémoire pour en disposer la ligne suivante.

Segment Terme utilisé en spécification TCP pour décrire une unique unité d'information de couche transport.

Segmentation Opération qui consiste à découper une unité de données en unités plus petites lors d'une transmission sur un support de réseau qui ne peut pas supporter la taille d'origine de l'unité de données.

Segmentation et réassemblage Processus par lequel les unités de données sont segmentées en cellules ATM à l'émission et réassemblées sous le format d'origine à la réception.

Selecting Technique de scrutation d'un terminal. Voir *Invitation à recevoir*.

Sémaphore Indicateur d'état dans un processus. Voir aussi *Canal Sémaphore.*

Semi-duplex Voir *Half duplex.*

Série de Fourier Voir *Théorème de Fourier*.

Serveur de noms Serveur du réseau qui associe un nom de machine à son adresse réseau.

Serveur Web Système hébergeant des documents hypertextes mis à disposition sur Internet ou en Intranet et consultable par un logiciel de navigation.

Signal analogique Signal électrique variant de manière analogue à un phénomène physique (voix, pression...). Les signaux analogiques sont essentiellement caractérisés par l'infinité de valeurs prises par le signal entre les bornes de variation du phénomène physique.

Signalisation Processus qui consiste à envoyer des informations de service sur un support physique pour établir une communication la superviser et la rompre.

Signalisation E&M Standard de signalisation téléphonique utilisée sur les lignes interurbaines et intercommutateurs.

Signalisation hors bande Protocole de transmission utilisant des fréquences ou des canaux situés en dehors des fréquences ou des canaux utilisés normalement pour le transfert d'informations.

Signalisation intrabande Transmission d'information de service sur le même canal que celui utilisé pour la transmission de données. À l'opposé de la *signalisation hors-bande* qui transmet les informations de service sur un canal différent du canal de transmission des données.

Signalisation par canal sémaphore Système de signalisation hors-bande utilisé par de nombreux réseaux téléphoniques, qui sépare les informations de signalisation des données utilisateur.

SIM (*Subscriber Identification Module*) Carte à puce utilisée dans un système terminal GSM et qui contient toutes les informations relatives à l'abonné.

SIMlock Verrouillage, par l'opérateur, de la carte SIM pour en interdire l'usage.

SLIP (*Serial Line Internet Protocol*) Protocole utilisé pour transporter IP sur des liaisons séries (circuits téléphoniques par exemple). SLIP n'assure que la délimitation des unités de données (datagrammes IP).

SMDS (*Switch Multimegabit Data Service*) Service de transfert rapide de données (organisé en cellules de taille fixe) sur longue distance, défini par les laboratoires américains BelCore. Achemine du trafic issu des réseaux locaux. Synonyme *CBDS*.

SMS (*Short Message Service*) Service d'envoi de messages courts à destination d'un téléphone mobile.

SMTP (*Simple Mail Transfer Protocol*) Protocole Internet offrant des services de courrier électronique.

SNA (*System Network Architecture*) Architecture générale de communication en couches développée par IBM au cours des années 70.

SNMP (*Simple Network Management Protocol*) Protocole de gestion des réseaux Internet qui permet de contrôler et de spécifier la configuration du réseau et les paramètres d'exécution.

SNPA (*SubNerwork Point of Attachment*) Adresse d'un point d'accès au réseau de transport. Une adresse X.121 désigne un SNPA.

Socket Structure logicielle fonctionnant comme point d'accès entre couches de communication dans une station en réseau (*API socket*).

Somme de contrôle Méthode permettant de vérifier l'intégrité des données transmises. Une somme de contrôle est une valeur entière calculée par une série d'opérations arithmétiques sur une séquence d'octets. La valeur est recalculée à l'extrémité réceptrice et comparée à la valeur d'origine. Voir *CRC, FCS*.

SONET (*Synchronous Optical NETwork*) Réseau synchrone rapide (pouvant fonctionner à 2,5 Gbit/s) déclaré norme internationale en 1988. Voir *SDH*.

Source routing Technique de routage dans laquelle c'est l'émetteur du message qui définit la route à suivre Les données sont émises avec la liste des nœuds à traverser.

Sous-canal En terminologie large bande, subdivision de fréquences créant un canal de communication séparé.

Sous-couche MAC (MAC, *Medium Access Control*) Voir *MAC*.

Sous-réseau Terme parfois utilisé pour faire référence à un segment de réseau. Dans les réseaux IP, sous-ensemble de machines réseau partageant une adresse réseau particulière et distingué par un champ de bits (SubNet_ID).

Spanning tree Voir *Algorithme du spanning tree*.

Spectre de fréquences Voir *Largeur de bande*.

SPOOL (*Simultaneous Peripherals Operation On-Line*) Voir *Spooler.*

Spooler Application qui gère les requêtes ou les travaux qui lui sont soumis à des fins d'exécution. Les spoolers traitent les requêtes qui lui sont soumises dans l'ordre dans lequel elles figurent dans la file d'attente. L'exemple le plus connu de spooler est probablement le spooler d'impression.

SQE (*Signal Quality Error*) Dans les réseaux Ethernet, message renvoyé par un récepteur au contrôleur pour lui indiquer si le circuit de collision fonctionne.

SQL (*Structured Query Langage*) Langage de requêtes pour base de données développé par IBM.

STA (*Spanning Tree Algorithm*) Voir *Algorithme du spanning tree*.

Standard de fait Standard consacré davantage par l'usage que par une norme officielle.

Station primaire Dans les protocoles de couche Liaison de données synchrone par bit comme HDLC et SDLC, station qui contrôle la transmission des stations secondaires et assure d'autres fonctions de gestion comme le contrôle des erreurs (par rejet sélectif ou autre). Les stations primaires envoient des commandes aux stations secondaires et en reçoivent des réponses. Voir aussi *Station secondaire.*

Station secondaire Dans les protocoles de couche de liaison de données synchrone orientés bit, comme HDLC, station qui réagit aux commandes que lui envoie une station primaire. Voir aussi *Station primaire.*

Store and forward Technique de commutation de messages dans laquelle des messages sont stockés momentanément en des points intermédiaires entre la source et la destination, jusqu'à ce que les ressources du réseau (une liaison non utilisée, par exemple) soient disponibles.

STP (*Shielded Twisted Pairs*) Paire torsadée blindée. Câble constitué de plusieurs paires torsadées protégées par un blindage.

Suppresseur d'écho Dispositif utilisé pour éliminer les échos sur les transmissions vocales à longue distance. L'écho provient généralement d'une désadaptation d'impédance au passage de la ligne de 2 à 4 fils et inversement.

SVC (*Switch Virtual Circuit*) Voir *Circuit virtuel commuté.*

Switched Ethernet Voir *Commutation Ethernet*.

Synchrone Caractéristique d'un mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, en synchronisation d'une même référence temporelle.

Syntaxe abstraite Description de structure de données indépendante des structures et des codes matériels (exemple ASN-1).

Système à tolérance de pannes (*SFT, System Fault Tolerance*) Ensemble de mécanismes mis en œuvre pour pallier la défaillance d'un élément du système et assurer la continuité du service. Les principaux mécanismes mis en œuvre dans les systèmes à tolérance de pannes sont : les disques miroirs, les disques en *duplex*.

© Dunod – La photocopie non autorisée est un délit

Système autonome Ensemble de réseaux ayant une administration commune et une stratégie de routage commune. Un système autonome doit avoir un numéro d'identification à 16 bits qui lui est affecté par le centre d'information réseaux (également appelé NIC ou *Network Information Center*).

Système intermédiaire Voir *Relais*.

T

T0 *Voir Accès de base.*

T1 Accès spécifique, non disponible en France, du réseau RNIS faisant référence à un lien multiplex numérique utilisé pour la transmission des données à 1,544 Mbit/s sur lignes téléphoniques.

T2 *Voir Accès primaire.*

TAPI (*Telephony Application Programming Interface*) Ensemble de DLL de Microsoft permettant le développement d'applications de gestion des communications téléphoniques.

TCP/IP (*Transmission Control Protocol/Internet Protocol*) Regroupement de deux protocoles Internet bien connus, souvent considérés à tort comme un seul et même protocole. TCP correspond à la couche 4 (transport du modèle OSI) et permet une transmission fiable des données. IP correspond à la couche 3 (couche réseau du modèle OSI) et offre un service de datagrammes en mode non connecté. TCP/IP a été développé pour le ministère américain de la défense dans les années 70.

TDM (*Time Division Multiplexing*) Voir *Multiplexage à répartition temporelle.*

TDMA (*Time Division Multiple Access*) Voir *AMRT.*

TEI (*Terminal End-Point Identifier*) Champ de la trame LAP-D sur 7 bits, qui correspond à l'identification du terminal proprement dit. Les TEI peuvent être attribués par le constructeur (TEI de 0 à 63) ou par le réseau, la TNR alloue les TEI de 64 à 126. Le TEI 127 est réservé à la diffusion de messages. Lorsqu'un terminal à allocation automatique de TEI est connecté au bus, il demande au réseau de lui attribuer un TEI, alors qu'un terminal à affectation non automatique s'assure de l'unicité de son TEI. Un terminal multifonction peut utiliser plusieurs TEI, un par fonction.

Télécommunications Terme regroupant l'ensemble des techniques de transmission.

Télécopieur Système de transmission de l'écrit par numérisation du document et transmission. Le résultat de la transmission est une télécopie ou fac simile.

Tempête de diffusion Phénomène survenant sur le réseau lorsque plusieurs messages sont transmis simultanément, en utilisant une largeur de bande importante.

Temporisation (retransmission sur temporisation) Événement qui se produit lorsqu'une station d'un réseau s'attend à recevoir d'une autre station du réseau des informations qui ne lui parviennent pas pendant le délai prévu. La temporisation entraîne généralement une retransmission des informations ou l'annulation du circuit virtuel entre les deux stations.

Temps de groupe Voir *Distorsion de phase.*

Temps de propagation Voir *Délai de propagation.*

Temps de transmission aller-retour (RTT, *Round-Trip Time*) Temps compris entre le moment d'émission d'un message et la réception de son accusé de réception. Le RTT est utilisé dans certains algorithmes de routage pour le calcul des routes optimales.

Terminaison Résistance électrique placée à l'extrémité d'une ligne de transmission, et qui absorbe les signaux circulant sur la ligne, empêchant ainsi l'écho.

Terminal asynchrone Terminal très simple dans lequel chaque caractère entré au clavier est immédiatement transmis au système hôte. Le système hôte renvoie au terminal le caractère reçu qui est alors affiché (écho distant). Certains terminaux asynchrones gèrent l'écho localement. Les terminaux Minitel, VT100 et Telnet sont des exemples de terminaux asynchrones. Les caractères sont envoyés sur le support au rythme de la frappe, la transmission est du type asynchrone. Voir *Asynchrone*, *Terminal synchrone*.

Terminal synchrone Terminal dans lequel les caractères frappés au clavier ne sont transmis qu'après validation (par bloc). L'écho des caractères introduit est local. La transmission entre le terminal et le système hôte est dite transmission synchrone. Voir *Synchrone*, *Terminal asynchrone*.

TFTP (*Trivial File Transfer Protocol*) Version simplifiée de FTP qui permet le transfert de fichiers d'un ordinateur à l'autre sur un réseau.

Théorème de Fourier Une fonction périodique de fréquence f_0 peut être considérée comme la somme d'une constante (*composante continue*) et de fonctions sinusoïdales de fréquence égale à celle du signal périodique (*fondamental*) et multiple de celle-ci (*harmoniques*). Est utilisée notamment pour passer du domaine temporel au domaine fréquentiel dans l'analyse des signaux, c'est-à-dire pour transformer une impulsion en une somme de signaux périodiques sinusoïdaux afin d'étudier le comportement d'un système auquel on applique ce signal.

Théorème de Shannon Le théorème de Shannon définit la fréquence minimale d'échantillonnage d'un signal. Celle-ci doit être au minimum le double de la fréquence maximale du signal à échantillonner.

Time Out Exprime la borne maximale pour qu'un événement intervienne. Voir *Temporisation*.

Time slot Voir *IT*.

Token Ring Réseau local à passage de jeton développé et supporté par IBM. Très semblable à un réseau local (LAN) IEEE 802-5.

Topologie Disposition physique des nœuds et des supports d'un réseau dans une structure de réseaux d'entreprise.

Topologie en anneau Topologie dans laquelle le réseau se compose d'une série de répéteurs reliés les uns aux autres par des liaisons de transmission unidirectionnelle pour former une unique boucle fermée. Chaque station du réseau se connecte au réseau au niveau d'un répéteur.

Topologie en bus Architecture LAN selon laquelle les transmissions des stations du réseau se propagent sur toute la longueur du support et sont reçues par toutes les autres stations.

Topologie en étoile Topologie dans laquelle les extrémités d'un réseau sont connectées à un commutateur central commun par des liaisons point à point.

Topologie logique Caractérise le dialogue dans un réseau local. Voir *Topologie physique*.

Topologie physique Désigne comment les stations d'un réseau local sont raccordées au réseau, alors que la topologie logique caractérise l'échange de messages. Le réseau Token Ring a une topologie physique en étoile (les stations sont raccordées à un concentrateur spécifique, le MAU) alors que l'échange des messages s'effectue selon un anneau (topologie logique en anneau).

Total de contrôle Voir *Somme de contrôle.*

TP4 (*Transport Protocol Class 4*) Protocole de transfert ISO en mode connecté défini par la norme ISO 8073.

Trame Groupe logique d'informations supporté et transmis par la couche Liaison de données. Les termes *paquet, datagramme, segment et message* sont également utilisés pour décrire des groupes d'information logique à différentes couches du modèle ISO et dans différents cercles technologiques.

Tranceiver Voir *MAU.*

Transmetteur Voir *MAU.*

Transmission analogique Technique de transmission de signaux selon laquelle l'information est transmise par variation d'une combinaison d'amplitude, de fréquence et de phase de signaux.

Transmission asynchrone Mode de transmission dans lequel les horloges émission et réception sont indépendantes. Les caractères sont entre des bits de contrôle appelés *bits de départ et bits d'arrêt (ou start et stop),* qui désignent le début et la fin des caractères.

Transmission parallèle Transmission simultanée de tous les bits composant un caractère ou un octet. Voir aussi *Transmission série.*

Transmission série Méthode de transmission des données dans laquelle les bits d'un caractère de donnée sont transmis de manière séquentielle sur un unique canal. Voir aussi *Transmission parallèle.*

Transmission synchrone Mode de transmission dans lequel l'émetteur et le récepteur fonctionnent au même rythme, calés sur une même horloge.

Trap Message non sollicité envoyé par un agent SNMP à un système de gestion de réseau (NMS) pour signaler l'apparition d'un événement significatif.

Trou noir Terme de routage appliqué à une zone d'interconnexion de réseau dans laquelle les paquets entrent, mais d'où ils ne sortent pas, en raison de l'existence de conditions défavorables ou d'un problème de configuration de systèmes sur une partie du réseau.

Trunk Canal formé par plusieurs lignes de base reliant deux autocommutateurs**.**

Tube cathodique (*CRT, Cathode Ray Tube*) Élément de visualisation de la console écran.

© Dunod – La photocopie non autorisée est un délit

Tunnel Voir *Encapsulation.*

Tunneling Voir *Encapsulation*.

U

UART (*Universal Asynchronous Receiver and Transmitter*) Composant électronique émettant ou recevant des caractères sur une ligne de transmission en mode série asynchrone.

UBR (*Unspecified Bit Rate*) Classe de service dans ATM dans laquelle aucune garantie de qualité de service n'est donnée à la source. Mode *best effort*. Voir *ABR, CBR, VBR.*

UDP (*User Datagram Protocol*) Protocole de couche Transport sans connexion appartenant à la famille des protocoles Internet.

UIT (*Union Internationale de Télécommunications*) Organisme international dont le siège est à Genève et qui est chargé, dans le cadre de l'ONU, des questions de télécommunications.

UMTS (*Universal Mobile Telecommunications System*) Système de téléphonie mobile autorisant des accès haut débit à Internet.

UNI (*User Network Interface*) Interface réseau utilisateur définie par le forum ATM pour l'accès aux réseaux ATM privés et publics.

Unicast *Voir Adresse unique.*

URAD (Unité de raccordement d'abonnés déportés) Élément d'une installation de téléphonie qui autorise le raccordement d'abonnés ne pouvant être raccordés directement à l'installation principale. L'URAD et le PABX principal peuvent être reliés par des LIA ou par un lien MIC.

URL (*Uniform Ressource Locator*) Adresse logique d'un système dans le réseau Internet.

UTP (*Unshielded Twisted Pairs*) Câble à paires torsadées non écranté. Les câbles UTP représentent la majorité des câblages mondiaux. Les câblages français ont plutôt opté pour le câble FTP. Voir *FTP*.

V

V.24 Interface de couche physique utilisée dans de nombreux pays. Très semblable à EIA-232D et RS-232-C.

Valence Nombre d'états significatifs d'un signal. Permet pour une même rapidité de modulation d'obtenir un débit plus élevé.

Variables MIB (*Management Information Base*) Base de données d'information sur des objets gérés à laquelle il est possible d'accéder par des protocoles de gestion de réseau comme SNMP et CMIP.

VBR (*Variable Bit Rate*) Classe de service dans ATM dans laquelle le débit de la source varie entre deux valeurs négociées et garanties par le réseau. Voir *ABR, CBR, UBR.*

VCI (*Virtual Circuit Identifier*) Voir *VPI/VCI*.

VLSM (*Variable Length Subnet Mask*) Possibilité de spécifier, pour le même numéro de réseau, un masque différent sur différents sous-réseaux. Permet d'optimiser l'espace d'adressage disponible. Est actuellement supporté par le protocole de routage OSPF et le routage statique.

VPI/VCI (*Virtual Path identifier/Virtual Channel identifier*) Combinés, ces champs identifient une connexion au réseau ATM.

VPN (*Virtual Privat Network*) Technique qui simule un réseau privé dans un réseau public.

VRC (*Vertical Redundancy Check*) Contrôle vertical de redondance, technique de contrôle de parité appliquée à tous les mêmes bits d'un bloc et non à l'ensemble des bits d'un caractère (LRC, *Longitudinal Redundancy Check*).

VSAT (*Very Small Aperture Terminal*) Système de transmission par satellite géostationnaire utilisant des antennes de faible dimension.

VT (*Virtual Terminal*, ISO 9040 et 9041) définit un terminal virtuel (nombre de lignes, nombre de caractères par ligne, attributs de caractères, fontes...). Il assure la correspondance entre les caractéristiques du terminal virtuel et le terminal du système physique réel. VT gère les différents types de terminaux : terminal en mode défilement ou rouleau, terminal en mode page, terminal en mode masque d'écran et données, terminal graphique simple ou multi-fenêtre.

VTAM (*Virtual Telecommunications Access Method*) Ensemble de programmes qui contrôle les communications entre des nœuds et des programmes d'applications tournant sur un système hôte.

W

W3 Voir *World Wide Web*

W3C (*World Wide Web Consortium*) Organisme chargé de la normalisation de HTML.

WAN (*Wide Area Network*) Réseau recouvrant une région géographique relativement étendue. Également appelé *réseau longue distance.* Voir aussi *LAN et MAN.*

Web Voir *Word Wide Web*

Wi-Fi Nom commercial d'un système de transmission sans fil (IEEE 802.11).

World Wide Web (*WWW*) Ensemble des serveurs Web accessibles sur Internet, couramment appelé Web.

WWW Voir *World Wide Web.*

X

X.3 Avis CCITT qui définit différents paramètres PAD.

X.500 Avis CCITT (UIT) Service d'annuaire du monde OSI.

X-Modem Protocole de transmission de données du domaine public.

X.21 Avis CCITT (UIT) définissant un protocole de communication entre des unités utilisateur et un réseau à commutation de circuits.

X.25 Avis CCITT (UIT) qui définit les protocoles d'accès (protocole entre l'ETTD ou DTE et l'ETCD ou DCE) au réseau à commutation de paquets appelé réseau X.25 ou *PSPDN* (*Packet Switched Public Data Network*).

X.28 Avis CCITT qui définit l'interface terminal-PAD.

X.29 Avis CCITT qui définit l'interface ordinateur-PAD.

X.400 Avis CCITT qui spécifie une norme de transfert électronique de fichiers.

XID (*eXchange Identification*) Trame HDLC utilisée pour l'identification du terminal en X.25, ou pour déterminer les paramètres d'un échange dans les réseaux locaux (LLC1).

XNS (*Xerox Network System*) Ensemble de protocoles initialement conçus par Xerox PARC.

Y-Z

Y-modem Protocole de transmission de données par blocs en mode asynchrone. Ce protocole inclut un mécanisme de détection d'erreur mais pas de reprise sur erreur.

Zone d'autorité Associée au service DNS, elle correspond à une section de l'arbre de nommage sur lequel un serveur a autorité.

Z-modem Protocole asynchrone de transmission de données par blocs avec détection et reprise sur erreur.

Annexes

A. NORMALISATION

La normalisation peut être vue comme un ensemble de règles destinées à satisfaire un besoin de manière similaire. La normalisation dans un domaine technique assure une réduction des coûts d'étude, la rationalisation de la fabrication et garantit un marché plus vaste. Pour le consommateur, la normalisation est une garantie d'interfonctionnement, d'indépendance vis-à-vis d'un fournisseur et de pérennité des investissements.

En matière de télécommunication, la normalisation est issue d'organismes divers. Du groupement de constructeurs aux organismes internationaux, la normalisation couvre tous les domaines de la communication. D'une manière générale, elle ne s'impose pas, sauf celle émanant de l'**ETSI** (*European Telecommunications Standard Institute*) qui normalise les réseaux publics et leurs moyens d'accès.

Les principaux groupements de constructeurs sont :

- **ECMA** (*European Computer Manufactures Association*), à l'origine constituée uniquement de constructeurs européens (Bull, Philips, Siemens...), l'ECMA comprend aujourd'hui tous les grands constructeurs mondiaux (DEC, IBM, NEC, Unisys...). En matière de télécommunications, l'ECMA comprend deux comités : le TC23 pour l'interconnexion des systèmes ouverts et le TC24 pour les protocoles de communication ;
- **EIA** (*Electronic Industries Association*) connue, essentiellement, pour les recommandations RS232C, 449 et 442.

Les principaux organismes nationaux auxquels participent des industriels, administrations et utilisateurs sont :

- **AFNOR**, Association française de normalisation,
- **ANSI**, American National Standard Institute (États-Unis),
- **DIN**, *Deutsches Institut für Normung* (Allemagne), bien connu pour sa normalisation des connecteurs (prises DIN) ;
- **BSI**, British Standard Institute (Grande-Bretagne).

Les organismes internationaux :

- **ISO**, *International Standardization Organization*, regroupe environ 90 pays. L'ISO est organisée en *Technical Committee* (TC) environ 200, divisés en *Sub-Committee* (SC) eux-mêmes subdivisés en *Working Group* (WG) ; la France y est représentée par l'AFNOR ;
- **CEI**, Commission électrotechnique internationale, affiliée à l'ISO en est la branche électricité ;
- **UIT-T**, Union internationale des télécommunications secteur des télécommunications, qui a succédé en 1996 au CCITT (Comité consultatif international télégraphie et téléphonie), publie des recommandations. Celles-ci sont éditées tous les 4 ans sous forme de recueils. Les domaines d'application sont identifiés par une lettre :
  - V, concerne les modems et les interfaces,
  - T, s'applique aux applications télématiques,
  - X, désigne les réseaux de transmission de données,
  - I, se rapporte au RNIS,
  - Q, intéresse la téléphonie et la signalisation.

L'**IEEE**, *Institute of Electrical and Electronics Enginers*, société savante constituée d'industriels et d'universitaires, est essentiellement connue par ses spécifications sur les bus d'instrumentation (IEEE 488) et par ses publications concernant les réseaux locaux (IEEE 802), reprises par l'ISO (IS 8802).

Le panorama serait incomplet si on omettait de citer l'**IAB**, *Internet Architecture Board*, qui a la charge de définir la politique à long terme d'Internet, tandis que l'**IETF** (*Internet Engineering Task Force*) assure par ses publications (**RFC**, *Request For Comments*) l'homogénéité de la communauté TCP/IP et Internet.

La rédaction d'une norme est une succession de publications, la durée entre le projet et la publication définitive peut être très longue. En effet, chaque partie tente d'y défendre ses intérêts économiques et commerciaux. D'une manière générale, un projet de normalisation est formalisé dans un document brouillon qui expose les concepts en cours de développement (*Draft*) ; lorsque ce document arrive à une forme stable, les « drafts » sont publiés (*Draft proposable*), chaque pays émet son avis (vote). Enfin, une forme quasi définitive est publiée, elle constitue une base de travail pour les constructeurs (*Draft International Standard*). La norme appelée *International Standard* (**IS**) est ensuite publiée.

B. QUELQUES DÉFINITIONS

	ASYNCHRONE	SYNCHRONE	ISOCHRONE	PLÉSIOCHRONE
Trafic ou flux de données	Notion utilisée dans les réseaux FDDI, les données de la classe asynchrone correspondent à un flux auquel n'est attachée aucune contrainte temporelle.	Notion utilisée dans les réseaux FDDI, les données de la classe synchrone correspondent à un flux auquel est attachée une légère contrainte temporelle (réservation de bande passante).	Données ayant une contrainte temporelle forte en relation directe avec le rythme de délivrance des informations. Ex. : la voix.	
Transmission	Transmission en mode caractère ou bloc, même si les données sont constituées en bloc, chaque caractère comporte un délimiteur de début et de fin (bit de start, bit de stop).	Transmission en mode bloc, chaque bloc comporte un délimiteur de début de bloc et de fin (fanion), les caractères ne sont pas délimités.		
Mode de transfert	Données émises au rythme de la source (mode paquet ou ATM).	Données émises au rythme du réseau (mode circuit ou STM).		
Réseau		Tous les nœuds du réseau ont une même référence temporelle (même horloge). Ex. : Token Ring.		Chaque noeud du réseau à sa propre horloge. Exemple : Ethernet, FDDI.
Terminal	Terminal en mode caractère. Ex. : VT100, Minitel.	Terminal en mode bloc.		

C. ABAQUES D'ERLANG

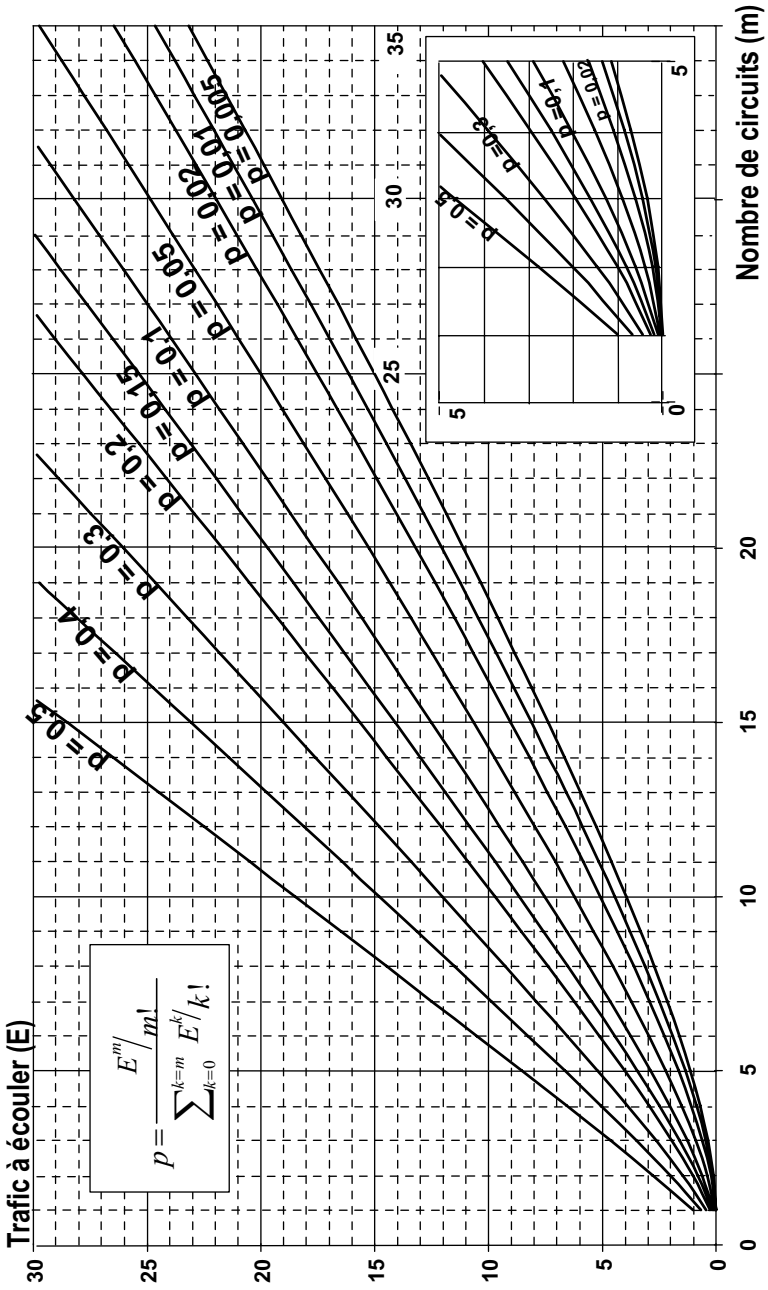


Figure C.1 – Abaque d'Erlang à refus

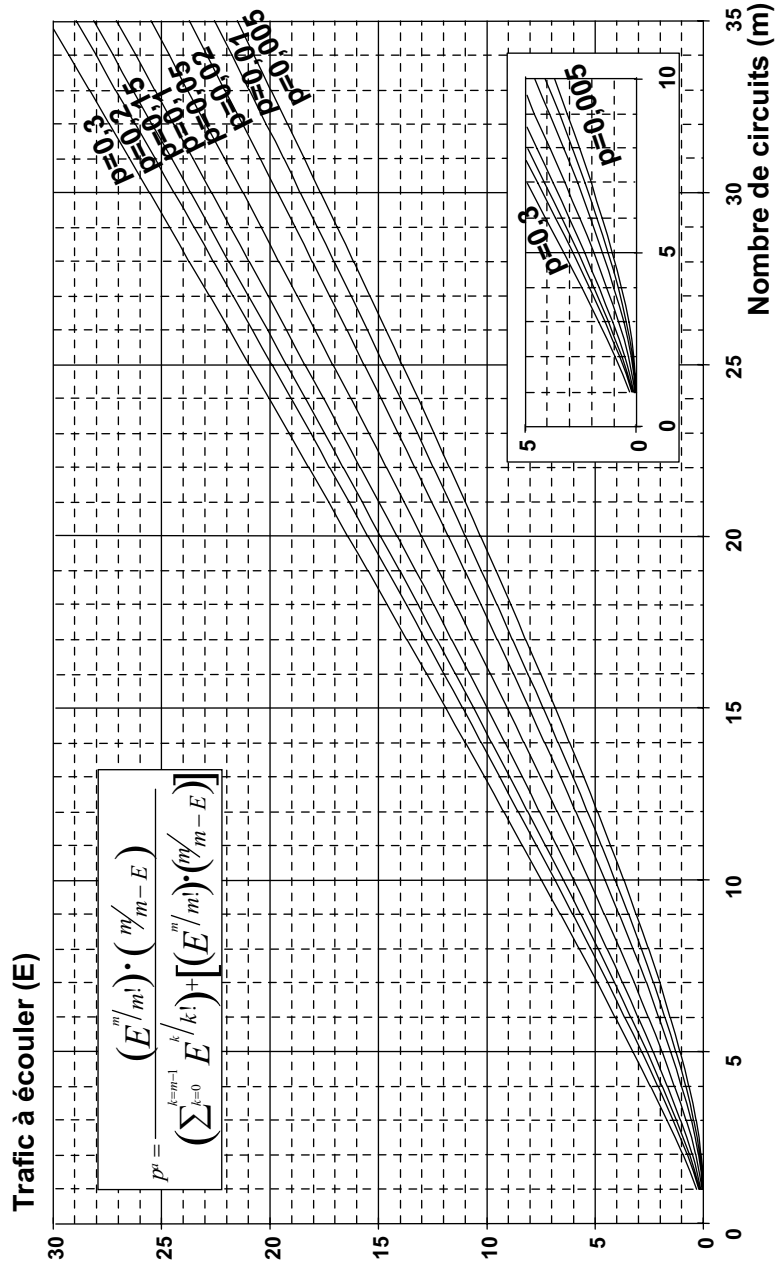


Figure C.2 – Abaque d'Erlang à attente

D. LISTE DES ABRÉVIATIONS ET SIGLES UTILISÉS

AAL *ATM Adaptation Layer*

ABM *Asynchronous Balanced Mode*

ABR *Available Bit Rate*

ARCEP Autorité de régulation des communications électroniques et des postes

ACF *Advanced Communication Function*

ACK *Acknowledge*

ACR *Attenuation Crosstalk Ratio*

ADCCP *Advanced Data Communication Control Protocol*

ADPCM *Adaptative Differential Pulse Code Modulation*

ADSL *Asymmetric Data Subscriber Line*

AF *Assured Forwarding*

AFI *Autority Format Identifier*

AFNOR Association française de normalisation

AMRT Accès multiple à répartition dans le temps

ANSI *Americain National Standard Institute*

AP *Access Point*

AP *Application Proccess*

API *Application Program Interface*

ARIS *Aggregate Route-based IP Switching*

ARM *Asynchronous Response Mode*

ARP *Address Resolution Protocol*

ARQ *Automatic Retransmission Request*

ART Autorité de régulation des télécommunications

ASCE *Association Control Service Element*

ASCII *Americain Standard Code for Information Interchange*

ASE *Application Service Element*

ASN-1 *Abstract Syntax Notation One*

ASP *Application Service Provider*

ATM *Asynchronous Transfer Mode*

AU *Administrative Unit*

BAS *Basic Activity Subset*

Bc *Committed Burst size*

BCC *Block Check Character*

BCCH *Broadcast Control Channel*

BCD *Binary Code Decimal*

BCS *Bull Cabling System*

Be *Excess Burst size*

BEB *Binary Exponentiel Backoff*

BECN *Backward Explicit Congestion Notification*

B-ICI-NNI *Broadband Inter-Carrier Interface Network to Network Interface*

B-ISDN *Broadband Integrated Service Digital Network*

BLR Boucle locale radio

BLU Bande latérale unique

BNC *Barrel Neck Connector*

BOF *Birth Of a Feature*

BPSK *Binary Phase Shift Keying*

BSA *Basic Service Area*

BSC *Basic Combined Subset*

BSC *Binary Synchronous Communication*

BSI *British Standard Institute*

BSS *Basic Service Set*

BSS *Basic Synchronized Subset*

BTS *Base Transmission Station*

BUS *Broadcast and Unknown Server*

C/R *Commande/Response*

CAC *Connection Admission Call*

CAP *Carrier Amplitude and Phase modulation*

CAS *Channel Associated Signaling*

CATV Câble d'antenne de télévision

CBDS *Connectionless Broadband Data Service*

CBR *Constant Bit Rate*

CCI *Client-to-Client Interface*

CCITT Comité consultatif international pour le télégraphe et le téléphone

CCR *Current Cell Rate*

CCRSE *Commitment Concurency and Recovery Service Element*

CCS *Common Channel Signaling*

CDMA *Code Division Multiple Access*
CDV *Cell Delay Variation*
CEI Commission électrotechnique internationale
CELP *Code Excited Linear Prediction*
CER *Cell Error Ratio*
CES *Circuit Emulation Structured*
CFP *Contention Free Period*
CGM *Computer Graphics Metafile*
CI *Congestion Indication*
CIDR *Classless InterDomain Routing*
CIR *Committed Information Rate*
CLLM *Consolited Link Layer Management*
CLNAP *ConnectionLess Network Access Protocol*
CLNIP *ConnectionLess Network Interface Protocol*
CLNS *ConnectionLess Network Service*
CLP *Cell Loss Priority*
CLR *Cell Loss Ratio*
CLS *ConnectionLess Server*
CMR *Cell Misinsertion Rate*
CNLS *ConnectionLess Oriented Network Service*
CODEC Codeur décodeur
COF *Connection Oriented Function*
CONS *Connection Oriented Network Service*
CORBA *Common Object Request Broker Architecture*
CoS *Class of Service*
COS *Comittee Of Standardization*
CPCS *Common Part Convergence Sublayer*
CPI *Common Part Indication*
CRC *Cyclic Redundancy Check*
CS *Convergence Sublayer*
CSI *Convergence Sublayer Information*
CSMA *Carrier Send Multiple Access*
CSR *Cell Switched Router*
CSS *Common Channel Signaling*
CTD *Cell Transfert Delay*
CTI Couplage téléphonie/informatique
CTS *Clear To Send*
CV Circuit virtuel
CVC Circuit virtuel commuté
CVP Circuit virtuel permanent
DAB *Digital Audio Broadcast*
DAC *Double Attachment Concentrator*
DARPA *Defence Advanced Projet Adgency USA*
DAS *Double Attachment Station*
DBR *Deterministic Bit Rate*
DCB Décimal codé binaire
DCE *Data Circuit Equipment*
DCF *Distributed Coordination Function*
DDCMP *Digital Data Communication Message Protocol*
DE *Discard Eligibility*
DECT *Digital Enhanced Cordless Telephone*
DES *Data Encryption Standard*
DF *Do not Fragment*
DHCP *Dynamic Host Configuration Protocol*
DiffServ *Differentiated Services*
DIFS DCF IFS
DIN *Deutsches Institut für Normung*
DISOSS *Distributed Office Support System*
DIT *Directory Information Tree*
DIX Digital, Intel et Xerox
DLC *Data Link Control*
DLCI *Data Link Connection Identifier*
DM-PDU *Derived MAC PDU*
DMT *Discrete MultiTone*
DMZ *DeMilitarized Zone*
DNIC *Data Network Identification Code*
DNS *Domain Name System*
DoD *Department of Defence*
DOM *Document Object Model*
DPAM *Demand Priority Access Method*
DQDB *Distributed Queue Dual Bus*
DS *Directory Service*
DS *Distribution System*

© Dunod – La photocopie non autorisée est un délit

DSA *Distributed System Architecture*

DSAP *Destination Service Access Point*

DSL *Digital Subscriber Line*

DSP *Domain Specific Part*

DSSS *Direct Sequence Spread Spectrum*

DSSSL *Document Style Semantics and Specification Language*

DTD *Document Type Definition*

DTE *Data Terminal Equipment*

DTIM *Delivery Traffic Information Map*

DTL *Designated Transit List*

DTMF *Dual Tone Multi Frequency*

DTP *Distributed Transaction Processing*

DVB *Digital Video Broadcast*

DWDM *Dense WDM*

E&M *Earth & Mouth*

EA *End Address*

EB *Elasticity Buffer*

EBCDIC *Extended Binary Decimal Interchange Code*

EBCI *Explicit Backward Congestion Identifier*

ECMA *European Computer Manufacturers Association*

ECN *Explicit Congestion Notification*

ECR *Explicit Cell Rate*

EDCF *Extended DCF*

EDGE *Enhanced Data Rates for GSM Evolution*

EFCI *Explicit Forward Congestion Identifier*

EFCN *Explicit Forward Congestion Notification*

EIA *Electronic Industries Association*

EIFS *Extended IFS*

EIR *Excess Information Rate*

ELAN *Emulated LAN*

EOP *Element of Procedure*

EPD *Early Packet Discard*

ERBdB Émétteur récepteur en bande de base

ES *End System*

ESI *End System Identifier*

ESS *Extended Set Service*

ETCD Équipement terminal de circuit de données

ETR *Early Token Release*

ETTD Équipement terminal de traitement de données

FCS *Fibre Channel Standard*

FCS *Frame Check Sequence*

FDDI *Fiber Distributed Data Interface*

FDM *Frequency Division Multiplexing*

FDSE *Full Duplex Switched Ethernet*

FEC *Forwarding Equivalence Class*

FECN *Forward Explicit Congestion Notification*

FHSS *Frequency Hopping Spread Spectrum*

FLP *Fast Link Pulse*

FR *Frame Relay* (relais de trames)

FRAD *Frame Relay Access Device*

FSK *Frequency Shift Keying*

FTAM *File Transfer Access and Management*

FTP *File Transfer Protocol*

FTP *Foiled Twisted Pair*

GFA Groupe fermé d'abonnés

GFC *Generic Flow Control*

GFU Groupe fermé d'utilisateurs

GMPLS *Generalized MPLS*

GPRS *General Packet Radio Services*

GPS *Global Positioning System*

GSM *Global System for Mobile communications*

GSMP *General Switch Management Protocol*

HC *Hybrid Coordinator*

HCF *Hybrid Coordination Function*

HDBn Haute densité binaire d'ordre *n*

HDLC *High Level Data Link Protocol*

HDSL *High data rate DSL*

HEC *Header Error Control*

HEL *Header Extension Length*

HiPPI *High Performance Parallel Interface*

HLPI *Higher Layer Protocol Identifier*

HLR *Home Local Register*

HR/DSSS *High Rate DSSS*

HSTRA *High Speed Token Ring Alliance*

HTML *Hyper Text Markup Language*

HTTP *Hyper Text Transfer Protocol*

IAB *Internet Activities Board*

IBSS *Independent Basic Service Set*

ICANN *Internet Corporation Assigned Names and Numbers*

ICF *Isochronous Convergence Function*

ICMP *Internet Control and error Message Protocol*

ICS *IBM Cabling System*

IDI *Initial Domain Identifier*

IDL *Interface Definition Language*

IDP *Initial Domain Part*

IEEE *Institue of Electrical and Electronics Enginers*

IFG *InterFrame Gap*

IFS *InterFrame Space*

IGRP *Interior Gateway Routing Protocol*

IISP *Interim Inter Switch Protocol*

IKE *Internet Key Exchange*

ILMI *Interim Local Management Interface*

IM-PDU *Initial MAC Protocol Data Unit*

IMSI *International Mobile Subscriber Identity*

InARP *Inverse ARP*

IntServ *Integrated Services*

IP *Internet Protocol*

IPBX *Internet Protocol private Branch eXchange*

IPsec *IP Security*

IRL *Inter Repeater Link*

ISDN *Integrated Services Digital Network*

IS-IS *Intermediate System to Interme- diate System*

ISO *International Standardization Organization*

IT Intervalle de temps

JPEG *Joint Photographic Experts Group*

JTM *Job Transfer and Manipulation*

LAN *Local Area Network*

LAP *Link Access Protocol*

LAPD *Link Access Protocol on the D channel*

LASER *Light Amplification by Stimulated Emission of Radiation*

LC *Late_Counter*

LCR *Least Cost Routing*

LDAP *Lightweight Directory Access Protocol*

LDP *Label Distribution Protocol*

LEC *LAN Emulation Client*

LEC-ID *LEC-Identifier*

LECS *LAN Emulation Configuration Server*

LED *Light Emitting Diode*

LER *Label Edge Router*

LES *LAN Emulation Server*

LI *Length Indicator*

LIA Liaison inter automatique

LIS *Logical IP Subnetworking*

LL Liaison louée

LLC *Logical Link Control*

LMI *Layer Management Interface*

LPDU *Link Protocol Data Unit*

LRC *Longitudinal Redundancy Check*

LS Liaison spécialisée

LSAP *Link Service Access Point*

LSDU *Link Service Data Unit*

LSP *Label Switched Path*

LSR *Label Switched Router*

LTP *Link Test Pulses*

LU *Logical Unit*

LUNI *LAN emulation User to Network Interface*

LVC Liaison virtuelle commutée

LVR Liaison virtuelle réservée

MAC *Medium Access Control*

MACF *Multiple Association Control Function*

MAN *Metropolitain Area Network*

MAU *Medium Access Unit*

MBGP MPLS BGP

MBS *Maximum Burst Size*

MCF *MAC Convergence Function*

MCR *Minimum Cell Rate*

© Dunod – La photocopie non autorisée est un délit

MCU *Multipoint Control Unit*
MDI *Medium Dependent Interface*
MHS *Message Handling System*
MIC Modulation par impulsion et codage
MII *Medium Independent Interface*
MIME *Multipourse Internet Mail Extension*
MMF *MultiMode optical Fiber*
MNP *Microcom Networking Protocol*
MOCAM Modem à carte à mémoire
MODEM Modulateur Démodulateur
MPEG *Motion Picture Expert Group*
MPLS *MultiProtocol Label Switching*
MPOA *MultiProtocol Over ATM*
MPλS *MultiProtocol Lambda Switching*
MSS *Maximum Segment Size*
MTBF *Mean Time Between Failure*
MTTR *Mean Time To Repair*
MTU *Maximum Transfert Unit*
NAV *Network Allocation Vector*
NBS National Bureau of Standards
NCP *Network Control Program*
NEXT *Near End Crosstalk loss*
NHRP *Next Hop Resolution Protocol*
NI *No Increase*
NIC *Network Information Center*
NLPID *Network Level Protocol ID*
NNI *Network Node Interface*
NNI *Network to Network Interface*
NPR *Normal Priority Request*
NRM *Normal Response Mode*
NRZ *Non Return to Zero*
NRZI *No Return to Zero Inverted*
NTI Noeud de transit international
NTT *Nippon Telephon and Telegraph Corporation*
NUA *Network User Address*
NVL Numéro de voie logique
OAM *Operation And Maintenance*
OCR *Optical Character Recogniton*
ODA *Office Document Architecture*
OFDM *Orthogonal Frequency Division Multiplexing*
OSI *Open System Interconnection*
OSNS *Open System Network Service*
OSPF *Open Short Path First*
OSTSS *Open System Transport and Session Support*
OUI *Organizational Unit Identifier*
OWS *Optical Wireless Solutions*
OXC *Optical Cross Connect*
PABX *PrivAte Branch eXchange*
PAD *Packet Assembler Disassembler*
PAF *Pre-Arbitrated Function*
PAVI Point accès vidéotex
PBX *Private Branch eXchange*
PC *Point Coordination*
PCF *Point Coordination Function*
PCH *Paging CHannel*
PCI *Protocol Control Information*
PCM *Pulse Code Modulation*
PCR *Peak Cell Rate*
PDH *Plesiochronous Digital Hierarchy*
PDU *Protocol Data Unit*
PE *Provider Edge*
PGP *Pretty Good Privacy*
PID *Protocol ID*
PIH *Protocol Identifier Header*
PIN *Personal Identifier Number*
PIN *Positive Intrinsic Negative*
PIU *Path Information Unit*
PL *PAD Length*
PL-OH *Physical Layer Over Head*
PM *Physical Medium*
PMD *Physical Medium Dependent*
PMI *Physical Medium Independent*
PNNI *Private Network to Network Interface*
POH *Path OverHead*
POSI *Promotion conference for OSI*

PPP *Point to Point Protocol*
PSK *Phase Shift Keying*
PTI *Payload Type Identifier*
Pty *Parity Bit*
PU *Physical Unit*
PVC *Permanent Virtual Circuit*
QAF *Queue Arbitrated Function*
QoS *Quality of Service*
QPSK *Quadrature Phase Shift Keying*
RA *Request Acknowledge*
RARP *Reverse Address Resolution Protocol*
RAS *Registration Admission Session*
RAS *Rivest Shamir Adleman*
RDA *Remote Database Access*
RFC *Request For Comments*
RIP *Routing Information Protocol*
RLE Réseaux locaux d'entreprise
RLE *Run Length Encoding*
RM *Ressource Management*
RNIS Réseau numérique à intégration de service
RNIS-LB RNIS large bande
RNR *Receive Not Ready*
RON/TRON Réception et transmission
ROSE *Remote Operation Service Element*
RPC *Remote Procedure Call*
RR *Receive Ready*
RR *Relative Rate*
RSVP *Ressource ReserVation Protocol*
RTC Réseau téléphonique commuté
RTCP *Real Time Control Protocol*
RTO *Retransmission Time Out*
RTP *Real Time Transport Protocol*
RTS *Real Time Stamp*
RTS *Request To Send*
RTSE *Reliable Transfer Service Element*
RTSP *Real Time Stream control Protocol*
RTT *Round Trip Time*
SAAL *Signaling AAL*
SABM *Set Asynchronous Balanced Mode*
SAC *Single Attachment Concentrator*
SACF *Simple Association Control Function*
SALL *Signaling AAL*
SAO *Simple Application Objet*
SAP *Service Access Point*
SAR *Segmentation And Reassembly*
SAS *Single Attachment Station*
SBR *Statistical Bit Rate*
SCR *Sustainable Cell Rat*e
SDA Sélection directe à l'arrivée
SDH *Synchronous Digital Hierarchy*
SDLC *Synchronous Data Link Control*
SDU *Service Data Unit*
SECAM Séquentiel couleur à mémoire
SEL *SELector field*
SF *SuperFrame*
SFD *Start Frame Delimitor*
SHTTP *Secure HTTP*
SIF *Short IFS*
SIM *Subscriber Identification Module*
SIP *Session Initiation Protocol*
SLA *Service Level Agreement*
SLIP *Serial Line Internet Protocol*
SMF *Single Mode optical Fiber*
SMON *Switched RMON*
SMS *Short Message Service*
SN *Sequence Number*
SNA *System Network Architecture*
SNACP *SubNetwork Access Protocol*
SNAP *SubNetwork Access Protocol*
SNC *Sequence Number Counter*
SNDCP *SubNetwork Dependant Convergence Protocol*
SNICP *SubNetwork Independant Convergence Protocol*
SNP *Sequence Number Protection*

© Dunod – La photocopie non autorisée est un délit

SNPA *SubNetwork Point of Attachment*
SOH *Section OverHead*
SONET *Synchronous Optical NETwork*
SPAG *Standard Promotion and Application Group*
SSAP *Source Service Access Point*
SSCS *Service Specific Convergence Sublayer*
SSCS *Service Specific Convergence Sublayer*
SSL *Secure Socket Layer*
STM *Synchronous Transfer Mode*
STP *Shielded Twisted Pairs*
SVC *Switched Virtual Circuit*
Tc *Committed rate measurement interval*
TC *Transmission Convergence*
TCCA *Time Critical Communication Architecture*
TCP *Transmission Control Protocol*
TDM *Time Division Multiplexing*
TDMA *Time Division Multiple Access*
TDP *Tag Distribution Protocol*
THT *Token Holding Timer*
TIM *Traffic Information Map*
TINA *Telecommunication Information Networking Architecture*
TNR Terminaison numérique de réseau
TP_IDL *Twisted Pair Idle Signal*
TPDDI *Twisted Pair Distributed Data Interface*
TRT *Token Rotation Timer*
TTI Taux de transfert des informations
TTL *Time To Live*
TTRT *Target Token Rotation Time*
UBR *Unspeciefied Bit Rate*
UCR *User Cell Rate*
UDP *User Datagram Protocol*
UE *User Element*
UI *Unnumbered Information*
UIT Union internationale des télécommunications
UMTS *Universal Mobile Telecommunication System*
UNI *User to Network Interface*
UPC *Usage Parameter Control*
URAD Unité de raccordement d'abonnés déportés
URL *Uniform Ressource Locator*
UTP *Unshielded Twisted Pairs*
UU *CPCS User-to-User*
VBR *Variable Bit Rate*
VBR-rt *VBR real time*
VC *Virtual Connection*
VC *Virtual Contener*
VCC *Virtual Channel Connection*
VCI *Virtual Channel Identifier*
VCS *Virtual Carrier Sense*
VIP *Visual Information Protocol*
VL Voie logique
VLAN *Virtual Local Aera Network*
VLR *Visitor Local Register*
VoD *Video on Demand*
VPI *Virtual Path Identifier*
VPN *Virtual Private Network*
VR *Virtual Route*
VRC *Vertical Redundancy Check*
VT *Virtual Terminal*
VTAM *Virtual Telecommunication Access Mode*
VTOA *Voice and Telephony Over ATM*
W3C *World Wide Web*
WAN *Wide Area Network*
WAP *Wireless Application Protocol*
WDM *Wavelength Division Mode*
WEP *Wired Equivalent Privacy*
WLAN *Wireless LAN*
WWW *World Wide Web*
XID *eXchange IDentification command*

Bibliographie

AFNOR – *Interconnexion de systèmes ouverts (OSI)*, recueil de normes françaises, AFNOR (1991).

M. BOISSEAU, M. DEMANGE, J.-M. MUNIER – *Réseaux ATM*, Éditions Eyrolles (1995).

M. BOISSEAU, M. DEMANGE, J.-M. MUNIER – *Réseaux haut débit*, Éditions Eyrolles (1992).

D. COMER – *TCP/IP : Architecture, protocoles, applications*, 4e édition, InterEditions (2001). Traduit de l'américain par J.-A. HERNANDEZ, B. JOACHIM et R. JOLY.

J. HENSHALL, S. SHAW – *OSI Les normes de communication entre systèmes ouverts*, Éditions Masson (1991).

O. HERSENT, D. GURLE, J.-P. PETIT – *La voix sur IP*, 2e édition, Éditions Dunod (2006).

D. KOFMAN, M. GAGNAIRE – *Réseaux Haut Débit*, InterEditions (1996).

C. MACCHI, J.-F. GUILBERT – *Téléinformatique*, Éditions Dunod (1989).

D. MACKINNON, W. MCCRUM, D. SHEPPARD – *Introduction à l'OSI*, AFNOR Technique (1991).

J.-L. MÉLIN – *Pratique des réseaux*, Éditions Eyrolles (1997).

H. NUSSBAUMER – *Téléinformatique*, vol. 1 à 4, Éditions Presses Polytechniques Romandes (1991).

G. PUJOLLE – *Les réseaux*, Éditions Eyrolles (2005).

G. PUJOLLE, D. SERET, D. DROMARD, E. HORLAIT – *Réseaux et Télématique*, Éditions Eyrolles (1989).

A. TANENBAUM – *Réseaux*, 3e édition, InterEditions (1996). Texte français par J.-A. HERNANDEZ et R. JOLY.

K.-L. THAI, V. VÈQUE, S. ZNATY – *Architecture des réseaux haut débit*, Éditions Hermès (1995).

L. TOUTAIN – *Réseaux locaux et Internet*, Éditions Hermès (1996).

P. ROLIN, G. MARTINEAU, L. TOUTAIN, A. LEROY – *Les réseaux, principes fondamentaux*, Éditions Hermès (1997).

P. ROLIN – *Réseaux haut débit*, Éditions Hermès (1995).

L'Echo des Recherches (périodique).

Réseaux & Télécoms, mensuel IDG Communication SA.

Revue des télécommunications (Alcatel).

Index

802.3 100BaseT 512
802.3 10Base2 508
802.3 10Base5 507
802.3 10BaseT 509

A

AAL 428
ABR (*Available Bit Rate*) 35
ACCM 278
adaptative error free 559
ADPCM 25, 677
adressage agrégé 269
adresse
    anycast 270
    de site local 268
    hiérarchique 186
    MAC 470
    privée 258
ADSL 390, 392
AFNIC 253
aire de routage 587
algorithme
    de Kruskal 758
    de Prim 757
Aloha 161
alternat 64
AMRC 648
AMRF 162, 647
AMRT 162, 648
anneau 169
annuaire 339
anycast 267
AnyLAN 482
appels
    off-net 665
    on-net 665
arbre de nommage 715
ARCEP 384
area backbone 587
ARP 298
ART 384
AS 587
ASCII 8
ASE 238
ASN-1 237
Assured Forwarding 598
ATM 379, 421
atténuation 40
audiotex 657
authentification 730

B

bande
    de base 74
    de garde 154
    passante 41
Baudot 8
BEB 504
BECN 412
BER 113
best effort 599
BGP 596
bit
    CLP 433
    DE 412
    de bourrage 113
    de parité 115
    de start 69
    de stop 69
BLR 387
BLU (Bande latérale unique) 86
Bluetooth 536
BOOTP 301
boucle locale 383
    radio 387
BPSK (*Binary Phase Shift Keying*) 87
brasseurs 425
BRI 629
broadcast 185, 261, 472
bruit 4
    de quantification 93
BTS 644
bus 168

C

câble coaxial 48
CAC 428, 433
Call manager 693
canal
    B 627
    D 627
    E 634
    sémaphore 625
carrier extention 513
CAS 625
CATV 49
CBR (*Constant Bit Rate*) 35, 430
CCBNT 630
CCBT 631
CCITT N° 7 632

CCS 625
CDMA 519, 648
CDV 433
CELP 25, 678
CES 684
CHAP 281, 738
chiffrement
    asymétrique 733
    symétrique 731
chrominance 17
CIDR 263
CIF 20, 661
CIR 414
circuit virtuel 180
classe d'adressage 255
classe de services 431
    1 - Platinium 599
    2 - Gold 599
    3 - Silver 599
    4 - Bronze 599
Classical IP 485
clé
    asymétrique 733
    publique 733
    secrète 733
CLLM 418
CLP 427, 433
CLR 433
CMIP 712
CMIS 711
codage
    à la source 6
    d'entropie 22
    en ligne 74
    en longueur de plage 22
    Manchester 75
    Manchester différentiel 75
    par substitution 22
code
    ASCII 8
    Baudot 8
    bipolaire 76
    Delay Mode 76
    Huffman 11
    Huffman modifié 37
    Miller 76
collision 466
commutateur 556
commutation
    de cellules 174
    de circuits 171
    de messages 172
    de paquets 173
concentrateur 151
cône d'acceptance 51
confidentialité 730
connexion de transport 320
container 371
contrôle
    d'admission 204
    de congestion 326
    de flux 131, 327
    de flux dynamique 132
    de flux explicite 328
    de flux implicite 132
COPS 602
CoS 429, 597
couche
    adjacente 215
    application 238
    homologue 215
    liaison de données 226
    physique 225
    présentation 236
    réseau 227
    session 235
    transport 231
courants porteurs 393
CPL 393
CRC 117
critère de Nyquist 79
CRTP 690
cryptographie 730
CS-ACELP 26
CSMA/CA 470, 520
CSMA/CD 470, 501
CSMA/CR 634
CSTA 659
CT1 649
CTD 432
CTI 659
CTS 530
C*ut through* 559
CVC 181
CVP 181

D

datagramme
    IP 289
    IPv6 305
DCE (*Data Circuit Equipment*) 63
DCF 528, 529
DCT 28
DE 412
débit binaire 4
dégroupage
    partiel 384
    total 384
délai de paquétisation 207
démarrage lent 329
déni de service 730
Dense WDM 155
DES 732
désaveu 730
détection d'erreur par clé calculée 115
DHCP 301, 302
diaphonie 46
Differentiated Services 598
Diffie-Hellman 734
DiffServ 291, 598
diffusion
    dirigée 257
    générale 257
DIFS 529
Discret Cosinus Transform 28
distorsion 40
DIT 346
DLCI 412
DMT 390
DMZ 745
DNS 340
DQDB 495
DSI 677
DSSS 164
DTE (*Data Terminal Equipment*) 63
DTMF 624
duplexing 724
DVMRP 606
DWDM 155, 373

E

E.164 623
E1 669
E&M 668
EBCDIC 8
écho 44
EDGE 650
effet Doppler 56

EGP 198, 583, 587
EIFS 529
EIR 414
ELAN 489
embrouillage 89
encapsulation 215, 222, 572
entropie 10
ERBdB 79
Erlang 150, 663, 761
étalement de spectre 164
état des liens 586
ETCD 63
Ethernet full duplex 560
EtherType 251
étoile 169
ETTD 63
EUI-64 268
Expedited Forwarding 599

F

F/TDMA 519
fading 55
faisceaux hertziens 57, 61
fanion 111
Fast Ethernet 511
Fast forward 559
fax 680
FCS (*Frame Check Sequence*) 137
FDDI 492
FDM 154
FDMA 162, 519, 647
FEC 445
FECN 412
fenêtre 128
  d'anticipation 131
  de collision 503
  stupide 328
fermeture douce 323
Fext 46
FHSS 164, 523
fiabilité 728
fibre
  à gradient d'indice 52
  à saut d'indice 51
  optique 49
Fibre Channel 496
FIFO 600
firewall 744
FLIB 445
fondamental 40
Fourier 40
FQDN 342
fragmentation 294
Frame Relay 378, 411
fréquence de coupure 42
FRF11 685
FRF12 685
FTP 47, 350, 467
  anonyme 350
full duplex 64, 88, 235
FXO 683
FXS 683

G

G.711 27, 677, 678
G.721 27, 678
G.722 27, 678
G.722-1 27, 678
G.723 27, 678
G.723-1 27, 678
G.726 27, 677, 678
G.727 27, 678
G.728 27, 678
G.729 27, 678
G.729 a 27
G.Lite 392
GARP 560
gatekeeper 694
GbE 513
giga-routeur 582
Gigabit Ethernet 513
gigue 365, 679
GMRP 561
GPRS 649
GPS 652
GRE 315
GSM 643, 649
GVRP 561, 566

H

H.225 694
H.245 694
H.261 661
H.323 694
half duplex 64
Hamming 120
handover 521, 647
harmoniques 40
Hayes 90
HDLC (*High Level Data Link Control*) 136
HDSL 392
HEC 425
Hello 590
HiPPI 496
HLR 644
horizon coupé 584
Host_ID 254
HTML 357
HTTP 357
hub 509
hyperviseurs 719

I

IAB 253
IANA 253
ICANN 341
ICI 217
ICMP 295, 741
IDSL 392
IEEE 802.11 522
IEEE 802.12 482
IEEE 802.15-1 536
IEEE 802.1p/Q 564
IEEE 802.3 1000BaseT 514
IEEE 802.3ae 517
IEEE 802.3af 692
IEEE 802.4 480
IEEE 802.5 477
IETF 253
IFG 505
IGMP 605
IGP 197, 583
IGRP 585
image vidéo 15
impédance caractéristique 44
Integrated Services 597
intégrité 730
intensité de trafic 148, 761
intervalle de temps 156
IntServ 597
IP multicast 603
IP Precedence 291, 597
IPSec 738
IPv6 266
ISDN 242, 626
ISN 322
ISP 94
IT 156

© Dunod – La photocopie non autorisée est un délit

J

jeton 478
jitter 365
jonction 96
JPEG 28

K

Krustal 757

L

LAN 166
LAN Emulation 487
LAP-B 110, 143, 399
LAP-D 633, 636
large bande 84
largeur de bande 42
LASER 50
LCP 278
LD-CELP 26
LDAP 347
LDP 452
LED 50
LEO 652
LER 445
LIA 668
liaison
- à l'alternat 64
- de données 63
- *full duplex* 64
- *half duplex* 64
- multipoints 110
- point à point 110
- simplex 64

link status 197, 510
lissage du trafic 205
LLC 473
LLC1 474
LLC2 475
LLC3 475
LMI 418
LSDU 474
LSP 445
LSR 444
luminance 17

M

MAC 469
macroblocs 30
maillé 169
maintenabilité 728
maître/esclave 110
MAN 166
MAQ 88
masque de sous-réseau 260
MBS 433
MCR 433
messagerie vocale 657
métrique 192
MGCP 701
MIB 710
MIC 23
MICDA 25
middleware 353
Minitel 86
mirroring 724
MLP 398
MLPPP 284, 691
mode
- circuit 760
- connecté 180
- datagramme 179, 224
- non connecté 180
- orienté connexion 180
- paquet 763

modèle OSI 213
modem 84
- temps de retournement 102

modulation 84
- d'amplitude 84
- de fréquence 84
- de phase 84

MOS 27, 678
mot de verrouillage de trame 369
MPEG 19, 28
MPLS 201, 443
MPOA 490
MPPP 688
MSS 252, 333
MTBF 728
MTTR 728
MTU 202
multicast 185, 256, 472
multiplexage
- d'étiquette 158
- de position 156
- fréquentiel 154
- par étiquette 174
- temporel 154

multiplexeur 153
MUX 153

N

NAPT 743
NAS 724
NAT 258, 743
NAV 530
NCP 282
Net_ID 254
Next 46
NLA_id 269
NLPID 575
NNI 426
nommage 188
NOS 463
notification d'erreur 225
NRZ (*No Return to Zero*) 75
null modem 102
numérotation fréquentielle 624

O

OEM 54
OFDM 525
Olympic Service 598
ondes électromagnétiques 54
onduleurs 727
OSPF 586
OUI 471

P

PABX 655
PAP 281, 738
pare-feu 744
PAT 743
Pause 514
PAVI 152
PCF 528
PCI 217
PCR 433
PDH 160, 368
PIFS 529
piggybacking, 141
PIM 606
PING 296
PKI 737
PNNI 435
PoE 692

poison reverse 584
polling/selecting 111
ponts 546, 578
  transparents 547
PoP 381
port 251, 320
  bien connu 321
  référencé 321
PPP 276
PPPoA 285, 391
PPPoE 285, 391
Premium Service 599
PRI 629
Prim 757
primitives de service 215
protocole 251
  à anticipation 126
  D 632, 638
PSTN 617
PVC 181

Q

Q-SIG 673
Q.23 624, 668
Q.931 638, 694
QAM (*Quadrature Amplitude Modulation*) 88
QCIF 20, 661
QoS 225, 438, 597
qualité de service 33, 597
quantité d'information 7

R

RAID 724
raie de fréquence 41
rapidité de modulation 80
RARP 299
RAS 694, 747
RED 600
redirecteur 464
rejet
  sélectif 129
  simple 129
relais de trames 378
relation de Shannon 83
répéteurs 577
réseau
  à commutation 165, 171
  de desserte 756
  dorsal 756
  en bus 168
  maillé 169
résolution d'adresses 298
RFC 253
RFC 1490 575
RFC 1356 581
RFC 1483 576
RFC 2338 725
RIP 583
RIPE 253
RMON MIB 714
RNIS 242, 626
roaming 521, 648
RON/TRON 668
Round Robin 601
routage
  à état des liens 194
  aire de 587
  au moindre coût 192
  inter-domaine 583
  intra-domaine 583
  par inondation 191
  par la source 553
  statique 190
  vecteur-distance 192, 583
routeur 579
  désigné 588
  giga- 582
RPC 354
RPIS 665
RS 232 96
RSA 733, 864
RSVP 597, 688
RTC 617
RTCP 683, 687, 690
RTO 121, 141, 326
RTP 687, 689
RTS 530
RTT 124, 326

S

S-HTTP 738
SAN 724
SAP 216
SAPI 633
SCR 433
SCTP 703
SDA 632
SDH 160, 370
SDSL 392
segmentation 223
sélection directe à l'arrivée 632
Send and Wait 121
Service Level Agreement 414
services supports 630
SET 750
Shannon 13
SIFS 529
signalisation 134
  CAS 669
  CCS 671
  par canal sémaphore 136, 671
  voie par voie 136, 625, 668, 669
SIM 645
SIP 699
SLA 414, 599, 602
SLA_id 268
SLIP 274
SMI 712, 714
SMON 714
SMS 645
SNAP 476, 575, 607
SNMP 714, 717
SNPA 227
SNR 5
SNR (*Signal Noise Ratio)* 83
socket 320, 356
SONET 371
sous-réseau 259
SPA 663
Spanning Tree Protocol 550
SPB 663
split horizon 584
SS7 640
SSL 739
store and forward 559
STP 47, 550
subnetting 259
sûreté de fonctionnement 723
SVC 181
Switched Ethernet 556
synchronisation 66
  caractère 112
syntaxe de transfert 237
système autonome 197, 587

© Dunod – La photocopie non autorisée est un délit

T

T.120 694
T0 629
T1 370, 629, 670
T2 629
table
    d'acheminement 189
    de routage 189
TAPI 659
taux
    d'activité 148
    d'erreur binaire 113
    de compression 22
TCP 319
TDMA 162, 519, 648
TEI 633, 637
télécopie 680
téléservices 630, 656
Telnet 351
TELR 681
temps de retournement du modem 102
terre
    de protection 73
    de signalisation 73
TFTP 348
Time slot 162
TLA_id 269
TLD 341
ToIP 687
Token 478, 479
Token Bus 480
Token Ring 477
tolérance de panne 724
topologie 168
    en anneau 169
    étoile 169
Traceroute 297
translation d'adresses 742
transmission
    analogique 84
    asynchrone 66, 69
    parallèle 65
    série 66
    synchrone 66, 71
transparence
    au caractère 112
    binaire 112
TSAPI 659
tunneling 572

U

UADSL 392
UBR (*Unspecified Bit Rate*) 35
UDP 335
UMTS 650, 651
UNI 426
unicast 185, 471
Unicode 12
UPC 434
URA 620
URAD 620, 666
URL 357
UTP 47, 467, 469

V

V.22 89
V.24 96, 98
V.28 97
V.34 93
V.42 89
V.90 93
VAD 682
valence 83
VBR 430
VBR-nrt (*Variable Bit Rate non real time*) 35
VBR-rt (*Variable Bit Rate*) 35
VCI 424
VDSL 392
Vector distance 197
vélocité 45
VFRAD 685
vidéotex 152
visiophonie 660
VLAN 562
VLR 644
VoFR 685
VoIP 687
voix paquétisée 676
VPI 424
VPN 166, 183, 454, 747
    sécurisé 747
VRID 725
VRRP 385, 725
VTOA 684

W

WAN 166
WAP 649
WDM 155, 373
Well known ports 321
WFQ 600
Wi-Fi 521
WiMax 388
WRED 600
WRR 601
WWW 357

X

X-Modem 70
X.21 96, 103
X.21bis 96
X.25 375
X.25 PLP 402
X.500 346
XON-XOFF 70

Y

Y-Modem 70

Z

zone 587

SCIENCES SUP



2e édition

Claude Servin

Préface de Jean-Pierre Arnaud

RÉSEAUX & TÉLÉCOMS

Cet **ouvrage de référence**, clair et complet, répond à la nécessité d'explorer et de comprendre tous les aspects des technologies des réseaux et télécoms.

Issu du cours enseigné par l'auteur au **CNAM de Paris**, il explique les notions théoriques indispensables et décrit avec précision toutes les solutions couramment mises en œuvre dans les entreprises et par les opérateurs. Les techniques les plus récentes (comme IPv6, MPLS, les réseaux sans fil ou les VLAN…) sont traitées, mais aussi d'autres plus anciennes (comme X.25, ATM ou Frame Relay) qui continuent à être encore largement présentes dans les entreprises. La téléphonie d'entreprise, qui intègre de plus en plus les techniques multimédia et notamment la voix sur IP, y est décrite en détail.

Cette édition 2006/2007 s'enrichit de compléments sur MPLS (les infrastructures hauts débits des opérateurs), la voix sur IP et le Wi-Fi, ainsi que de nouveaux exercices corrigés. Elle rassemble **129 exercices avec leur corrigé détaillé**, plus de 1 000 schémas et images ainsi qu'un glossaire technique des termes incontournables.

Codage des données de la voix et de la vidéo • Techniques de transmission • Protocoles • Concentrateurs et multiplexeurs • Architectures protocolaires • Couches OSI • TCP/IP • X.25 • Frame Relay • ATM • Boucles locales • Ethernet • Wi-Fi • Token Ring • VLAN • FDDI • DQDB • Ponts et routeurs • RNIS • PABX • Réseaux voix/données • Voix sur IP • MPLS • VPN • Sécurité • Administration

Public : Élèves ingénieurs, étudiants en licence et en master, ingénieurs en entreprise ou en formation continue trouveront ici les éléments indispensables à la compréhension, la conception et la mise en œuvre des réseaux modernes.

CLAUDE SERVIN

Longtemps responsable réseaux et télécoms au sein du ministère de la Défense, il enseigne aujourd'hui au Conservatoire national des Arts et Métiers (CNAM) de Paris.

MATHÉMATIQUES
PHYSIQUE
CHIMIE
SCIENCES DE L'INGÉNIEUR
INFORMATIQUE
SCIENCES DE LA VIE
SCIENCES DE LA TERRE

9 782100 491483

6461537
ISBN 978-2-10-049148-3

www.dunod.com

DUNOD