



# Communication Multimédia

Mustafa Ali Hassoune  
Département d'informatique  
Université des Sciences et de la Technologie d'Oran



# Réseaux et Streaming

## Réseaux et Streaming

Dans un système de streaming, le terme réseau englobe les infrastructures matérielles et protocoles logiciels permettant de transmettre au serveur les commandes des utilisateurs et de délivrer aux clients les données audiovisuelles choisies tout en respectant leur isochronisme.

# Communications multimédias sur les réseaux



# Réseaux

## Protocoles dédiés aux AMD

RTP

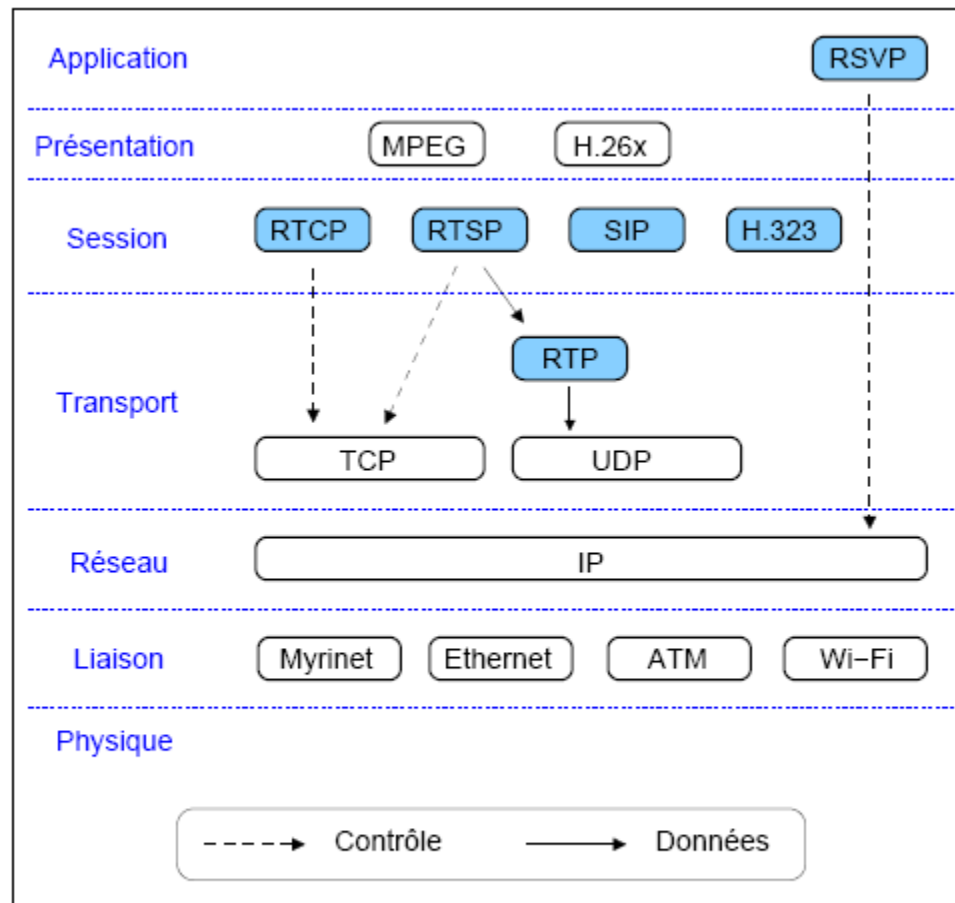
RTSP

SIP

RTCP

RSVP

# Réseaux et Streaming



Classement des protocoles de streaming dans les couches du modèle OSI.

# Réseaux et Streaming

## SIP

Session Initiation Protocol (SIP) est un protocole standard ouvert de gestion de sessions souvent utilisé dans les télécommunications multimédia (son, image, etc.) Il est depuis 2007 le plus courant pour la téléphonie par internet (la VoIP).

# Session Initiation Protocol

- The Session Initiation Protocol (SIP) is a signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video and messaging applications. SIP is used for signaling and controlling multimedia communication sessions in applications of Internet telephony for voice and video calls, in private IP telephone systems, in instant messaging over Internet Protocol (IP) networks as well as mobile phone calling over LTE (VoLTE).

# Session Initiation Protocol

- The protocol defines the specific format of messages exchanged and the sequence of communications for cooperation of the participants. SIP is a text-based protocol, incorporating many elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP). A call established with SIP may consist of multiple media streams, but no separate streams are required for applications, such as text messaging, that exchange data as payload in the SIP message.



# Session Initiation Protocol

- SIP works in conjunction with several other protocols that specify and carry the session media. Most commonly, media type and parameter negotiation and media setup is performed with the Session Description Protocol (SDP), which is carried as payload in SIP messages. SIP is designed to be independent of the underlying transport layer protocol, and can be used with the User Datagram Protocol (UDP), the Transmission Control Protocol (TCP), and the Stream Control Transmission Protocol (SCTP). For secure transmissions of SIP messages over insecure network links, the protocol may be encrypted with Transport Layer Security (TLS). For the transmission of media streams (voice, video) the SDP payload carried in SIP messages typically employs the Real-time Transport Protocol (RTP) or the Secure Real-time Transport Protocol (SRTP).

# SIP: History

- SIP was originally designed by Mark Handley, Henning Schulzrinne, Eve Schooler and Jonathan Rosenberg in 1996. The protocol was standardized as RFC 2543 in 1999. In November 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IP Multimedia Subsystem (IMS) architecture for IP-based streaming multimedia services in cellular networks. In June 2002 the specification was revised in RFC 3261 and various extensions and clarifications have been published since.
- SIP was designed to provide a signaling and call setup protocol for IP-based communications supporting the call processing functions and features present in the public switched telephone network (PSTN) with a vision of supporting new multimedia applications. It has been extended for video conferencing, streaming media distribution, instant messaging, presence information, file transfer, Internet fax and online games.
- SIP is distinguished by its proponents for having roots in the Internet community rather than in the telecommunications industry. SIP has been standardized primarily by the IETF, while other protocols, such as H.323, have traditionally been associated with the International Telecommunication Union (ITU).

# SIP: Protocol Operation

- SIP is only involved for the signaling operations of a media communication session and is primarily used to set up and terminate voice or video calls. SIP can be used to establish two-party (unicast) or multiparty (multicast) sessions. It also allows modification of existing calls. The modification can involve changing addresses or ports, inviting more participants, and adding or deleting media streams. SIP has also found applications in messaging applications, such as instant messaging, and event subscription and notification.
- SIP works in conjunction with several other protocols that specify the media format and coding and that carry the media once the call is set up. For call setup, the body of a SIP message contains a Session Description Protocol (SDP) data unit, which specifies the media format, codec and media communication protocol. Voice and video media streams are typically carried between the terminals using the Real-time Transport Protocol (RTP) or Secure Real-time Transport Protocol (SRTP).

# SIP: Protocol Operation

- Every resource of a SIP network, such as user agents, call routers, and voicemail boxes, are identified by a Uniform Resource Identifier (URI). The syntax of the URI follows the general standard syntax also used in Web services and e-mail. The URI scheme used for SIP is sip and a typical SIP URI has the form sip:username@domainname or sip:username@hostport, where domainname requires DNS SRV records to locate the servers for SIP domain while hostport can be an IP address or a fully qualified domain name of the host and port. If secure transmission is required, the scheme sips is used.
- SIP employs design elements similar to the HTTP request and response transaction model. Each transaction consists of a client request that invokes a particular method or function on the server and at least one response. SIP reuses most of the header fields, encoding rules and status codes of HTTP, providing a readable text-based format.

# SIP: Protocol Operation

- SIP can be carried by several transport layer protocols including Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Stream Control Transmission Protocol (SCTP). SIP clients typically use TCP or UDP on port numbers 5060 or 5061 for SIP traffic to servers and other endpoints. Port 5060 is commonly used for non-encrypted signaling traffic whereas port 5061 is typically used for traffic encrypted with Transport Layer Security (TLS).
- SIP-based telephony networks often implement call processing features of Signaling System 7 (SS7), for which special SIP protocol extensions exist, although the two protocols themselves are very different. SS7 is a centralized protocol, characterized by a complex central network architecture and dumb endpoints (traditional telephone handsets). SIP is a client-server protocol of equipotent peers. SIP features are implemented in the communicating endpoints, while the traditional SS7 architecture is in use only between switching centers.

# SIP: Network Elements

- The network elements that use the Session Initiation Protocol for communication are called *SIP user agents*. Each *user agent* (UA) performs the function of a *user agent client* (UAC) when it is requesting a service function, and that of a *user agent server* (UAS) when responding to a request. Thus, any two SIP endpoints may in principle operate without any intervening SIP infrastructure. However, for network operational reasons, for provisioning public services to users, and for directory services, SIP defines several specific types of network server elements. Each of these service elements also communicates within the client-server model implemented in user agent clients and servers.

# SIP: Network Elements : **User agent**

- A user agent is a logical network end-point that sends or receives SIP messages and manages SIP sessions. User agents have client and server components. The user agent client (UAC) sends SIP requests. The user agent server (UAS) receives requests and returns a SIP response. Unlike other network protocols that fix the roles of client and server, e.g., in HTTP, in which a web browser only acts as a client, and never as a server, SIP requires both peers to implement both roles. The roles of UAC and UAS only last for the duration of a SIP transaction.
- A SIP phone is an IP phone that implements client and server functions of a SIP user agent and provides the traditional call functions of a telephone, such as dial, answer, reject, call hold, and call transfer. SIP phones may be implemented as a hardware device or as a softphone. As vendors increasingly implement SIP as a standard telephony platform, the distinction between hardware-based and software-based SIP phones is blurred and SIP elements are implemented in the basic firmware functions of many IP-capable communications devices such as smartphones

# SIP: Network Elements : **User agent**

- In SIP, as in HTTP, the user agent may identify itself using a message header field (User-Agent), containing a text description of the software, hardware, or the product name. The user agent field is sent in request messages, which means that the receiving SIP server can evaluate this information to perform device-specific configuration or feature activation. Operators of SIP network elements sometimes store this information in customer account portals, where it can be useful in diagnosing SIP compatibility problems or in the display of service status.



# SIP: Network Elements : Proxy Server

- A proxy server is a network server with UAC and UAS components that functions as an intermediary entity for the purpose of performing requests on behalf of other network elements. A proxy server primarily plays the role of routing, meaning that its job is to ensure that a request is sent to another entity closer to the targeted user. Proxies are also useful for enforcing policy, such as for determining whether a user is allowed to make a call. A proxy interprets, and, if necessary, rewrites specific parts of a request message before forwarding it.
- SIP proxy servers that route messages to more than one destination are called forking proxies. The forking of SIP requests means that multiple dialogs can be established from a single request. This explains the need for the two-sided dialog identifier; without a contribution from the recipients, the originator could not disambiguate the multiple dialogs established from a single request.
- SIP forking refers to the process of "forking" a single SIP call to multiple SIP endpoints. This is a very powerful feature of SIP. A single call can ring many endpoints at the same time. SIP forking allows a desk phone ring at the same time as a mobile, allowing a call to be taken from either device.

# SIP: Network Elements : Registrar

- SIP user agent registration to SIP registrar with authentication.
- A registrar is a SIP endpoint that provides a location service. It accepts REGISTER requests, recording the address and other parameters from the user agent. For subsequent requests it provides an essential means to locate possible communication peers on the network. The location service links one or more IP addresses to the SIP URI of the registering agent. Multiple user agents may register for the same URI, with the result that all registered user agents receive the calls to the URI.
- SIP registrars are logical elements, and are often co-located with SIP proxies. To improve network scalability, location services may instead be located with a redirect server.

# SIP: Network Elements : **Gateway**

- Gateways can be used to interconnect a SIP network to other networks, such as the public switched telephone network, which use different protocols or technologies.

# SIP messages

- **Requests**
- **Reponses**

# SIP messages : **Requests**

- Requests initiate a functionality of the protocol. They are sent by a user agent client to the server, and are answered with one or more SIP responses, which return a result code of the transaction, and generally indicate the success, failure, or other state of the transaction.

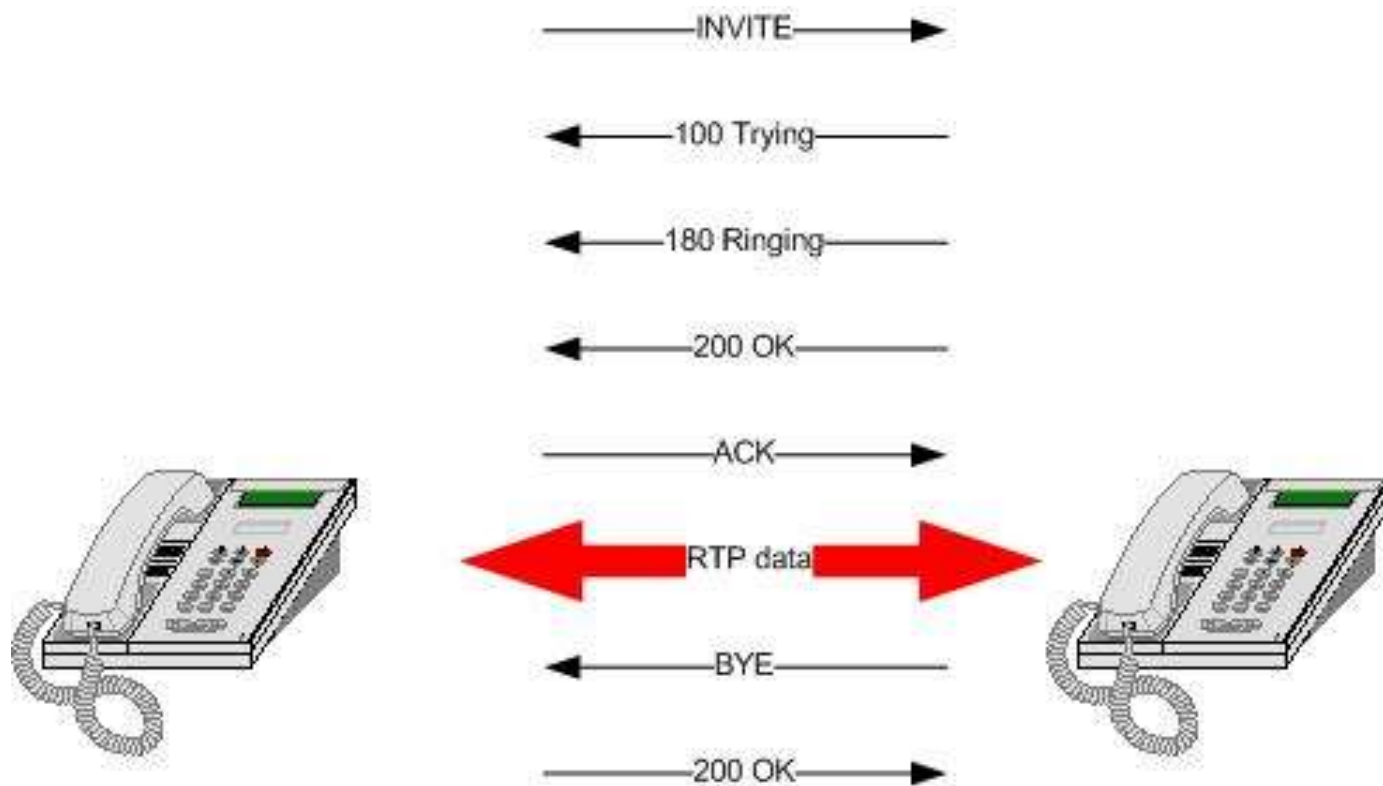
# SIP messages : Requests

Request name	Description	Notes	RFC references
<b>REGISTER</b>	Register the URI listed in the To-header field with a location server and associates it with the network address given in a <i>Contact</i> header field.	The command implements a location service.	<a href="#">RFC 3261</a>
<b>INVITE</b>	Initiate a dialog for establishing a call. The request is sent by a user agent client to a user agent server.	When sent during an established dialog ( <i>reinvite</i> ) it modifies the sessions, for example placing a call on hold.	<a href="#">RFC 3261</a>
<b>ACK</b>	Confirm that an entity has received a final response to an INVITE request.		<a href="#">RFC 3261</a>
<b>BYE</b>	Signal termination of a dialog and end a call.	This message may be sent by either endpoint of a dialog.	<a href="#">RFC 3261</a>
<b>CANCEL</b>	Cancel any pending request.	Usually means terminating a call while it is still ringing, before answer.	<a href="#">RFC 3261</a>
<b>UPDATE</b>	Modify the state of a session without changing the state of the dialog.		<a href="#">RFC 3311</a>
<b>REFER</b>	Ask recipient to issue a request for the purpose of call transfer.		<a href="#">RFC 3515</a>
<b>PRACK</b>	Provisional acknowledgement.	PRACK is sent in response to provisional response (1xx).	<a href="#">RFC 3262</a>
<b>SUBSCRIBE</b>	Initiates a subscription for notification of events from a notifier.		<a href="#">RFC 6665</a>
<b>NOTIFY</b>	Inform a subscriber of notifications of a new event.		<a href="#">RFC 6665</a>
<b>PUBLISH</b>	Publish an event to a notification server.		<a href="#">RFC 3903</a>
<b>MESSAGE</b>	Deliver a text message.	Used in instant messaging applications.	<a href="#">RFC 3428</a>
<b>INFO</b>	Send mid-session information that does not modify the session state.	This method is often used for DTMF relay.	<a href="#">RFC 6086</a>
<b>OPTIONS</b>	Query the capabilities of an endpoint.	It is often used for NAT <a href="#">keepalive</a> purposes.	<a href="#">RFC 3261</a>

# SIP messages : Responses

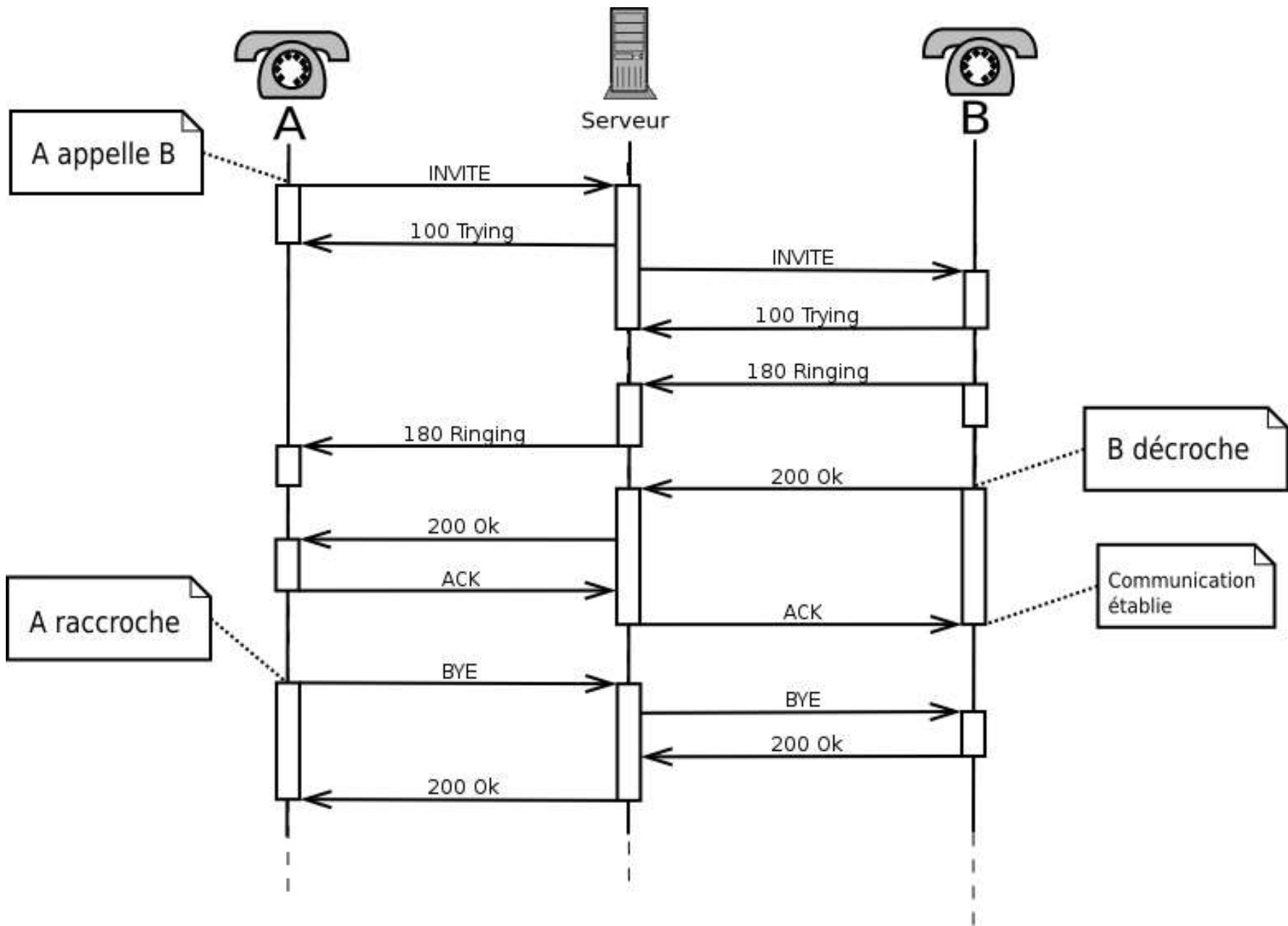
Responses are sent by the user agent server indicating the result of a received request. Several classes of responses are recognized, determined by the numerical range of result codes:

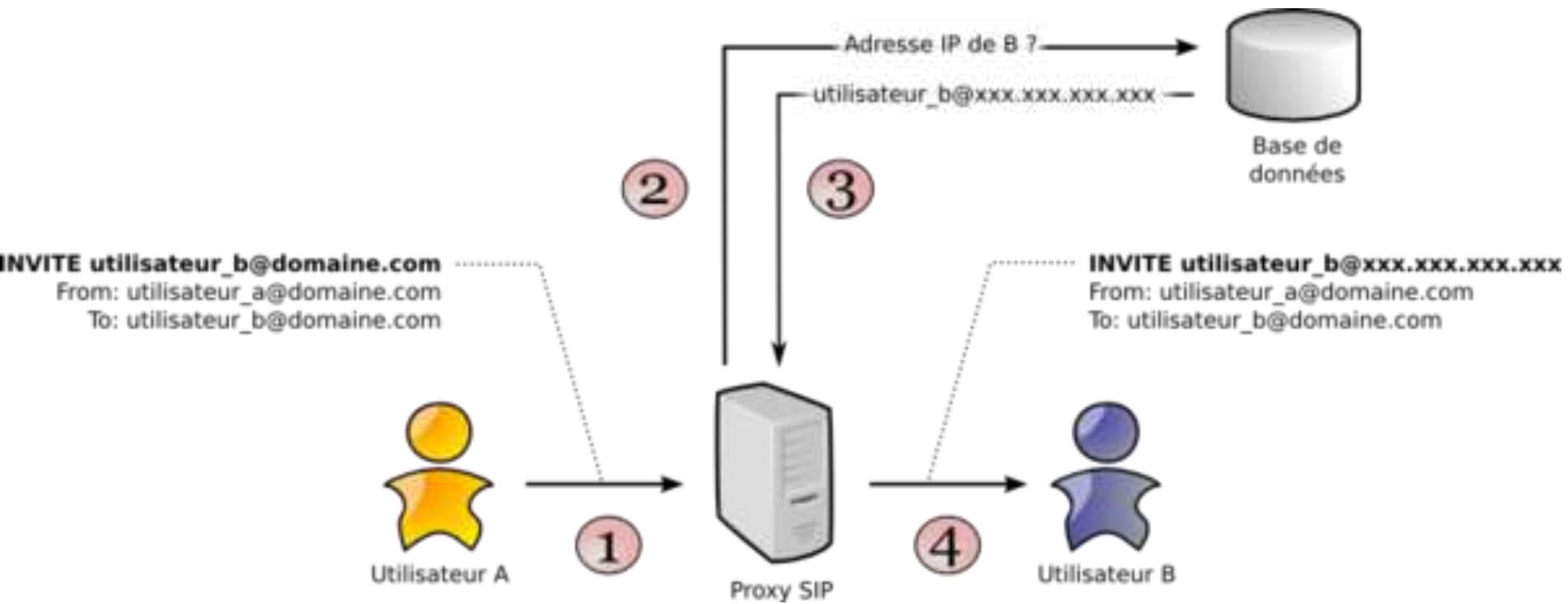
- 1xx: Provisional responses to requests indicate the request was valid and is being processed.
- 2xx: Successful completion of the request. As a response to an INVITE, it indicates a call is established. The most common code is 200, which is an unqualified success report.
- 3xx: Call redirection is needed for completion of the request. The request must be completed with a new destination.
- 4xx: The request cannot be completed at the server for a variety of reasons, including bad request syntax (code 400).
- 5xx: The server failed to fulfill an apparently valid request, including server internal errors (code 500).
- 6xx: The request cannot be fulfilled at any server. It indicates a global failure, including call rejection by the destination.



A SIP call session between 2 phones – without SIP PROXY







# SDP : Session Description Protocol

- The Session Description Protocol (SDP) is a format for describing streaming media communications parameters. The IETF published the original specification as a Proposed Standard in April 1998, and subsequently published a revised specification as RFC 4566 in July 2006.
- SDP is used for describing multimedia communication sessions for the purposes of session announcement, session invitation, and parameter negotiation. SDP does not deliver any media by itself but is used between endpoints for negotiation of media type, format, and all associated properties. The set of properties and parameters are often called a session profile.
- SDP is designed to be extensible to support new media types and formats. SDP started off as a component of the Session Announcement Protocol (SAP), but found other uses in conjunction with Real-time Transport Protocol (RTP), Real-time Streaming Protocol (RTSP), Session Initiation Protocol (SIP) and even as a standalone format for describing multicast sessions.

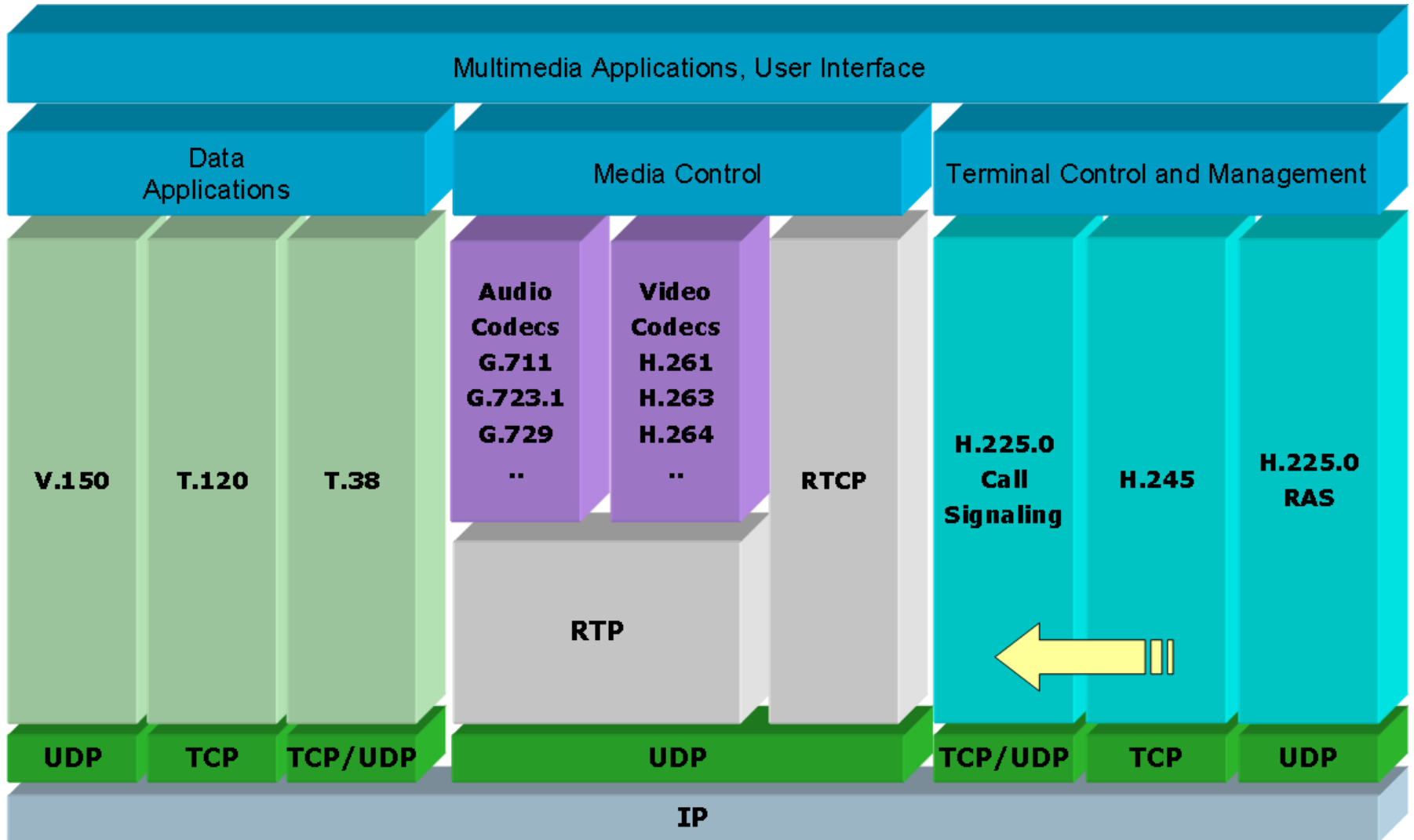
# RFC SIP

- <https://datatracker.ietf.org/>

# SIP SDP RTP RTCP over JAVA

<https://github.com/jitsi/jitsi/tree/master/src/net/java/sip/communicator/impl/protocol/sip>

# H323



# H323

H.323 is a system specification that describes the use of several ITU-T and IETF protocols. The protocols that comprise the core of almost any H.323 system are:

- H.225.0 Registration, Admission and Status (RAS), which is used between an H.323 endpoint and a Gatekeeper to provide address resolution and admission control services.
- H.225.0 Call Signaling, which is used between any two H.323 entities in order to establish communication. (Based on Q.931)
- H.245 control protocol for multimedia communication, which describes the messages and procedures used for capability exchange, opening and closing logical channels for audio, video and data, control and indications.
- Real-time Transport Protocol (RTP), which is used for sending or receiving multimedia information (voice, video, or text) between any two entities.
- Many H.323 systems also implement other protocols that are defined in various ITU-T Recommendations to provide supplementary services support or deliver other functionality to the user. Some of those Recommendations are:[citation needed]
- H.235 series describes security within H.323, including security for both signaling and media.
- H.239 describes dual stream use in videoconferencing, usually one for live video, the other for still images.
- H.450 series describes various supplementary services.
- H.460 series defines optional extensions that might be implemented by an endpoint or a Gatekeeper, including ITU-T Recommendations H.460.17, H.460.18, and H.460.19 for Network address translation (NAT) / Firewall (FW) traversal.

# H323

H.323 utilizes both ITU-defined codecs and codecs defined outside the ITU. Codecs that are widely implemented by H.323 equipment include:

Audio codecs: G.711, G.729 (including G.729a), G.723.1, G.726, G.722, G.728, Speex, AAC-LD

Text codecs: T.140

Video codecs: H.261, H.263, H.264

All H.323 terminals providing video communications shall be capable of encoding and decoding video according to H.261 QCIF. All H.323 terminals shall have an audio codec and shall be capable of encoding and decoding speech according to ITU-T Rec. G.711. All terminals shall be capable of transmitting and receiving A-law and  $\mu$ -law. Support for other audio and video codecs is optional.[6]



# Réseaux et Streaming

## RSVP

### Le protocole de réservation de ressources

Permet aux applications de réserver dynamiquement des ressources dans un réseau IP, afin de satisfaire leurs besoins en bande passante, délais de transfert autorisés,...

Il émet périodiquement des messages de réservation, ou de libération de ressources.

# Réseaux et Streaming

## RTSP

RTSP ou Real Time Streaming Protocol (protocole de streaming temps-réel) est un protocole de communication de niveau applicatif (niveau 7 du modèle OSI) destiné aux systèmes de streaming média. Il permet de contrôler un serveur de média à distance, offrant des fonctionnalités typiques d'un lecteur vidéo telles que « lecture » et « pause », et permettant un accès en fonction de la position temporelle.

RTSP ne transporte pas les données elles-mêmes et doit être associé à un protocole de transport comme RTP ou RDT de RealNetworks pour cette tâche.

# RTSP

"RTSP acts as a network remote  
Control for Multimedia Servers"

# Réseaux et Streaming

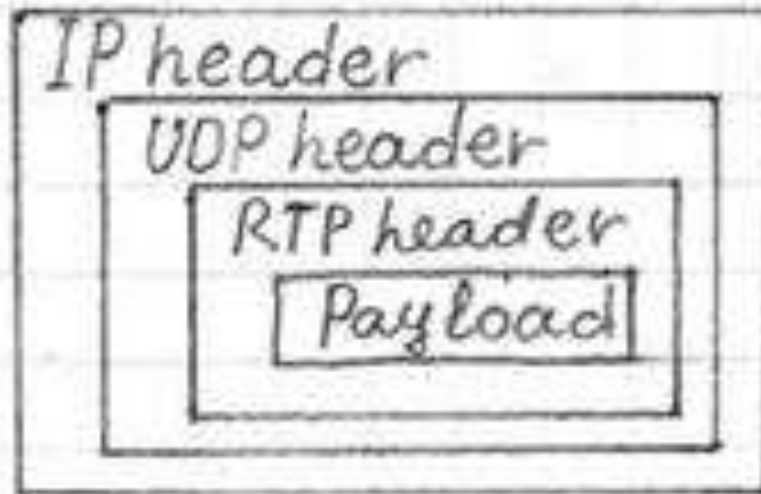
## RTP/RTCP

RTP est un protocole proposé pour transmettre des médias continus comme l'audio et la vidéo. Il est considéré comme un protocole de transport, mais il constitue en réalité une surcouche du protocole UDP.

Ceci signifie que les paquets UDP sont encapsulés dans des paquets RTP qui contiennent, entre autre, une entête permettant l'identification du contenu du flux transporté, un numéro de séquence et une référence au temps.

Il fournit des services tels que la détection de pertes et la sécurité. La référence au temps peut être utilisée pour déterminer quand doit être diffusé un paquet par rapport à un autre mais aussi pour synchroniser différents flux.

# *RTP packet encapsulation*



# Réseaux et Streaming

## RTP/RTCP

Cette possibilité peut être utilisée afin de gérer les transmissions par exemple en informant l'émetteur sur les propriétés du canal de transmission, sur l'état du tampon du récepteur ou pour demander des changements de format ou de débit des données.

Ces mécanismes peuvent être réalisés grâce aux informations fournies par le protocole RTCP (Real-Time Transport Control Protocol) qui va de pair avec RTP. RTP et RTCP sont utilisés par un grand nombre d'AMD à travers l'Internet.

# RTCP

- The RTP Control Protocol (RTCP) is an upper-layer companion protocol that allows monitoring of the data delivery. It's designed to give feedback on the quality of data transmission and information about participants in the on-going session.

# IPV6

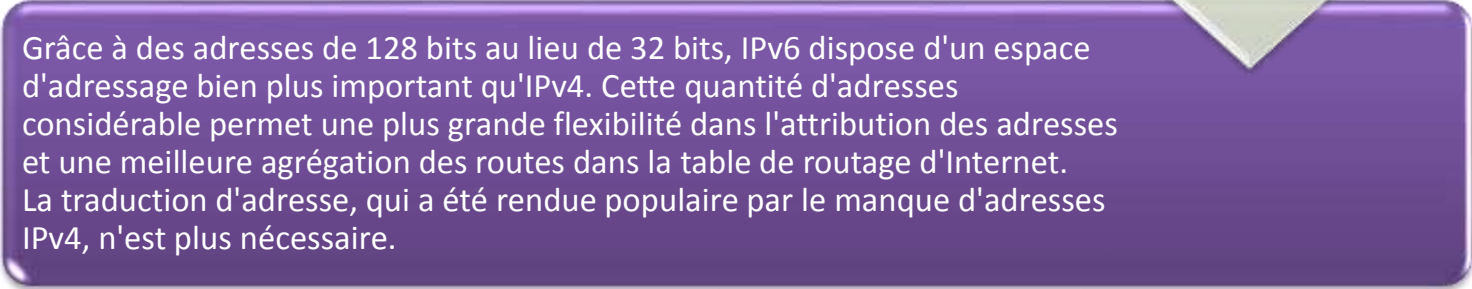
IPv6 (Internet Protocol version 6) est un protocole réseau sans connexion de la couche 3 du modèle OSI.



IPv6 est l'aboutissement des travaux menés au sein de l'IETF au cours des années 1990 pour succéder à IPv4 et ses spécifications ont été finalisées dans la RFC 2460 en décembre 1998.



Grâce à des adresses de 128 bits au lieu de 32 bits, IPv6 dispose d'un espace d'adressage bien plus important qu'IPv4. Cette quantité d'adresses considérable permet une plus grande flexibilité dans l'attribution des adresses et une meilleure agrégation des routes dans la table de routage d'Internet. La traduction d'adresse, qui a été rendue populaire par le manque d'adresses IPv4, n'est plus nécessaire.





# IPV6

Une adresse IPv6 est longue de 128 bits, soit 16 octets, contre 32 bits pour IPv4.

2001:0db8:0000:85a3:0000:0000:ac1f:8001

An IPv6 address

(in hexadecimal)

**2001 :0DB8 :AC10 :FE01 :0000 :0000 :0000 :0000**



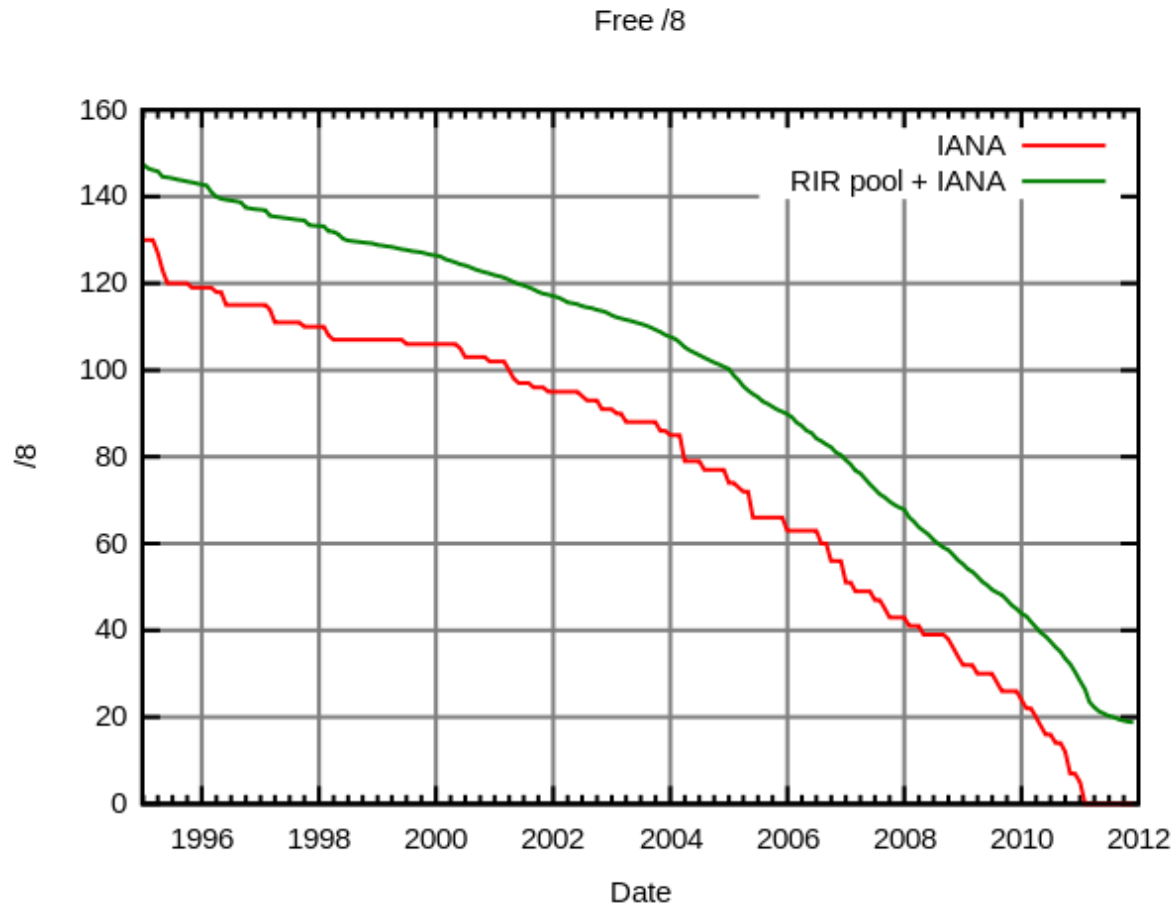
**2001 :0DB8 :AC10 :FE01 ::** Zeroes can be omitted



0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

# 2-1 IPV6



Épuisement des adresses IPv4 entre 1995 et 2011.

# Unicast

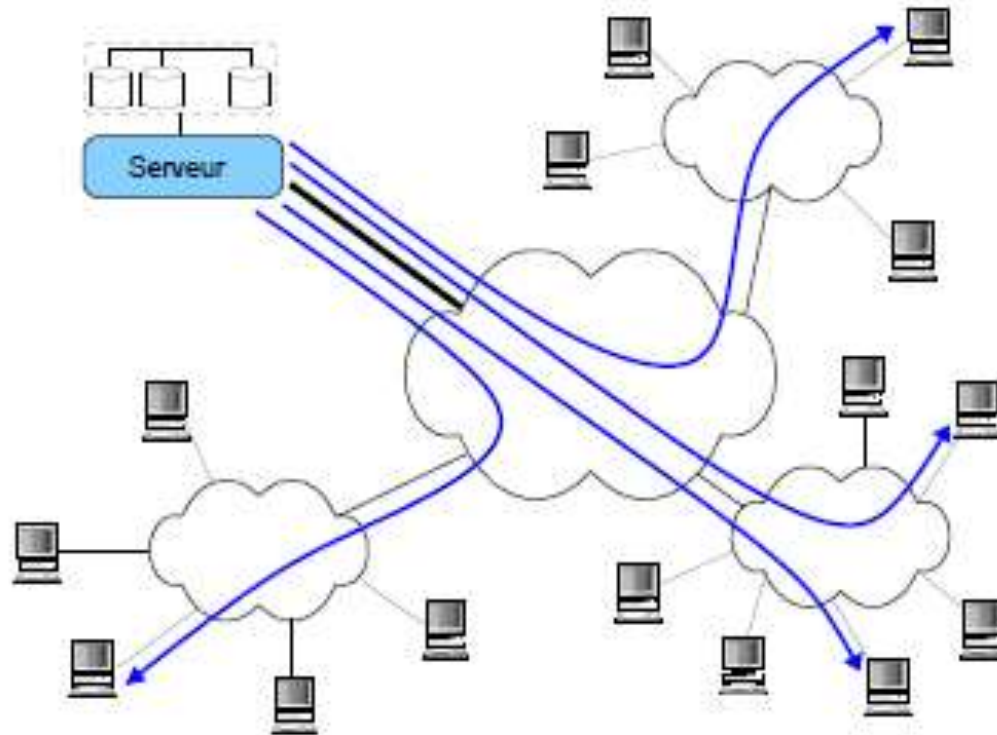


Figure 1.7 – Diffusion individuelle de vidéos à la demande.

# Multicast

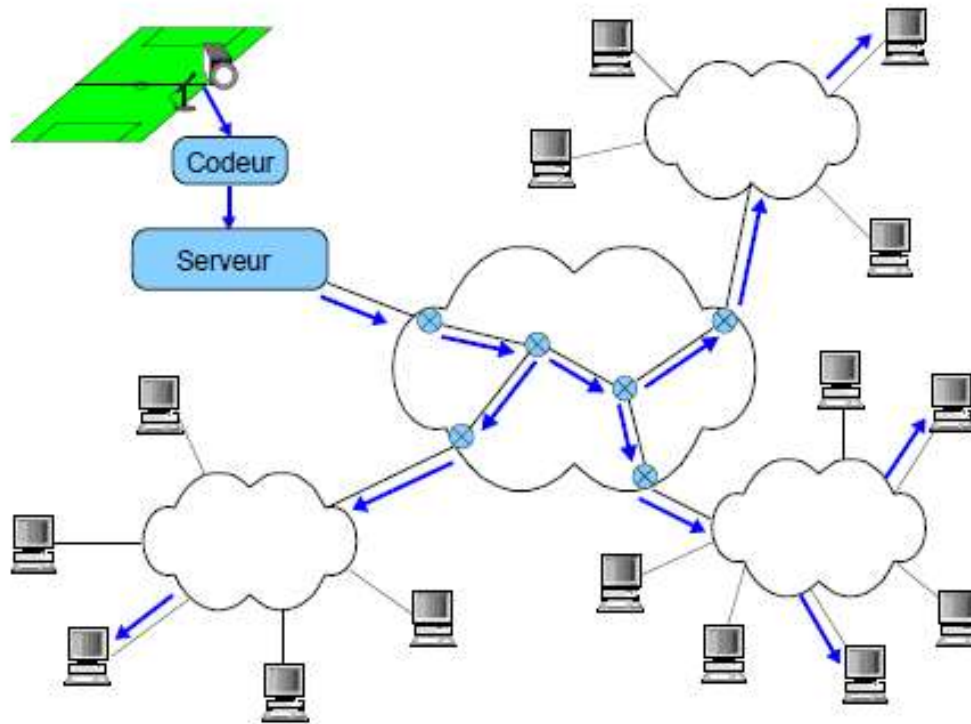


Figure 1.8 – Multidiffusion d'un événement en direct.