departamento de informática

SISTEMAS E REDES MULTISERVIÇO

Chapter 4 - Multimedia Architectures and Protocols

Introduction

Implementing Multimedia Architectures on IP networks has implications in TCP/IP model layers (with the exception of the physical layer):

The Transport Layer (UDP and TCP protocols) has limitations that must be addressed by Multimedia applications (example: SIP, SDP, RTP, RTCP)

In the Network Layer we have to create mechanisms to avoid high traffic in the network (e.g. Multicast) and QoS mechanisms as we saw in previous chapters

There is still the issue of security (Ex: TLS)

Summary

- Multimedia Applications:
  - Compression and encoding of audio and video;
  - Voice over IP Services (VoIP);
  - Protocolos SIP, RTP/RTCP;
  - VoIP Security: TLS
- Multicast networks and protocols;
- Streaming and RTSP: Internet Video Services (VCoIP, IPTV, VoD);

NEED FOR COMPRESSION

To stream video on IP networks, data compression is unavoidable:

- Example: Stream raw digital video with 1280 × 720 pixels with 8 bits per color (minimum HDTV setting):
  - 1280x720= 921600 pixels
  - 3 colors (RGB): 24 bits per pixel -> 921600x24= 22118400 bits per frame
  - 60 frames per second=> 60x22118400= 1327104000bps - 1.2Gbps!!!!

  It is necessary to apply a compression rate in the order of 1:1000 to reach transmission debits in the Mbps!

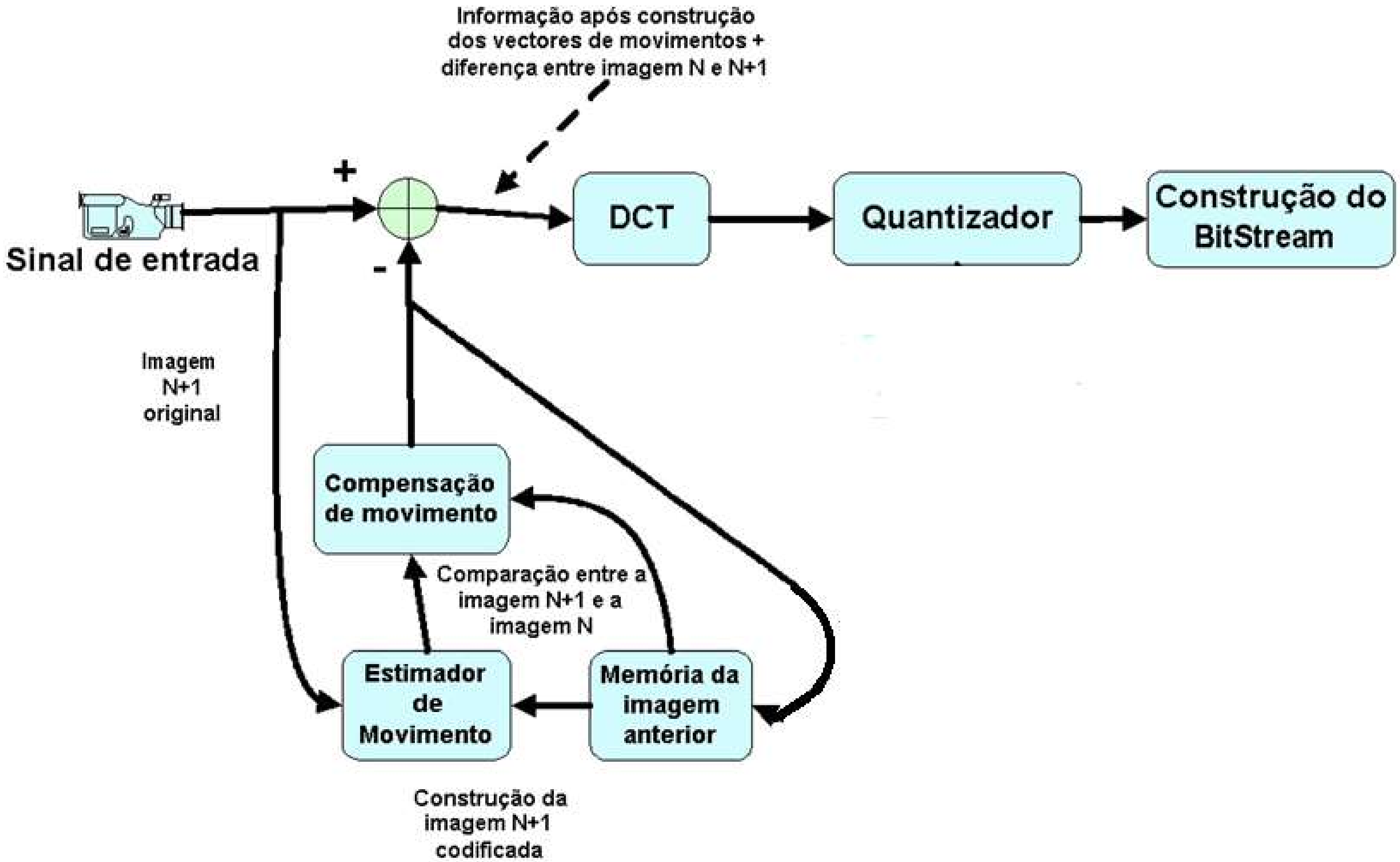
VIDEO COMPRESSION: MPEG

The most commonly used compression technologies are MPEG, especially MPEG-2 (channels occupy about 4Mbps) and MPEG-4 (1.8Mbps).

Compression is obtained by:

- Movement compensation: between consecutive frames only the modified information is transmitted;
- Use of motion vectors to determine pixel block positions in the next image;
- Elimination of redundant information by mathematical treatment of data (typically DCT- Discrete Cosine Transformed);
- Quantification and coding with smaller codes for the most frequent occurrences.

VIDEO COMPRESSION: MPEG



VOIP

Voice over IP (VoIP) is the transport of scanned voice signals in IP packets.

It's not the same as voice on Internet. The use of voice on top of a LAN is also VoIP;

The use of IP Voice (VoIP) is expanding and has already exceeded the volume of traditional voice traffic.

For the voice to be transported in IP, it must first be "encoded", that is, translated into zeros and ones that will be encapsulated in IP packets.

The requirements of reduced delays and jitter imply a differentiated treatment in the network.

VoIP CODECS

- VoIP Codecs ensure coding and compression mechanisms. Some examples:

Standard	Bit Rate	Observations
G.711 – PCM	64kbps	Used in traditional telephone networks. It doesn’t need compression.
G.726	16/32/40 kbps	Evolution of PCM with compression.
G.729	Desde 8kbps	In high growth of use

VOIP

To have a VoIP system we need to:

- A server (proxy) - responsible for user management: settings, permissions, location and address; audio and/or video conferencing management;
  - The server can be hardware (major manufacturers such as Cisco, Alcatel, Siemens, Mitel, etc.) or pure software running on a server (Asterisk, 3CX, OpenPBX, EdgeBox and those previously indicated) typically developed on Linux and sometimes free...

- Clients – can be an IP phone, a softphone (phone in software), a mobile phone that supports SIP or H.323, etc.
- An IP communications network with proper signaling - e.g. a LAN or the Internet, etc. complemented with the SIP protocol and, if possible, QoS!

MULTIMEDIA SIGNALING PROTOCOLS

Signaling multimedia IP sessions is required to:

- Establish communication;
- Locate interlocutors;
- Create a descriptive system of sessions that informs users of the contents, originator of the session and parameters of the session.

The most used protocol: Session Initiation Protocol (SIP)

MULTIMEDIA SIGNALING PROTOCOLS: SIP

The Session Initiation Protocol (SIP) is the most commonly used protocol for establishing, managing and ending multimedia sessions (VoIP, video, messaging, video conferencing, etc.):

- User location
- User availability (on, off, busy, etc.)
- User permissions
- Connection establishment
- Session management (link), p.e. end the session.

It is a protocol that allows Unified Communications

SIP and VOIP

- With SIP, aditionaly to a voice number, each user (User Agent- UA) has a URI: mailbox-like address (john@xpto.fr);
- The moment a user connects their phone or softphone, he sends SIP REGISTER packets to the server to validate the credentials and create a URI association with the IP address;
- The user can register from anywhere with ip connectivity to his server;
- The server knows, at any time, which machine/IP address a particular user is using and so can forward his calls;
- The user gains mobility because he is no longer required for a physical connection to the server and can be anywhere he has an IP connection to his VoIP server

SIP Protocol

SIP operations sequence:

- The user contacts the VoIP SIP server with SIP REGISTER packages
- The Server checks the request and requests the credentials;
- The user responds with the credentials
- The registration process ends with the user's acceptance of the parameterizations sent by the server - SIP ACK package

SIP Protocol

- SIP Operations Sequence (Registration):

SIP Protocol

1. To make a call, the user sends to the server a connection request (SIP INVITE message);
2. The server checks whether the recipient is in the same domain: If so, forward this INVITE to the destination; If he is away, act as a proxy and query DNS to get the IP address of the server where the target user is registered;
3. The server sends the originator SIP Trying packets (sent the call request) and Ringing (call beep)
4. The user being called accepts or not via an SIP OK packet to which the caller responds directly to the receiver with ACK.
5. Once the connection is established, the SIP does not intervene. All control is in charge of other protocols such as RDP, RTP, or RTCP (see following slides).
6. When one user wants to finish the call you must send a SIP BYE packet replied with ACK

SIP Protocol

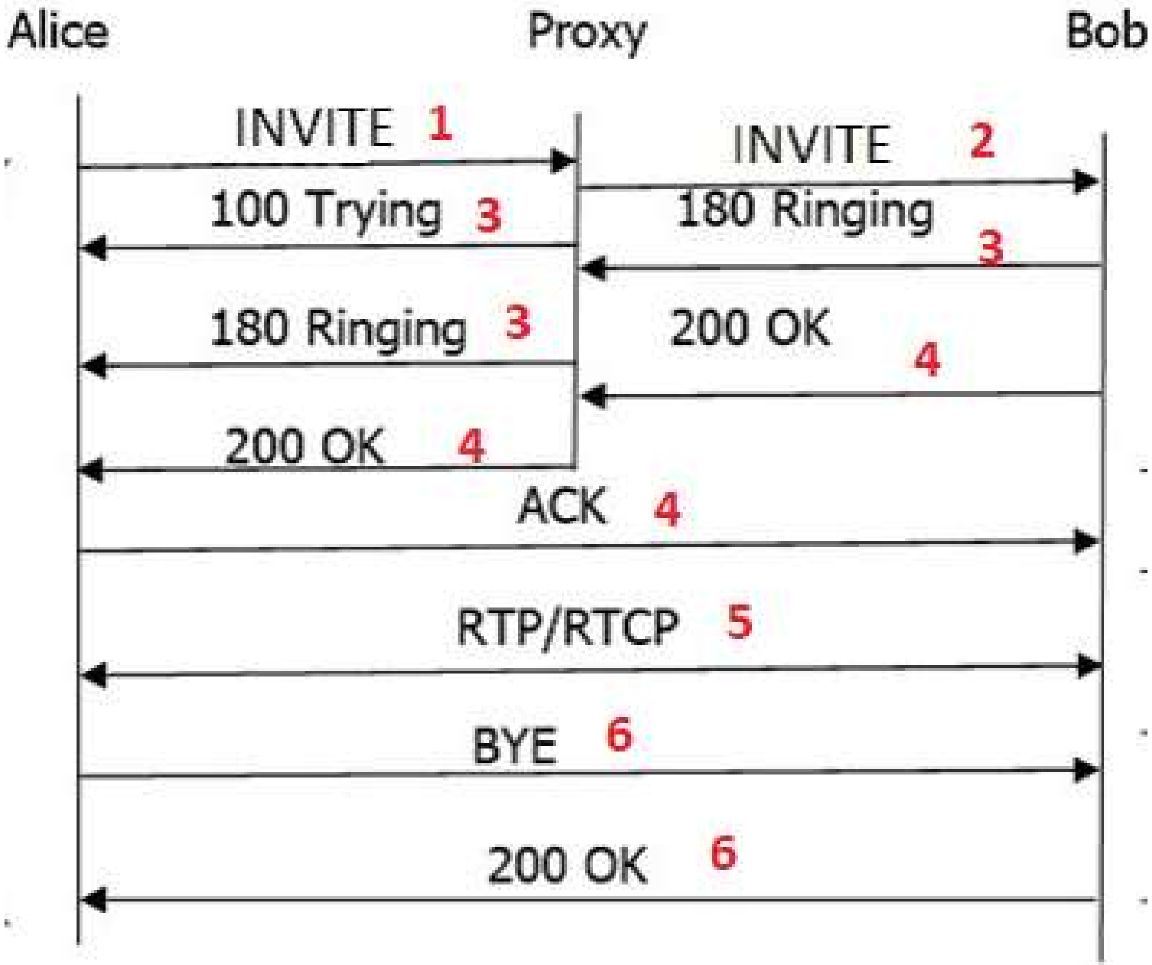


Imagem retirada de www.tutorialspoint.com

SIP and SDP

SIP is complemented by the SDP Protocol - Session Description Protocol to provide users with information about the sessions.
His function is to describe the session so that users can make the decision to join or not.

Includes information about:
- Session name and objective
- Information for access to the session
- Originator of the session
- IP addresses, ports, and codecs.
- Other information

SIP and SDP

Example of a SIP message with SDP :

SIP packet header:

- INVITE sip:rui@192.168.1.124 SIP/2.0
  Via: SIP/2.0/UDP 10.10.1.99:5060;branch=z9hG4bK343bf628;rport
  From: "Test 15" <sip:manel@192.168.1.112>;tag=as58f4201b
  To: <sip:rui@192.168.1.124>
  Contact: <sip:manel@192.168.1.112>
  Call-ID: 326371826c80e17e6cf6c29861eb2933@192.168.1.112
  CSeq: 102 INVITE
  User-Agent: Asterisk PBX
  Max-Forwards: 70
  Date: Wed, 06 Dec 2009 14:12:45 GMT
  Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY
  Supported: replaces
  Content-Type: application/sdp
  Content-Length: 244

SIP and SDP

Part of sdp (included in a SIP Invite package):

v=0 – *protocol version, typically zero*
o=root 1450 1450 IN IP4 192.168.1.112 – *Originator of session, session ID, network type, and address*
s=session – *session name*
c=IN IP4 192.168.1.112 – *Source IP Address*
t=0 0 – *time when the session will be active*
m=audio 11424 RTP/AVP 0 8 101 – *media type, transport protocol and codec*
a=rtpmap:0 PCMU/8000 – *from here are optional attributes*
a=rtpmap:8 PCMA/8000

RTP/RTCP PROTOCOLS

Multimedia applications in real time prefer the use of the UDP transport protocol to the detriment of TCP:

- Each unreceived TCP package requires the sender's resubmission, which may be incompatible with live streaming;
- TCP does not support multicast
- The congestion control mechanism requires a slow start
- The TCP header is much larger than UDP (40 vs 8 bytes)

However, the UDP protocol is very limited in the guarantees of establishment and maintenance of the session.

RTP/RTCP PROTOCOLS

To compensate for the absence of warranty delivery of UDP packets, the Real Time Protocol (RTP) is used.

Designed to support real-time applications provides detection of packet losses.

It is the most important of strandards developed for streaming because all packages, whatever the format, can be encapsulated in RTP packets.

Complements the UDP because, in the header, it has additional fields, including a time marker and a sequence number to allow the correct rebuild.

It does not ask for the retransmission of lost packages but allows you to identify losses! It is an information transfer protocol that can be supplemented with the Real Time Control Protocol (RTCP), which provides QoS information to RTP users.

RTP PROTOCOL

- RTP package structure:

Cabeçalho IP	Cabeçalho UDP	Cabeçalho RTP	Payload RTP
20 bytes	8 bytes	12 bytes (min)	Variável

The content of the media session is in the payload of the RTP package;

The RTP header (12 to 72 bytes) provides information about multimedia content: e.g. source, size, encoding type, sequence number, and time marker;

It is transported within the transport layer package (UDP or TCP) and routed within the IP packet.

RTP PROTOCOL

- Some of the functions guaranteed by RTP are:
  - Temporal marking of information, which can help synchronize the audio and video p.e.;
  - Sequence marking - important because UDP does not guarantee delivery on shipping order;
  - Marking by the type of payload, to identify the packages belonging to the different segments;
  - Source identification: useful in cases where the receiver receives information from different sources.

RTP/RTCP PROTOCOLS

RTCP collects information about the quality of the transmission. It implements quality of service feedback functions. Periodically sends packets between the sender and the receiver with session conditions:

- Percentage of lost RTP packets in the last period,
- Percentage of packets lost since the start of the session,
- Differences in packet delays as long as the last report is received.

This information is used by the source or network elements for improving network performance or changing compression parameters.

Practical topics for VoIP

To use VoIP in an enterprise you should consider:

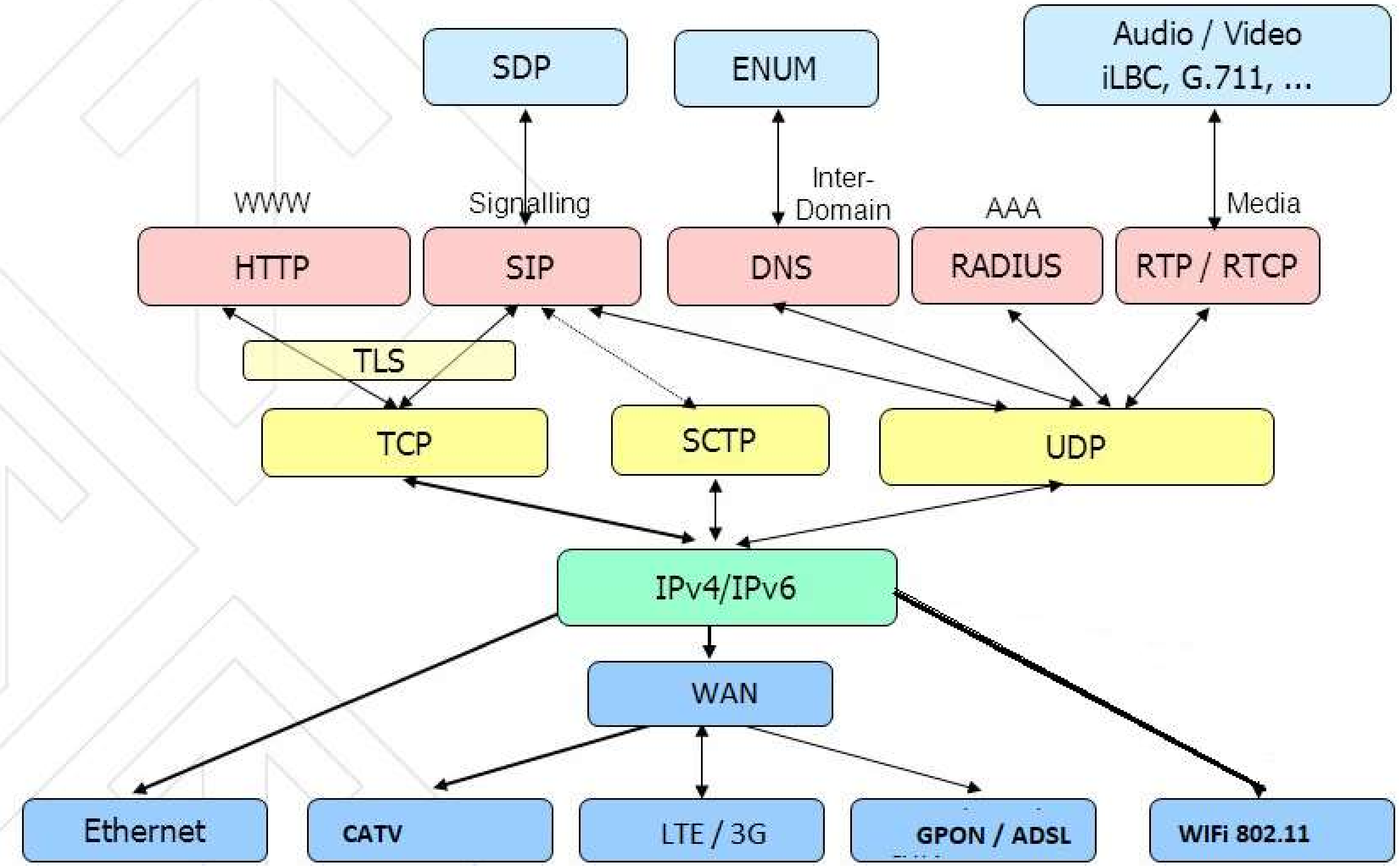
- There may be cost reduction (lower communications costs; no dedicated wiring required)
- Increase user mobility
- Can integrate with other apps (e.g. Outlook)
- There may be loss of quality and availability -> to minimize, use a VLAN for VoIP with QoS!
- VoIP devices are power dependent! -> consider using PoE (Power over Ethernet)
- VoIP uses the computer network and IP protocols -> security care

VoIP Security

To mitigate security issues, VoIP services typically use TLS - Transport Layer Security (in TCP) or their equivalent for UDP: DTLS - Datagram Transport Layer Security

- Security protocol that evolved from SSL – Secure Socket Layer used p.e. in HTTPs
- Works with encryption and digital certificates to encrypt:
  – The authentication process SIP signaling
  – The communication itself

Protocols Summary

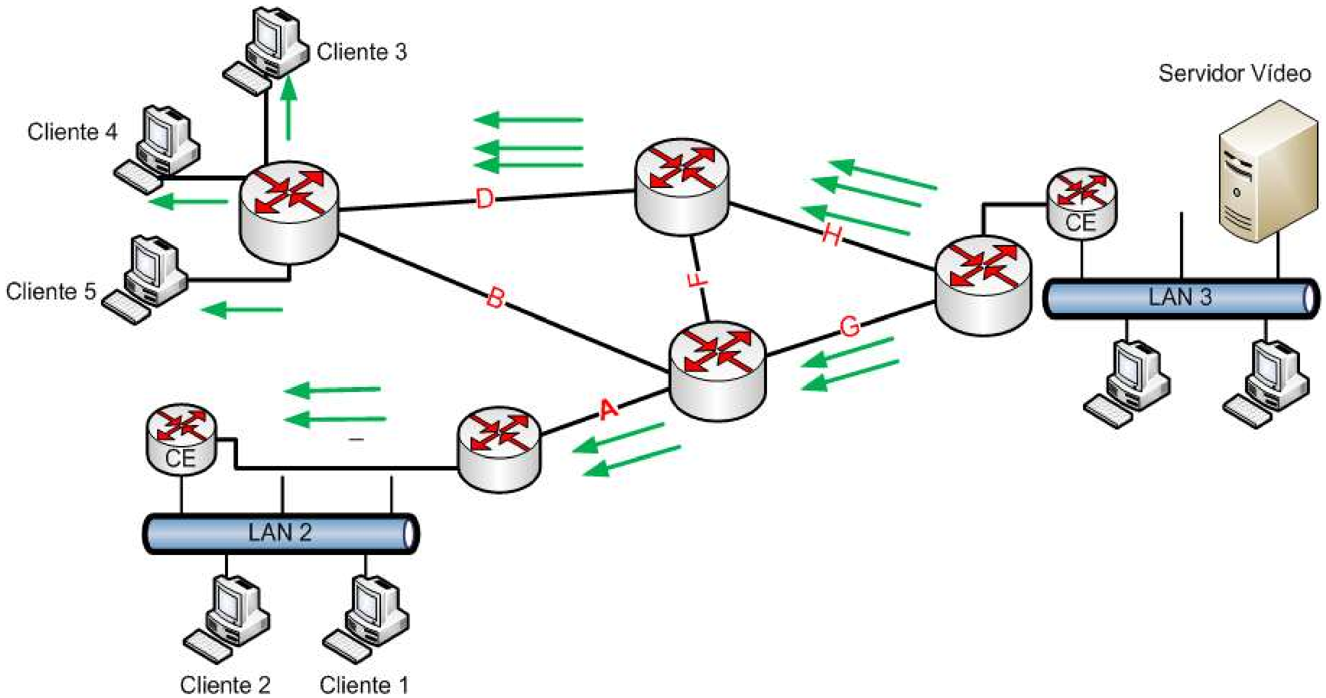


Summary

- Multimedia Applications:
  - Compression and encoding of audio and video;
  - Voice over IP Services (VoIP);
  - Protocolos SIP, RTP/RTCP;
  - VoIP Security: TLS
- Multicast networks and protocols;
- Streaming and RTSP: Internet Video Services (VCoIP, IPTV, VoD);

Unicast

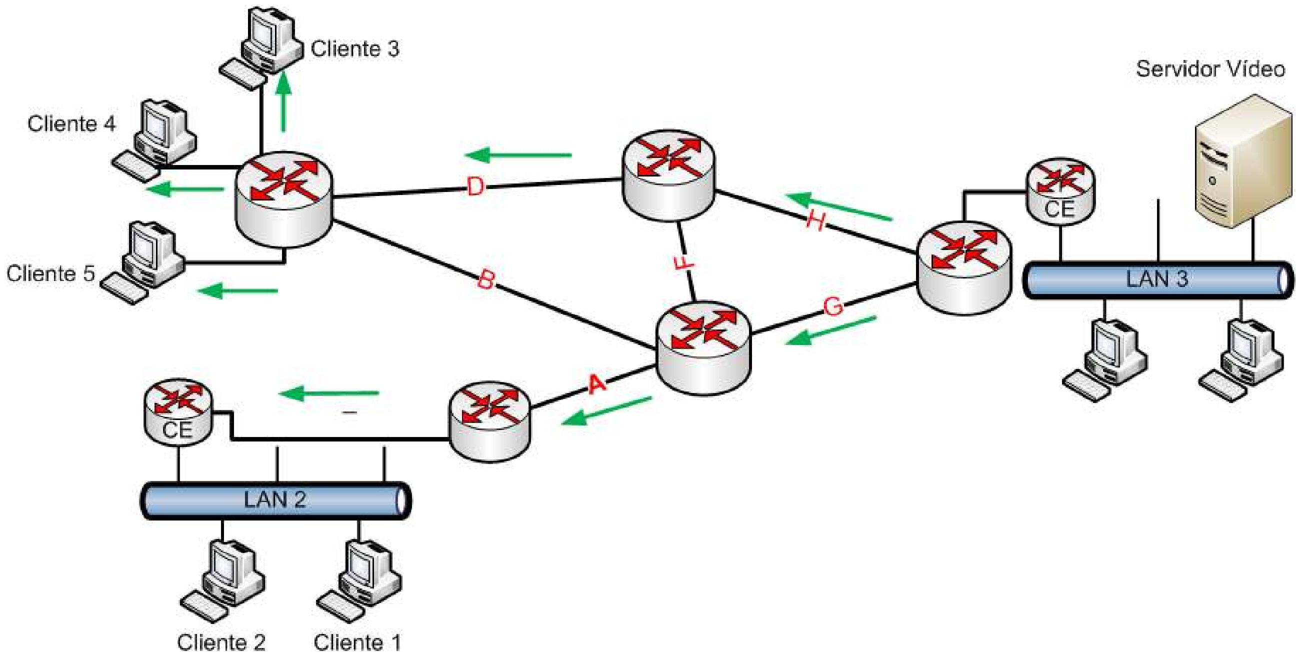
In traditional networks the dissemination of equal information to multiple receivers implies the creation of an information flow by each receiver from the origin:



This model (unicast) implies a linear growth in the volume of traffic on the network by each user and places great limitations on the number of customers served.

Multicast

Multicast is a technology that overcomes this problem by sending a single flow of information in each section:



In each section of the network, only is one unit of the information packet. Replication is done on the equipment (router, switch) where there is a need for information derivation.

Multicast - Groups

The use of Multicast is essential for the dissemination of TV broadcasting.

However, not all clients receive the same set of channels or, in the case of IPTV, each client receives a restricted set of channels.

A Multicast Group represents a set of hosts that receive the same Multicast broadcast.

It is an important multicast concept because it is based on memberships to groups that Routers decide whether or not to route packets from that group in the downstream.

Multicast - addressing

Since the beginning of IPv4, ip address ranges reserved for Multicast are planned:

4 bits				28 bits
1	1	1	0	*Group ID*

(In decimal notation: from 224.0.0.0 to 239.255.255.255)

In IPv6:

8 bits	4 bits	4 bits	112 bits
1111 1111	*flags*	*Scope*	*Group ID*

Group ID does not identify a host but a Multicast Group. All machines that want to access the content must join the Group and listen to packages with this Group ID i.e. intended for that IP address.

Multicast - IGMP

There are two distinct problems to solve:

1. Identify all group hosts (signaling/group management)
   - On IPv4 networks is the IGMP (Internet Group Multicast Protocol)
   - In IPv6 its MLD (Multicast Listener Discovery).
2. Create distribution trees (Multicast forwarding protocols)

Multicast - IGMP

The IGMP protocol is used by customers to communicate to routers/switchs the adhesion or abandonment of a Multicast Group on IPv4 networks.

It is based on the IGMP information sent by customers that Routers or Switches make packet forwarding decisions from a particular Multicast group through their ports.

It is also a IGMP function to periodically check customer activity.

Routers will need to inform upstream that they have customers connected to a group to receive packages from that group.

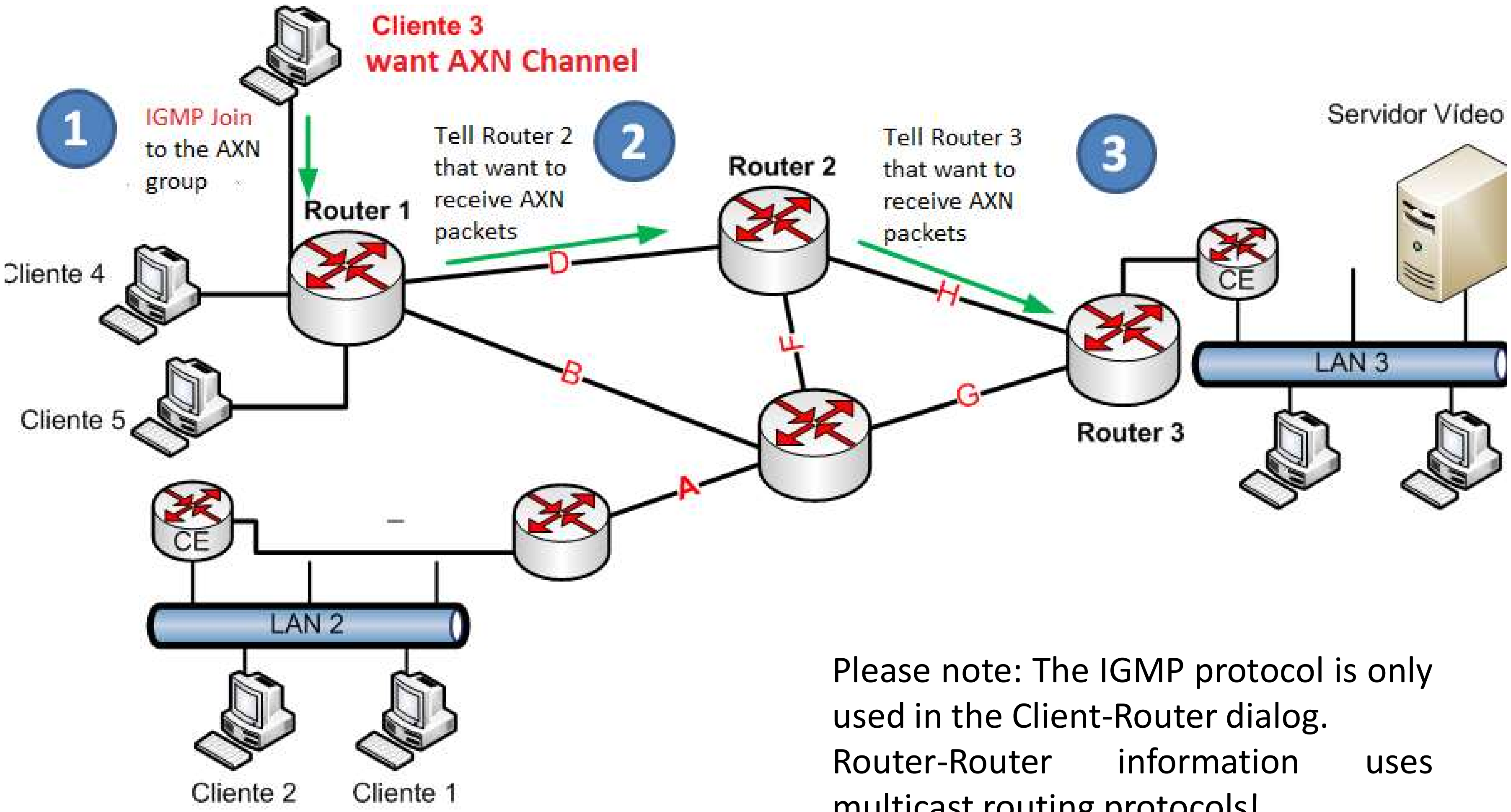
Multicast - IGMP

IGMP messages sent by clients to Multicast Agents routers can be of type:

- Join – to join a group
- Leave – to leave the group
- Query - asks for a list of subscribed groups.

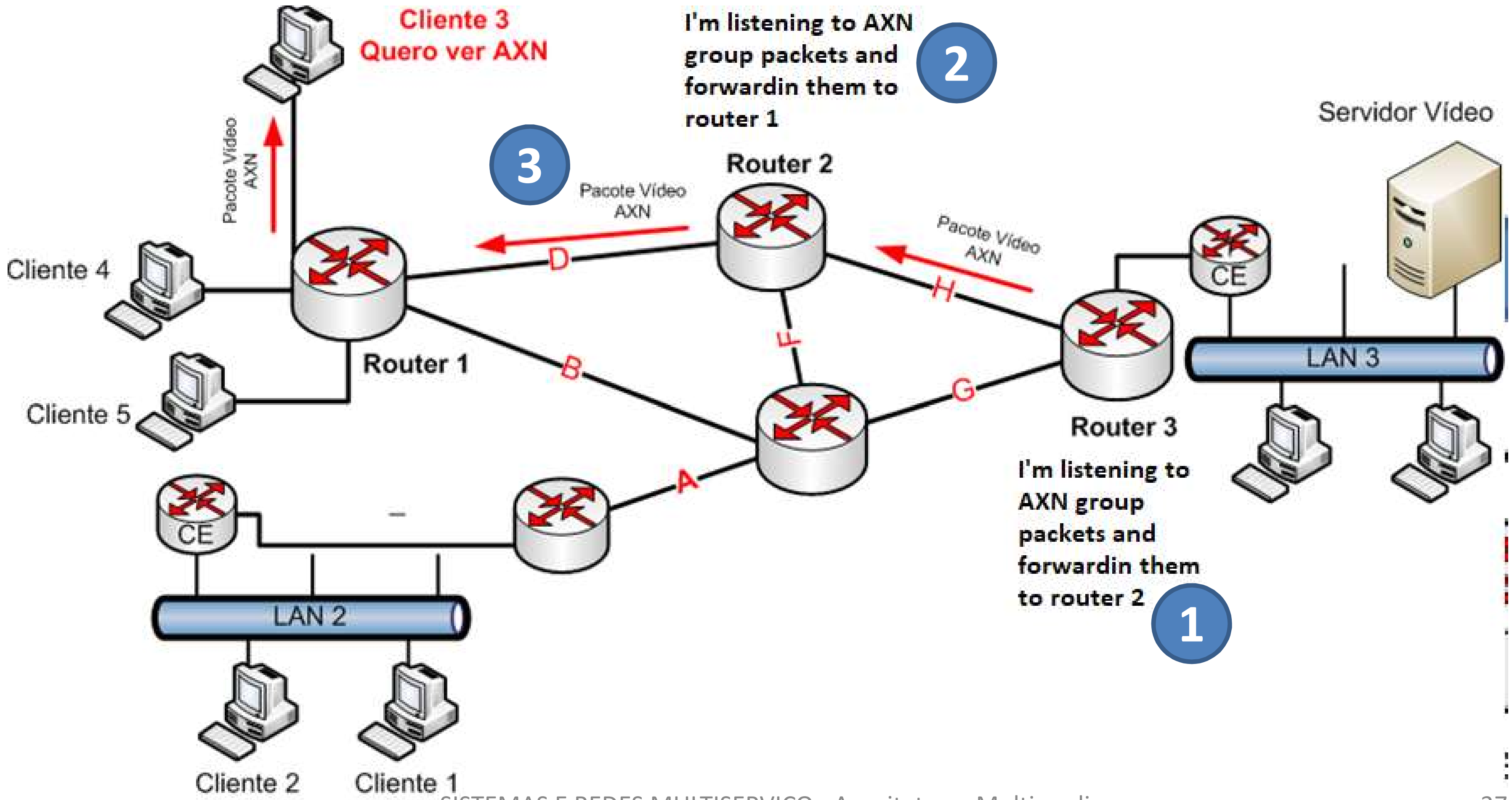
The versions of IGMP in use are The V2 and the latest version 3 that also allows simultaneous shipping of the Leave and Join request.

Multicast - IGMP - group membership

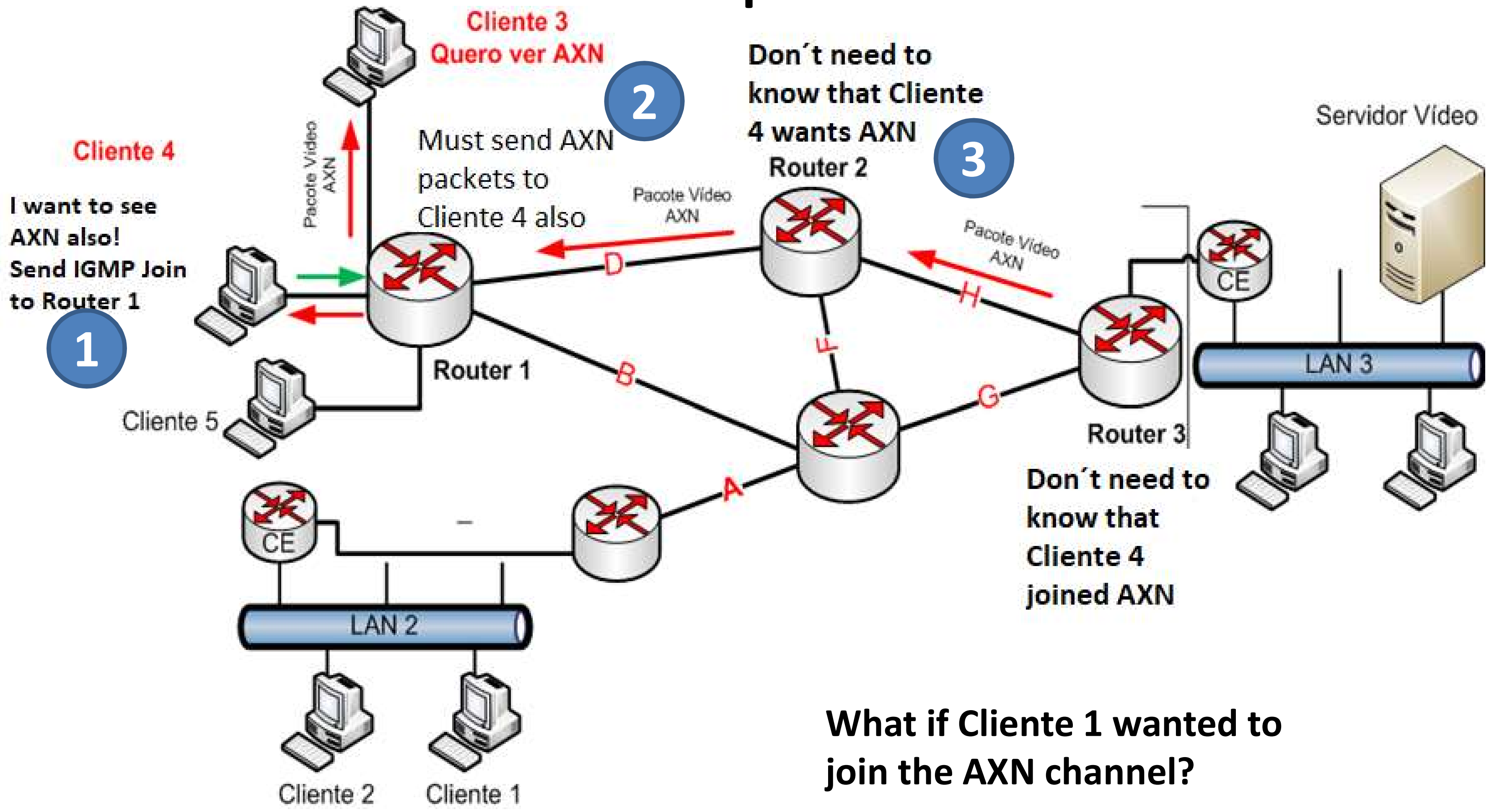


Please note: The IGMP protocol is only used in the Client-Router dialog. Router-Router information uses multicast routing protocols!

Multicast - IGMP - group membership

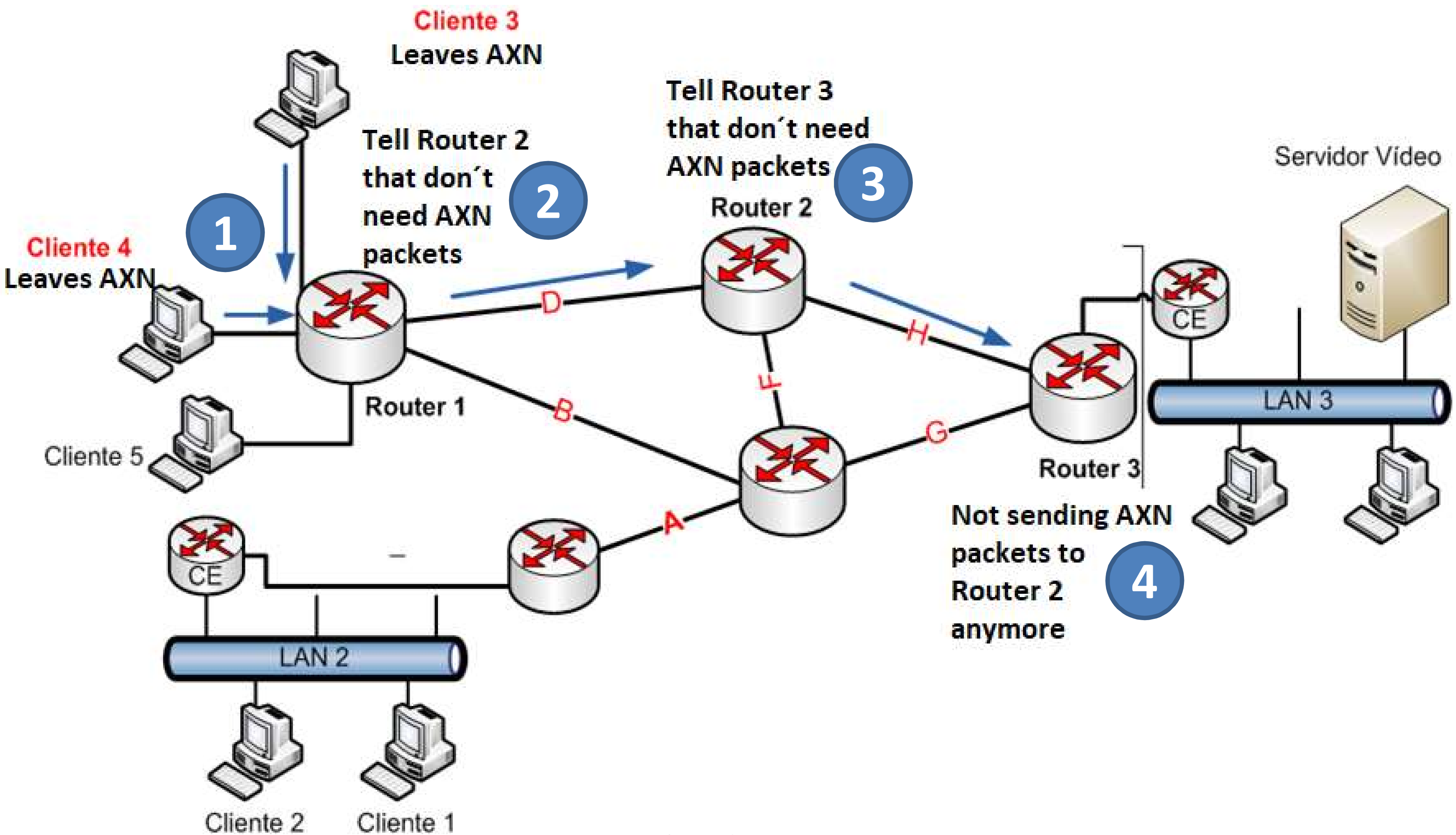


Multicast - IGMP - new memberships



What if Cliente 1 wanted to join the AXN channel?

Multicast - IGMP – Leave the group



MULTICAST and IGMP for IPTV

In IPTV technology, each customer's Top Box Set sends IGMP "Join" packages to Multicast Agent asking for membership of a particular group to which a television channel matches.

In the case of restricted access channels, Multicast Agents and Set Tob Boxes previously exchange IGMP messages with keys that allow access to private groups.

Summary

- Multimedia Applications:
  - Compression and encoding of audio and video;
  - Voice over IP Services (VoIP);
  - Protocolos SIP, RTP/RTCP;
  - VoIP Security: TLS
- Multicast networks and protocols;
- Streaming and RTSP: Internet Video Services (VCoIP, IPTV, VoD);

Video Streaming

Traditional Video Stream:

1. Capture Images
2. Scan, encode and place on servers.
3. The client ask the server for the video
4. The user waits for the complete download of the file; then, appropriate software decrypts and reads the video.

Inconvenience: Large storage spaces are required; The time the user has to wait; It does not allow the transmission of real time events.

Vídeo Streaming

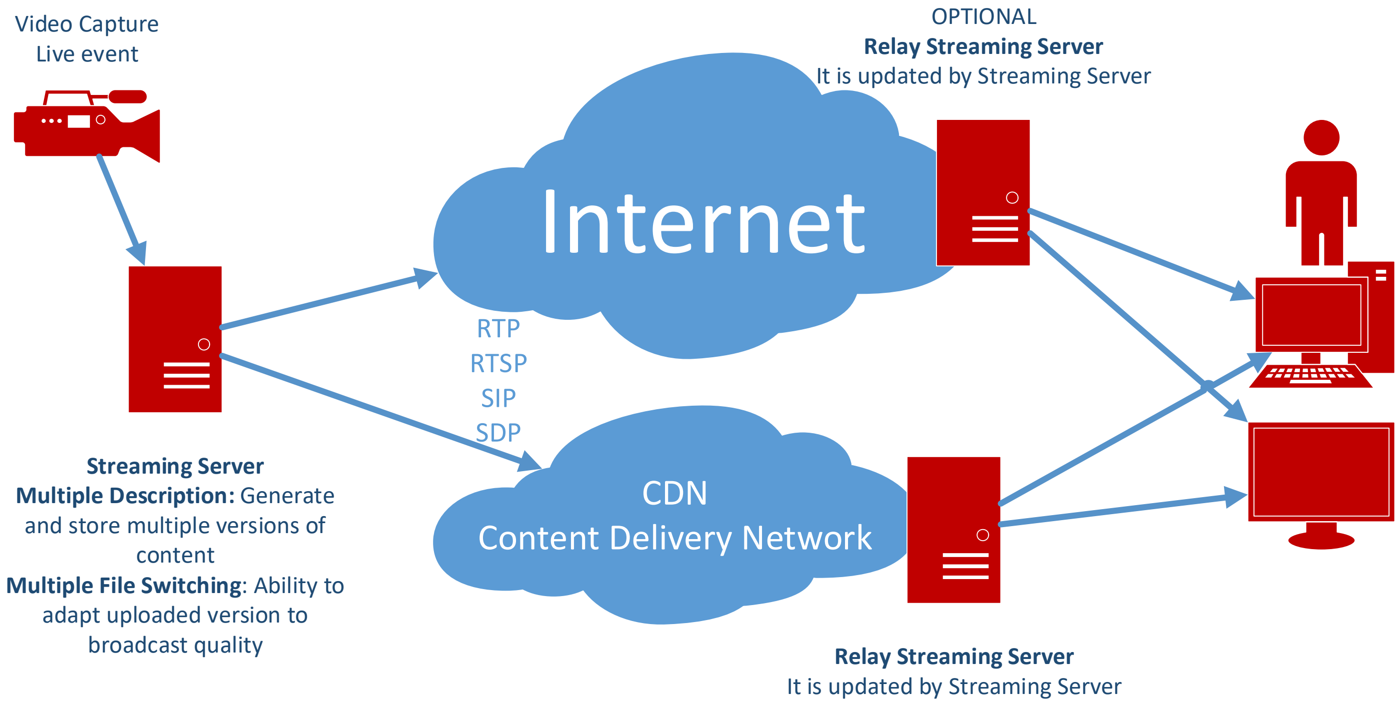
Video Streaming allows you to broadcast video in real time and on-the-fly, that is, you start the presentation while your broadcast is still taking place.

The receiver requests the transmission of a particular video and the server starts the transmission by breaking the file in small packets that are grouped into streams: pieces that can be displayed individually regardless of whether you have already viewed the previous excerpts.

The application will have to manage the received packages, rebuilding the streams and placing them in order of presentation.

Video Streaming

- Streaming Advantages:
- Allows live or VoD streams - VideoOnDemand;
- The information is not stored in the customers' PCs;
- Architecture:



Video Streaming Protocols

For each session control, the protocols used by streaming video on the Internet are the Real Time Streaming Protocol (RTSP) in conjunction with the Session Initiation Protocol (SIP) and RTP.

RTSP allows real-time Unicast or Multicast session control and enables the implementation of typical functions of a VCR such as:

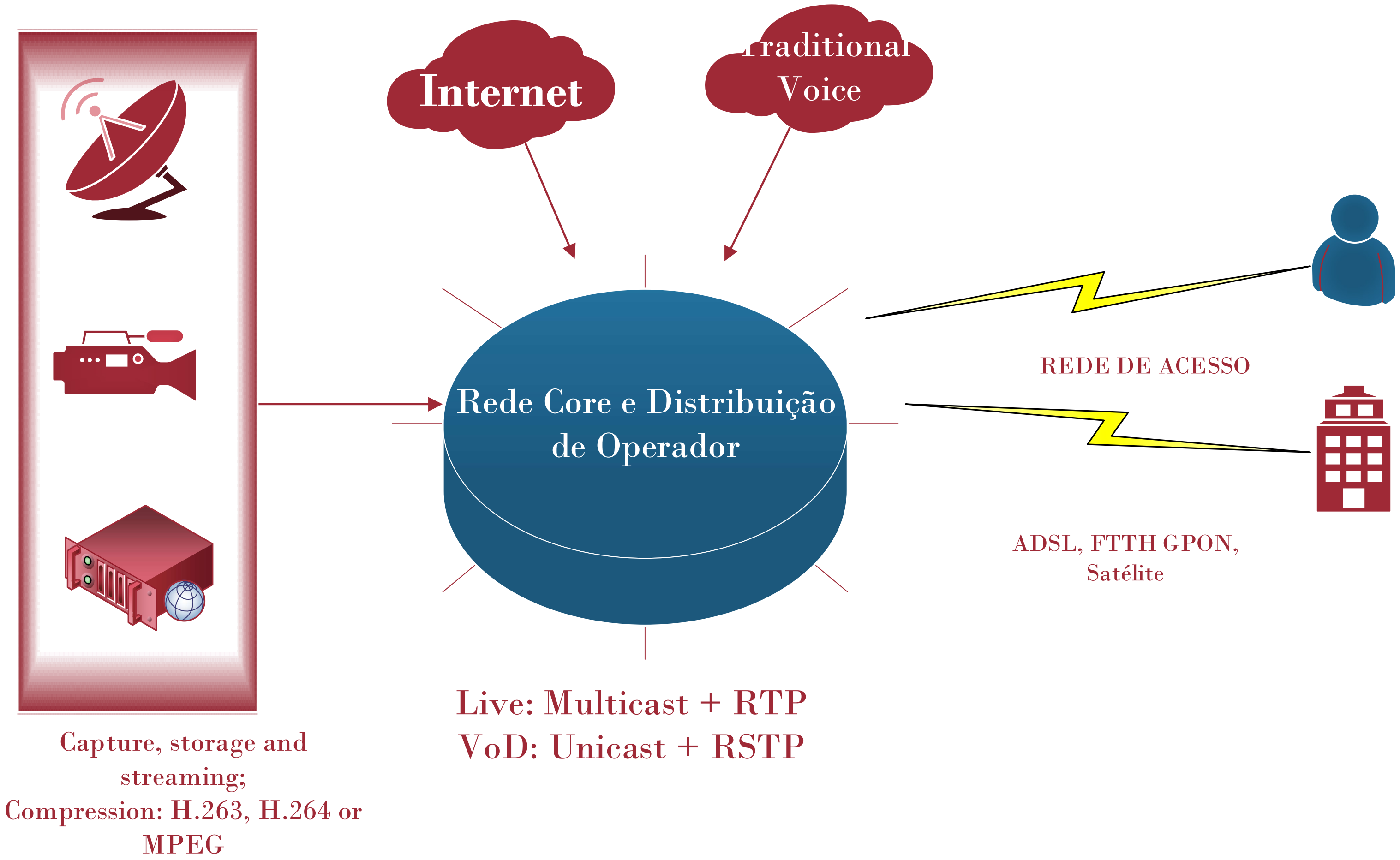
- pause
- fast forward
- establishment and control of streams between servers and customers
- additional content information available for transmission
- choose the best type of session for packet delivery, from unicast to multicast, or even if this is possible by implementing the tcp session.

IPTV and VoD

- IPTV - Television broadcast on IP networks
- Driven by the reliable/fast IP Networks and migration of traditional IP operators;
- Non-elastic application!
- It can be live, deferred, or on request (Video On Demand).
- It's not the same as Internet TV

IPTV and VoD

- Architecture:



Example of New Internet Video Services: Netflix

- www.netflix.com
- Video on Demand Streaming Service supported on the Internet since 2008;
- Possible due to improved internet access and low prices;
- In 2014 it already had more than 50 million users;
- It has been based on HTML5 since 2010.

Example of New Internet Video Services: Netflix

- All contents (movies, series, etc.) are scanned in various quality formats;
- Netflix has its own Content Delivery Network (CDN) with multiple storage locations to bring customers closer to servers;
  - This CDN is supported by multimedia protocols such as SIP, RTP, RTCP, etc.
  - Storage systems are optimized for Streaming with high density, low-consumption disks;
  - Each storage unit stores 100TB of information-> 10k to 20k movies
  - The total portfolio has already more than 1 PB

Example of New Internet Video Services: Netflix

- Netflix CDN's connection to the customer is supported on traditional internet connections;
- There are already ISPs that have an agreement with Netflix to house servers in their own Data Centers and, thus, have a competitive advantage in this market;
- The Netflix CDN has 20 points of peering and several ISP’s with housing.

CAPÍTULO 4 - Arquiteturas e Protocolos Multimédia

Doubts?