MODULO 2
TELEFONÍA IP

PARTE II

Curso EL6019
Departamento de Ingeniería Eléctrica
U. de Chile
V.2013

INDICE GENERAL DEL MODULO 2

Parte I

3 MODELOS OSI y TCP/IP

3.1 Introducción

3.2 Modelo OSI

3.2.1 Funciones y protocolos en Modelo OSI

3.2.2 Capas en Modelo OSI

3.2.3 Unidades de datos en las diferentes capas OSI

3.3 Modelo TCP/IP

3.3.1 Funciones y protocolos en Modelo TCP/IP

3.3.2 Capas en Modelo TCP/IP

3.3.3 Unidades de datos en las diferentes capas TCP/IP

3.3.4 Diferencias y semejanzas de TCP/IP con OSI

Parte II

6 CODEC: Funcionamiento, Especificaciones, Ancho de Banda

6.1 Principios de funcionamiento de los CODEC usados en telefonía

6.2 Otras especificaciones de los CODEC usados en telefonía

Parte III

6.3 Ancho de banda requerido para transmitir los datagramas generados por los CODEC

7 SERVIDORES de TELEFONIA IP

8 GATEWAYS VoIP y ROUTERS

Parte IV

9 TELEFONOS IP y SOFTPHONES

10 TOPOLOGIAS DE REDES DE TELEFONIA IP

11 DIMENSIONAMIENTO

5 PROTOCOLOS TELEFONIA IP

5.1 Introducción

- Nos dedicaremos ahora a estudiar protocolos correspondientes a las capas altas (sobre el stack), o sea “Aplicaciones” para nuestro tema: La Telefonía IP.

- Estos protocolos son los responsables de generar los bloques de datos que hemos llamado “payload”, y entregarlos al “stack” para su transmisión por la red de datos.

- Como vimos anteriormente, la implementación de llamadas telefónicas VoIP por una red de datos involucra:

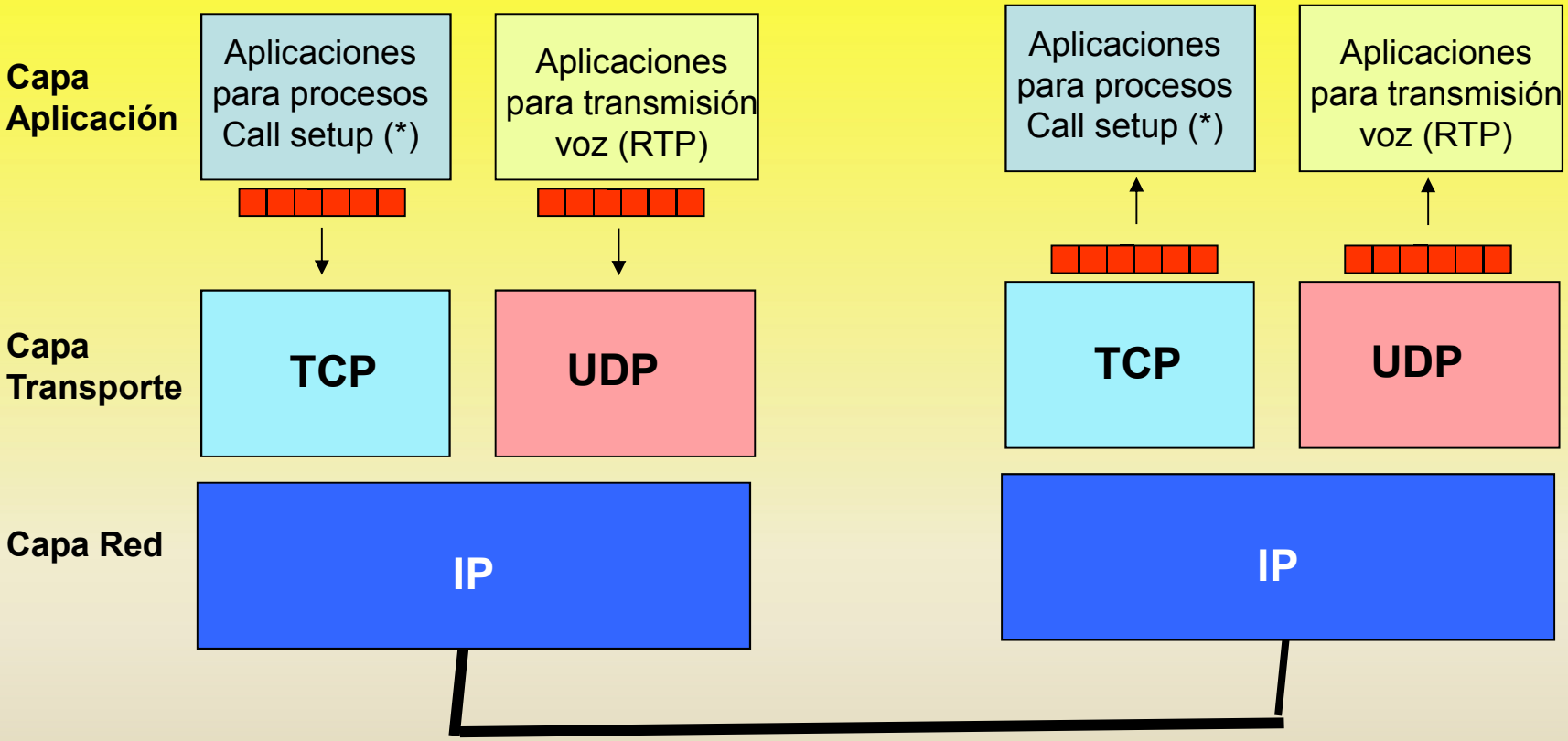
  El establecimiento (y disolución) **de las llamadas (Call Setup)**, es decir las funciones de señalización de la telefonía tradicional: obtener tono de invitación a marcar, marcar un número, obtener un tono de llamado o de ocupado, recibir señal “abonado B contestó” . Se incluye aquí también la disolución de las llamadas (Call Takedown).

  La comunicación telefónica misma (fase de conversación)

- Durante ambas fases se requieren los protocolos de Telefonía IP

Si la aplicación privilegia **seguridad** y **confiabilidad** se utiliza **TCP**

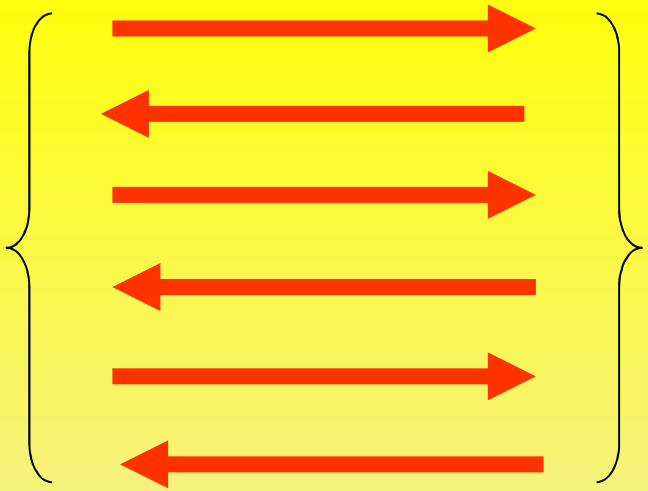
Si la aplicación privilegia **rapidez** se utiliza **UDP**



(*) también llamados de “señalización”

Call Setup (señalización)

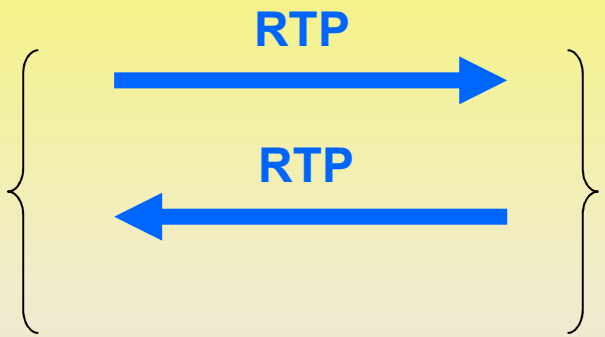
Intercambio de datagramas anidados en TCPs y UDPs simulan todos los pasos de señalización que ocurren en la Red Telefónica Conmutada Pública durante establecimiento y disolución de la comunicación



Conversación

Dos flujos de datos correspondientes a la voz digitalizada

Un flujo en cada dirección de conversación



Se distinguen dos familias de protocolos de alto nivel:

a) para transferir la información durante las fases Call Setup & Takedown

b) para transferir la voz digitalizada

Entonces

Hay dos conjuntos de protocolos de alto nivel

Protocolos Call Setup o de señalización

Utilizados para intercambiar la información necesaria para establecer y disolver la comunicación. Estos protocolos “se sirven” de la capa de transporte (TCP o UDP). Permiten simular todos los pasos de la señalización de Red Telefónica Conmutada Pública necesarios para establecer y deshacer las comunicaciones

Protocolo para el transporte del flujo de voz

Llamado Real-time Transport Protocol (RTP). Este protocolo se utiliza para el transporte de cada uno de las dos flujos de voz (uno para cada dirección de conversación). “Se sirve” de la capa de transporte UDP.

En honor a la rigurosidad, debemos mencionar otros dos conjuntos de protocolos que se relacionan indirectamente con la telefonía IP.

Protocolos de gestión

Son una ayuda para la gestión y mantenimiento de la red de datos, ya que **entregan información y estadísticas sobre el grado de utilización de la infraestructura existente**, la que es necesaria para ampliar y optimizar oportunamente la red.

Ejemplo de protocolo de gestión es RTCP XR, el que es capaz de medir pérdidas de paquetes, retardos, jitter, nivel de audio, nivel de ruido, eco, siendo capaz de entregar información integrada sobre la calidad de la voz de acuerdo a la escala Mean Option Score (MOS) y al modelo E de la UIT.

Permite discriminar si la pérdida de calidad se debe a mala configuración de los puntos finales o a problemas en la red

Protocolos de seguridad

Orientados **a evitar que las comunicaciones VoIP sean maliciosamente interceptadas o intervenidas por hackers**. Estos protocolos son necesarios ya que el uso de encriptación no es recomendable por el alto consumo de ancho de banda que significa.

En ambas fases, señalización y conversación, se requiere transferir información por la red IP

- Para el transporte de la información durante la fase señalización (Call Setup + Call Takedown) se pueden emplear varios tipos de Protocolos Call Setup, los que anidan la información en unidades TCP ó UDP, según se requiera privilegiar, respectivamente, la certeza o la rapidez en el transporte. Como veremos, existen diversos protocolos Call Setup, algunos muy seguros pero pesados y otros menos seguros y más livianos. **Los payloads intercambiados por los protocolos Call Setup corresponden a bloques de datos con información de señalización**.
- Para el transporte de la información durante la fase de conversación se emplea el **Protocolo Real time Transport Protocol** (RTP), el que anida la información (datagramas) en unidades (segmentos) UDP. Como la información del flujo de voz es en tiempo real y suficientemente redundante, es adecuado UDP, protocolo rápido y no orientado a la conexión. **Los datagramas intercambiados corresponden a muestras de la voz digitalizada entregada por el CODEC**
- Los segmentos TCP y UDP (ya sea que su payload corresponda a Call Setup ó RTP), se anidan en paquetes IP.

5.2 Protocolos Call Setup o de señalización

(utilizados en las fases Call Setup y Call Takedown)

- En telefonía IP cuando se habla de protocolos Call Setup, se debe entender que estos también realizan las funciones de disolución de las llamadas (Call Takedown)

- Los protocolos Call Setup administran funciones como:

  - Mapeo de los números telefónicos con las direcciones IP
  - Generación de tonos de invitación a marcar y señales de ocupado
  - Ringing del llamado
  - Descuelgue
  - Release

- Los Protocolos Call Setup o de señalización corresponden a los programas que **implementan los procesos para el establecimiento y disolución de las comunicaciones**

- Utilizan tanto TCP como UDP para encapsular los datos que es necesario intercambiar durante las fases de establecimiento y disolución de las llamadas

5.2.1 Los principales protocolos Call Setup o de señalización

- Los protocolos Call Setup impulsados por el mundo de la conmutación telefónica han sido desarrollados por la ITU-T y se agrupan en la recomendación H.323:

  - **Protocolo H.323**

- Los protocolos Call Setup impulsados por el mundo de la transmisión de datos han sido desarrollados por la IETF. Destaca:

  - **Protocolo SIP** (Session Initiation Protocol) IETF RFC 2543

- Protocolos desarrollados en forma conjunta por La ITU-T y por la IETF

  - **Protocolo Megaco / H.248 (Media Gateway Control Protocol)** IETF RFC 2885

  - **MGCP** (acrónimo también de **M**edia **G**ateway **C**ontrol **P**rotocol). IETF RFC 2705

- SIP y Megaco son protocolos livianos y por tanto más rápidos que H.323

Arquitecturas Centralizada y Distribuida

En el pasado todas las redes de voz se construían en base a arquitectura centralizada: terminales tontos (los teléfonos) todos controlados por centrales en que estaba toda la inteligencia de la red. **La arquitectura centralizada tiene la ventaja de la simplicidad del manejo de las llamadas y es adecuada al servicio telefónico básico, pero es poco flexible para introducir terminales más sofisticados y nuevos servicios.**

Cuando hablamos de inteligencia de la red nos referimos a su habilidad para controlar el estado de las llamadas, features de las llamadas, enrutamiento de las llamadas, provisión de servicios, tarificación y cualquier otro aspecto relacionado con el manejo de las llamadas.

La telefonía IP tiene la ventaja que puede ser diseñada en base a arquitecturas centralizadas o distribuidas, aprovechando las ventajas de cada una de ellas.

Arquitectura Centralizada: Protocolos MGCP y Megaco/H.248

Estos protocolos fueron **diseñados pensando en la existencia de un dispositivo central llamado** MEDIA GATEWAY CONTROLLER, CONTROLADOR o CALL MANAGER, que maneja la lógica de conmutación y el control de la llamada.

El dispositivo centralizado indica a los GATEWAYS como transmitir los flujos RTP con las muestras de voz, las que sí se transmiten directamente entre Gateways.

La inteligencia de red está centralizada y los terminales son relativamente tontos (con features limitados o no residentes en ellos).

Aunque la mayoría de las arquitecturas centralizadas usan los protocolos MGCP o Megaco/H.248, también es posible diseñarlas en base a protocolos SIP o H.323, usando agentes usuarios back to back (B2BUAs) o GATEKEEPER ruteadores de señalización (GKRCS), respectivamente.

Ventajas: Centraliza el control de las llamadas, la administración y la provisión de los servicios. Simplifica el flujo de las llamadas. Replica las características de la telefonía tradicional. Los Ingenieros de telefonía tradicional la prefieren.

Desventajas: Sus detractores dicen que ahoga la innovación de los features de los terminales y que es un obstáculo para diseñar nuevos servicios que no existen en la telefonía tradicional

Arquitectura Distribuida: Protocolos H.323 y SIP

Estos protocolos **permiten distribuir la inteligencia de la red entre los terminales y dispositivos controladores de llamadas.**

Los terminales pueden ser Gateways, Teléfonos IP, PC, Servidores o cualquier dispositivo que pueda iniciar y terminar una llamada de telefonía IP.

El controlador de llamadas se denomina GATEKEEPER en redes H.323 y PROXY o REDIRECT SERVERS en redes SIP.

Ventajas: Es más flexible. Permite tratar las aplicaciones de telefonía IP como cualquier otra aplicación IP. Permita agregar inteligencia a cualquier terminal y dispositivo de control de llamadas, dependiendo de los requerimientos del negocio que se está implementando y de la tecnología de la red. Los ingenieros de redes IP se encuentran más a gusto en este ambiente.

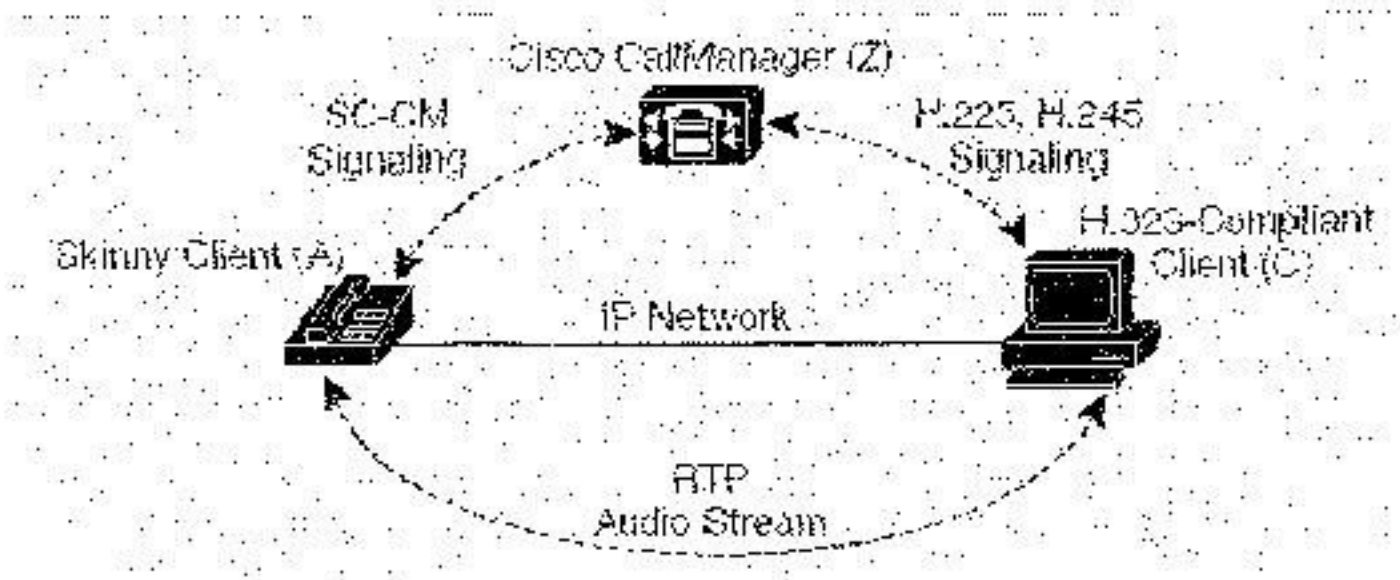
Desventajas: Sus detractores critican la mayor complejidad. Además indican que la infraestructura de PSTN es el único modelo que debiera usarse cuando se trata de replicar los servicios de voz existentes.

La empresa CISCO desarrolló el protocolo propietario llamado **"Skinny Client Control Protocol" (SCCP),** que como su nombre lo indica (1) destaca por ser un protocolo liviano.

- SCCP sigue el modelo maestro – esclavo (arquitectura centralizada)
- Se emplea principalmente para el control de los teléfonos IP Cisco.
- Los teléfonos IP Cisco con SCCP, son clientes del servidor Call Manager y se comunican durante la fase call setup de la llamada a dicho servidor utilizando el protocolo SCCP para el intercambio de los parámetros de control de la llamada
- Los payloads provenientes de la aplicación SCCP se transmite sobre IP
- Los clientes Skinny (teléfonos IP) para establecer, supervisar y deshacer las llamadas pueden también interoperar con terminales H.323, a través de un proxy H.323 (generalmente el mismo Call Manager)
- Existen modelos de teléfonos IP de bajo costo que funcionan en protocolo SCCP. Otra ventaja de SCCP es que ya se han desarrollado muchas facilidades para las existentes en la red PSTN.

(1) Skinny = ligero, escuálido. No confundir con protocolo de capa transporte SCTP para SIGTRAN

audio directly between each other.

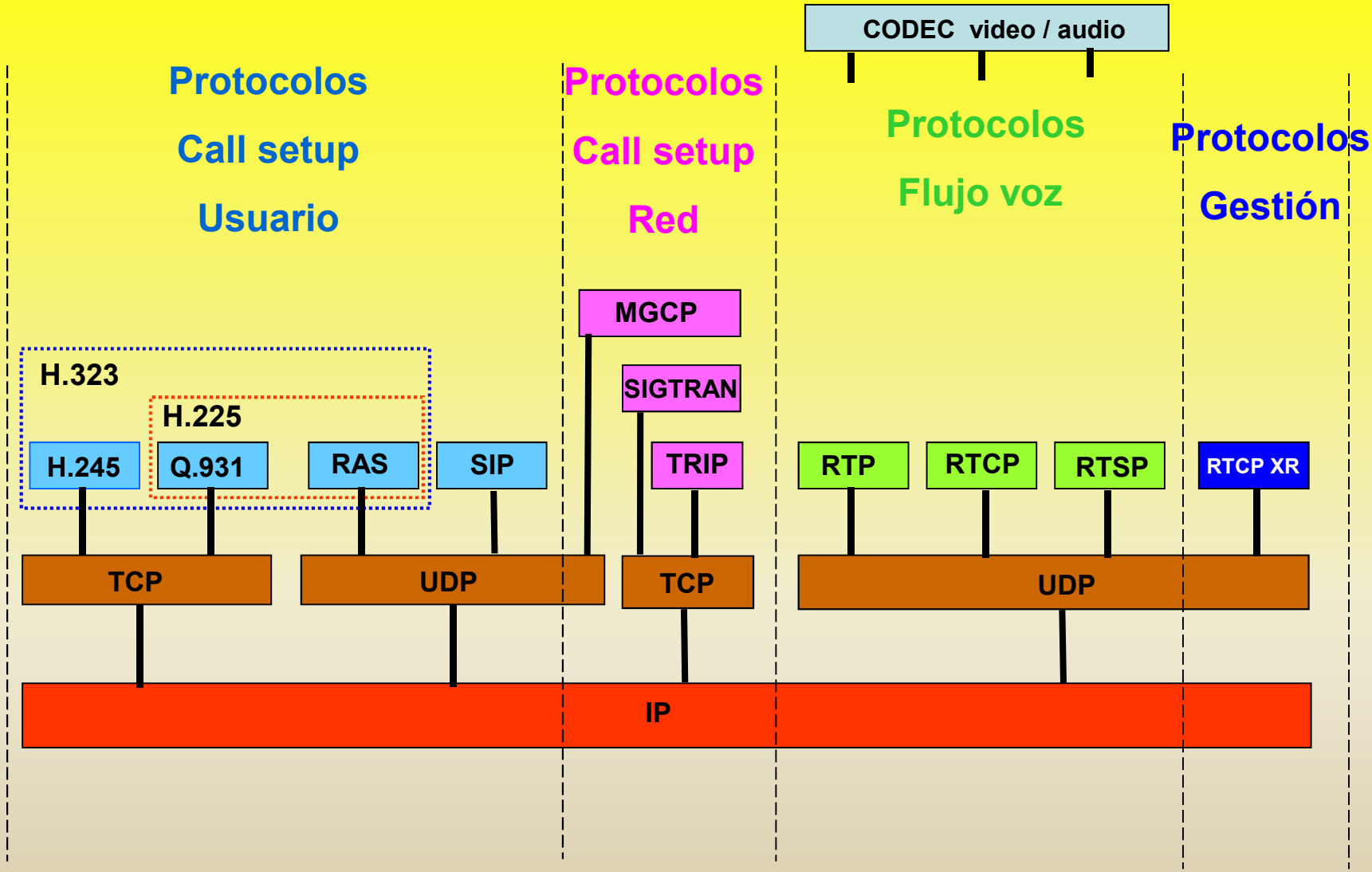


Los protocolos de señalización o call setup se pueden clasificar según ellos sean utilizados para señalización de usuario o para señalización de red.

La siguiente figura resume los protocolos según esta clasificación.

El protocolo TRIP (RFC 3219) provee un medio para que los nodos de la red TCP/IP, a través de servidores de localización (Location Servers), ubiquen el Gateway adecuado. TRIP es un **protocolo diseñado para ser usado entre operadores**. Permite conocer la accesibilidad, negociar las aptitudes y especificar los atributos de los Gateways que participan en la comunicación. Como subproducto, TRIP entrega a los operadores información estadística valiosa para dimensionar las redes.

TRIP = Telephone Routing over IP


CODEC video / audio
Protocolos
Call setup
Usuario
Protocolos
Call setup
Red
Protocolos
Flujo voz
Protocolos
Gestión
MGCP
SIGTRAN
H.323
H.225
H.245
Q.931
RAS
SIP
TRIP
RTP
RTCP
RTSP
RTCP XR
TCP
UDP
TCP
UDP
IP

Real-time Transport Control Protocol (**RTCP**) se definió en RFC 3550, la que reemplazó a RFC 1889.

RTCP **permite controlar la información de flujos RTP** (control "fuera de banda"). Se usa para transmitir periódicamente control de la transmisión de los paquetes a los participantes de la sesión multimedia

Provee feedback sobre la calidad de servicio que está siendo proporcionada por RTP

Real Time Streaming Protocol (**RTSP**), desarrollado por IETF y especificado en RFC 2326 (año 1993), es un protocolo que se usa en sistemas"streaming media"[1], **que permite al cliente controlar remotamente el servidor streaming media**, en forma similar a lo que hacemos con los comandos "play" y "pause" en un reproductor de DVD, permitiendo acceso "time-based" al servidor.

(1) La tecnología streaming media permite procesar contenidos multimedia (música , vídeo) sin necesidad de esperar a que éstos se descarguen completos al disco duro para iniciar su escucha o visualización.

5.2.2 Protocolo H.323 (ITU-T)

H.323

La versión 1 de H.323 se publicó en 1996. Luego en 1998 se publicó la versión 2, en 2006 la versión 6. En cada nueva versión se han ido introduciendo mejoramientos que han agregado facilidades de la telefonía tradicional en la telefonía IP, como por ejemplo transmisión de fax, servicios suplementarios (H.450), conferencia de llamados, etc.

H.323 prevé la transmisión en tiempo real de video y audio por redes de paquetes.

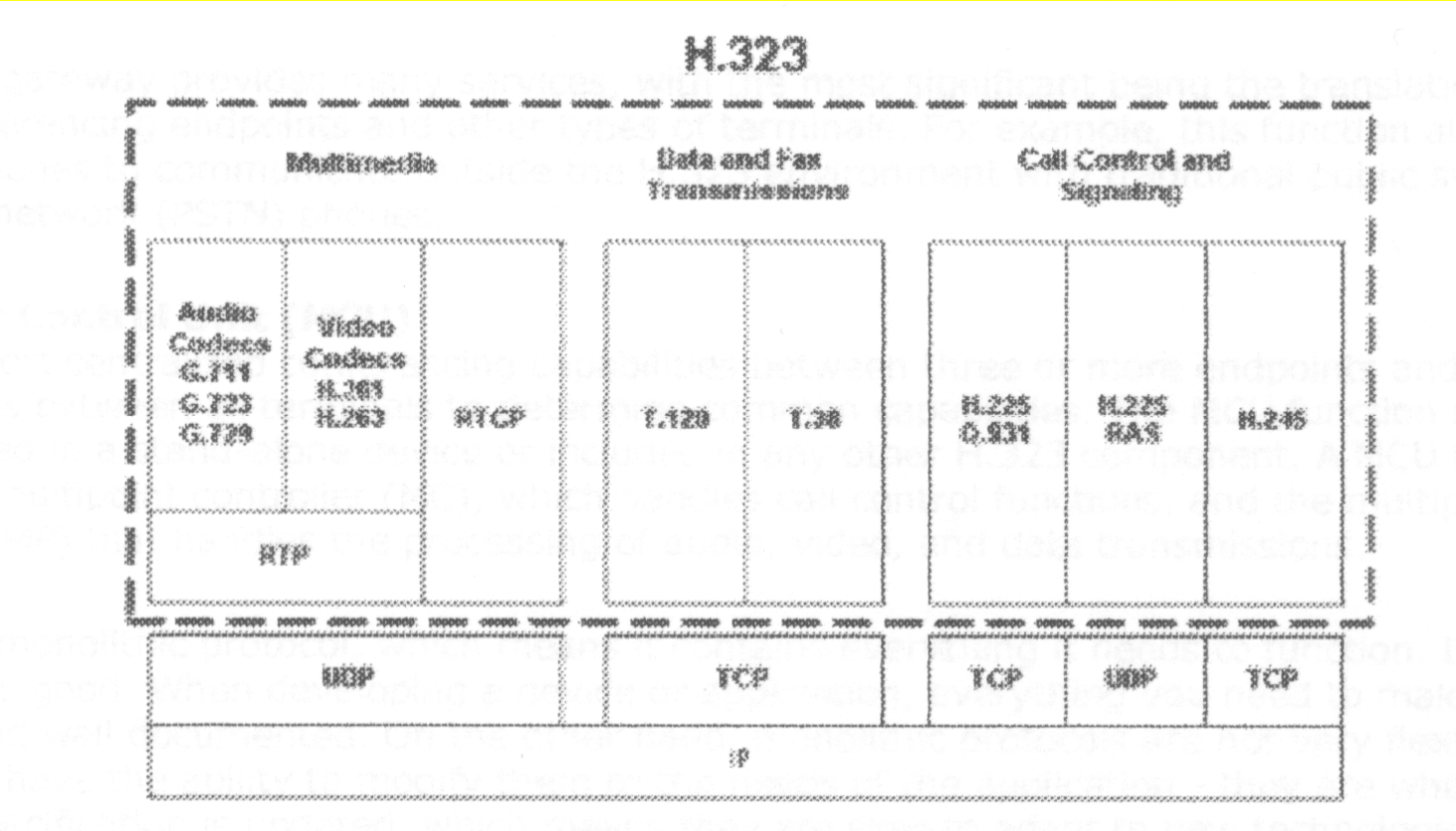
H.323

- Especifica mecanismos para el establecimiento, supervisión y disolución de los flujos de información, incluyendo los flujos de información de audio, entre dos terminales que cumplen H.323.
- Usa modelo peer to peer.
- H. 323 es realmente una familia de estándares, para telefonía y multimedia, incluyendo voz y videoconferencias. H 323 está compuesto por varios protocolos diferentes.
- H.323 es robusto y monolítico, es decir contiene todo lo necesario para funcionar. Esto es bueno y malo. Malo porque es poco flexible, de adaptación lenta a nuevas tecnologías.

H.323

- La familia H.323 ha ido siendo perfeccionada durante años, y como resultado ya ha alcanzado gran robustez
- Pero el costo de su robustez se paga con un alto overhead: una sesión incluye gran cantidad de handshakes y datos intercambiados para ejecutar cada función
- H.323 es ampliamente utilizado.
- H.323 se puede utilizar tanto en arquitectura centralizada como distribuida.
- H.323 utilizado en arquitectura distribuida, permite a los operadores construir redes escalables, flexibles, redundantes
- H.323 provee mecanismos para la interconexión con otras redes IP y permite que la inteligencia de la red resida o en los terminales o en los Gatekeepers

Protocolos H.323



H.323 es un conjunto de normas que especifican COMPONENTES, PROTOCOLOS y PROCEDIMIENTOS para soportar comunicaciones multimedia sobre redes de conmutación por paquetes.

H.323 cubre varios sub-protocolos que tienen que ver con el ESTABLECIMIENTO de las llamadas y la señalización a través de redes LAN y WAN.

Componentes de H.323

Se distinguen cuatro componentes principales:

TERMINAL: Corresponden a los dispositivos extremos de red capaces de proveer comunicaciones en tiempo real y full-duplex. Un terminal puede estar constituido por un simple teléfono IP o un computador con software con funcionalidades H.323. Los dispositivos “terminales” deben soportar software Call Setup, protocolo RTP, CODECs y stack TCP/IP. Como opción pueden disponer de software para comunicaciones de video.

GATEKEEPER: **Cuando esta entidad está presente**, todo dispositivo H.323 debe registrarse en ella antes de iniciar la comunicación con otro dispositivo H.323. El registro se realiza utilizando protocolo RAS (Registration, Admission, Status) sobre UDP, el que es parte de la especificación H.225. Desde el punto de vista lógico, el Gatekeeper está separado de los terminales H.323, pero sus funciones pueden cohabitar en el Gateway y en el multipoint control unit (MCU).

En nomenclatura H.323 **el Gatekeeper es el controlador de llamadas. Tiene asignadas varias funciones como control de admisión de los usuarios, traducción de número telefónico a dirección IP, gestión de Ancho de Banda, gestión de zona, etc.**

GATEWAY: Esta entidad provee varias funciones, entre las cuales la más importante es la **traducción entre terminales H.323 y otros tipos de terminales**. Así por ejemplo tiene la funcionalidad para la comunicación de terminales telefónicos IP con terminales telefónicos tradicionales ubicados en la Red Telefónica Conmutada Pública (PSTN).

MULTIPOINT CONTROL UNIT (MCU): Soporta en forma centralizada las **capacidades de conferencia de tres o más extremos que establecen una conferencia**, y maneja las negociaciones entre los terminales para determinar las capacidades comunes. Las funcionalidades MCU pueden residir en una entidad independiente o estar incluidas en cualquier otro componente H.323

MCU tiene dos partes principales: Multipoint Controller (MC), que maneja las funciones de control de llamada y Multipoint Processor (MP) que maneja el procesamiento de audio, video y transmisión de datos

H.323 trabaja bien en aquello para lo que fue diseñado: comunicaciones multimedia entre dispositivos conectados a una red de paquetes. Sin embargo cuando se creó, no se tuvo in mente **gran cantidad de usuarios**, por lo que sus versiones más nuevas ha debido superar limitaciones que fueron apareciendo cuando se usa en redes WAN.

Los diferentes protocolos a que se refiere la recomendación H.323 son usados en las diferentes fases de la comunicación. Así por ejemplo, en la primera fase, en que el abonado llamante inicia la comunicación, se utilizan los protocolos de **registro, admisión y estatus (RAS)** que especifica la recomendación **H. 225.0**.

La **señalización** entre terminales A y B se hace de acuerdo a las especificaciones **Q.931 y H.225.0**

El **control de la sesión**, que incluye la negociación entre A y B para **decidir el CODEC** que se utilizará durante el flujo RTP, el intercambio de mensajes para **control de flujo** y otras funciones de control de sesión, se hace siguiendo las especificaciones **H.245**

Los protocolos generan mensajes, los que como hemos visto, se parcelan en unidades de datos (payloads) para efectos de transmitirlos por la red de datos.

En H.323 se dice que el intercambio de mensajes durante las distintas fases de la comunicación (establecimiento, conversación, término) se hace por los siguientes canales lógicos:

Canal lógico RAS

Canal lógico de señalización

Canal lógico de control

Canal lógico RTP

Mensajes RAS/H.225 usados para Registration, Admission, Status

Usados durante diálogo entre terminal H.323 y Gatekeeper orientado al registro, autorización y control de estado del terminal H.323 en la red. Este diálogo se efectúa por el llamado "canal lógico RAS" que se establece en toda comunicación

Ej. **ARQ Admission ReQuest**

ACF Admission ConFirmation

Mensajes Q.931/H.225 usados para enrutamiento de la llamada

Usados para la señalización propiamente tal, la que se basa en el protocolo RDSI Q.931 En toda comunicación telefónica se establece un "canal lógico de señalización" por el cual se realiza este diálogo

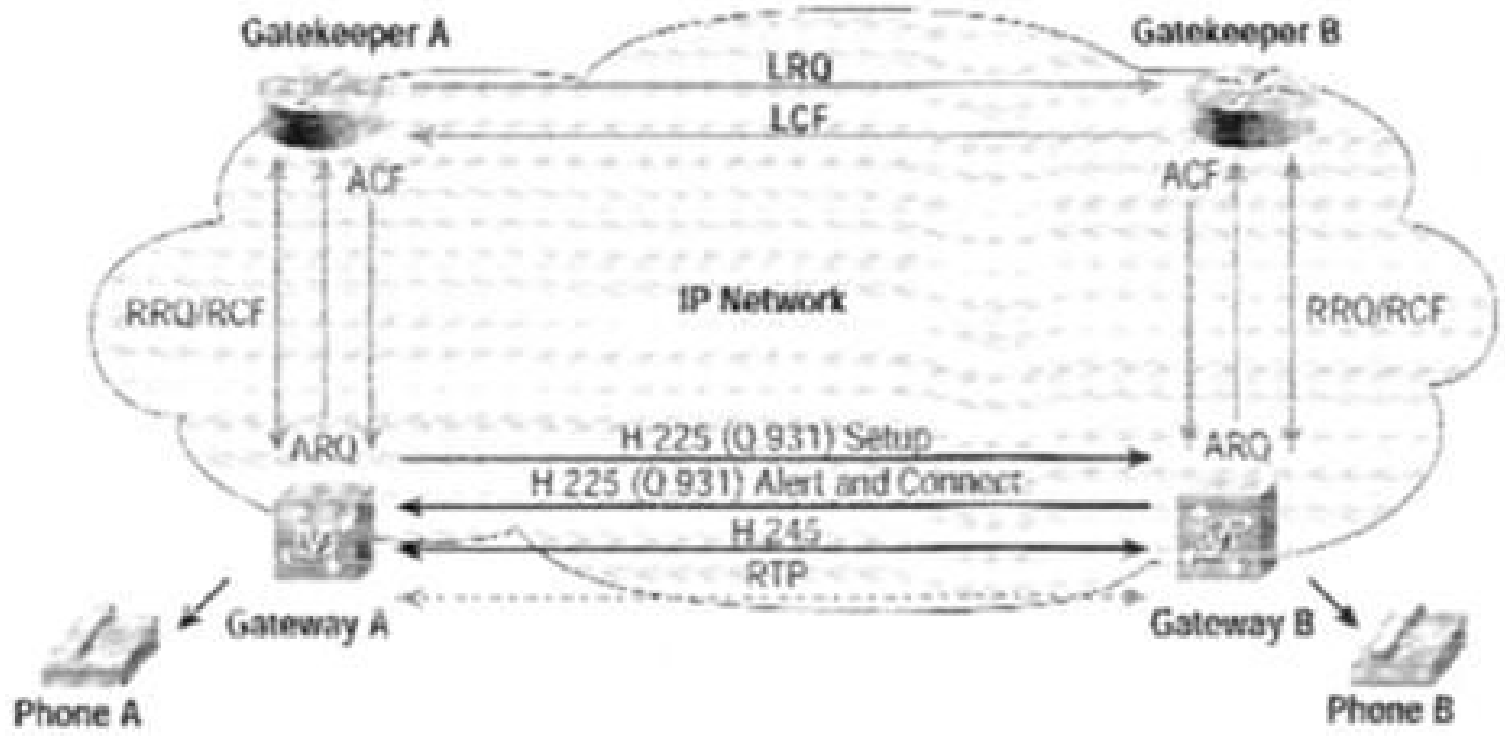
Ej. CONNECT (B descolgó)

Mensajes H.245 usados para control de la sesión

Mediante ellos las entidades se informan y deciden las capacidades a utilizar en la comunicación. Los mensajes fluyen por el "canal lógico de control"

Ej. maximumDelayJitter
alternateGatekeeper
Terminal CapabiliteSet (solicita datos del terminal como por ej. tipo de codec)

La figura siguiente muestra el flujo de señales durante el establecimiento de una comunicación H.323


Gatekeeper A
Gatekeeper B
LRQ
LCF
ACF
ACF
RRQ/RCF
IP Network
RRQ/RCF
ARQ
H 225 (Q 931) Setup
ARQ
H 225 (Q 931) Alert and Connect
H 245
RTP
Gateway A
Gateway B
Phone A
Phone B

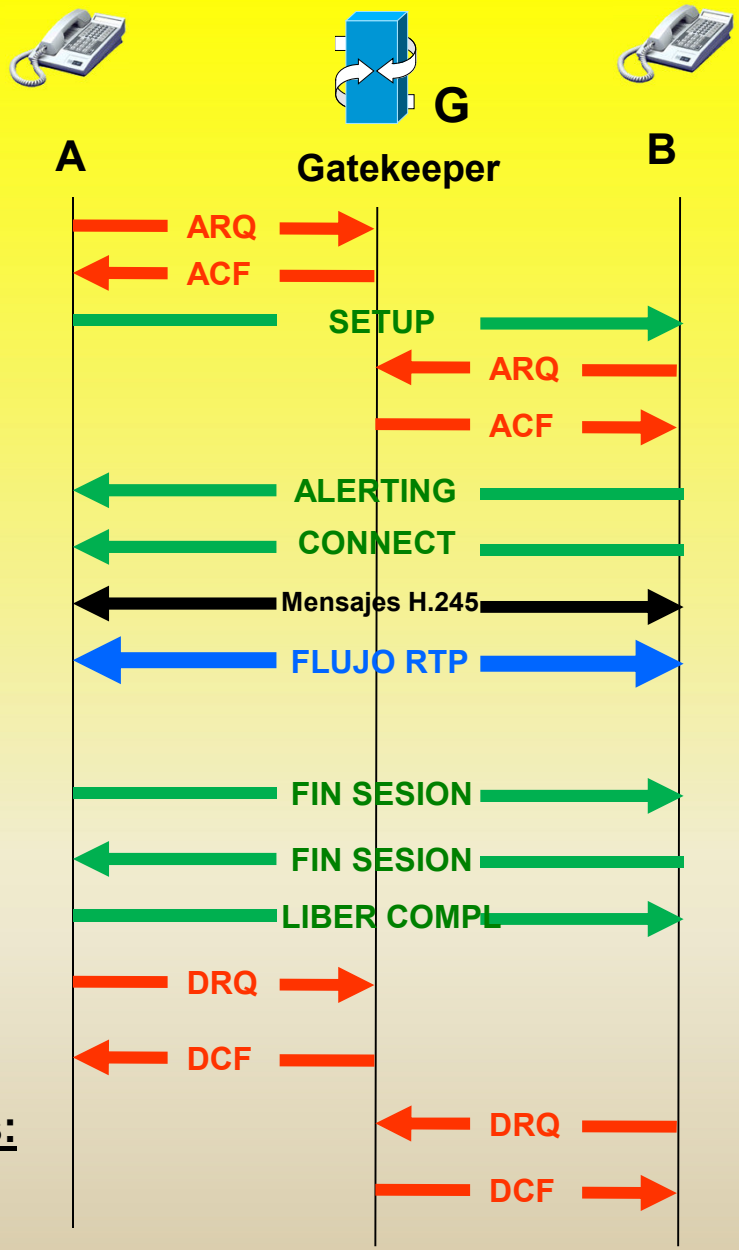
LRQ (Location_Request): Sent to request the gatekeeper contact information for one or more E.164 addresses.

LCF (Location_Confirm): Sent by the gatekeeper and contains the call signaling channel or RAS channel address of itself or the requested endpoint. LCF uses its own address when GKRCS is used. LCF uses the requested endpoint address when Directed Endpoint Call Signaling is used.

LRJ (Location_Reject): Sent by gatekeepers that received an LRQ for which the requested endpoint is not registered or has unavailable resources.

Fuente: http://www.cisco.com/en/US/tech/tk1077/technologies_tech_note09186a00800c5e0d.shtml

La figura siguiente muestra el flujo de señales durante una comunicación H.323 en un caso simple, en que los dos terminales pertenecen al mismo Gatekeeper



ARQ Admission ReQuest

ACF Admission ConFirmation

Nomenclatura

Mensajes Registration, Admission and Status (RAS) (H.225.0)

Mensajes Q.931

Mensajes control sesión (H.245)

Flujo RTP (entre CODEC)

DRQ Disengage ReQuest

DCF Disengage ConFirmation

A solicita a G iniciar llamada

Permiso concedido

Establecimiento llamada

B solicita a G recibir llamada

Permiso concedido

Campanilla de B sonando

B contestó

A y B negocian CODEC y otros

A y B conversan

A cuelga

B cuelga

Fin de la llamada

A informa a G fin llamada

G confirma recepción DRQ

B informa a G fin llamada

G confirma recepción DRQ

Cuatro canales lógicos:

RAS

Señalización

Control de la sesión

RTP

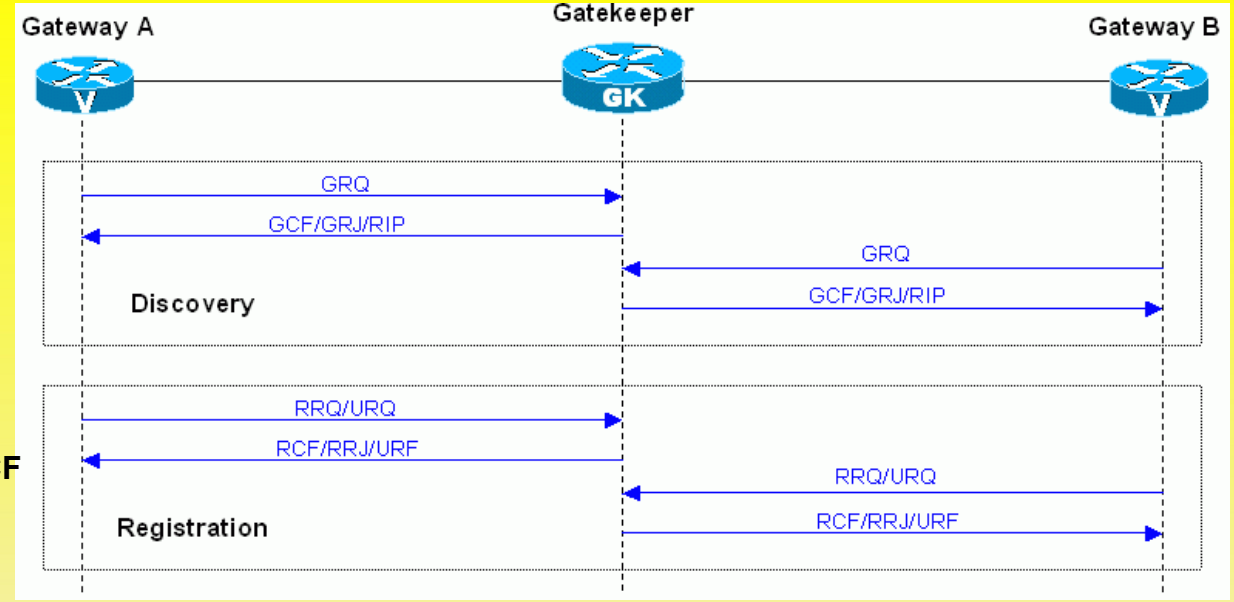
Cuando hay más de un Gatekeeper, previamente es necesario que el gateway "descubra" cual será el gatekeeper, que atenderá la solicitud.

El gateway envía mensajes tipo broadcast para "descubrir" que gatekeeper lo atenderá. Luego envía al gatekeeper que confirmó que lo atenderá, un mensaje solicitud de registro en ese gatekeeper.

Así se distinguen las etapas Discovery y Registration.

Gatekeeper Request GRQ
Gatekeeper Confirmation GCF

Registration Request RRQ
Registration Confirmation RCF



Caso registro de GW en GK

Intercambio de información para mantener activa la comunicación entre los Gateways (GW) y el Gatekeeper(GK). Se distinguen etapas Discovery y Registration:

Discovery: El GW determina ("descubre") cual es el GK que atenderá la solicitud. El GW manda paquetes multicast "Gatekeeper Request" (GRQ). El GW responde aceptando con "GK Confirmation" (GCF) o rechazando "GK Reject" (GK Reject). También puede solicitar más tiempo con "Request In Progress" (RIP) que resetea el timeout

Registration: El GW informa al GK su dirección enviando en forma periódica y solamente durante cierto tiempo, "Registration Request" (RRQ). El GK responde "Registration Confirmation" (RCF) o "Registration Reject" (RRJ).

El GW o el GK pueden solicitar cancelar la registration solicitada mediante "Unregister Request" (URQ), la que es respondida con "Unregister Confirmation" (URF).

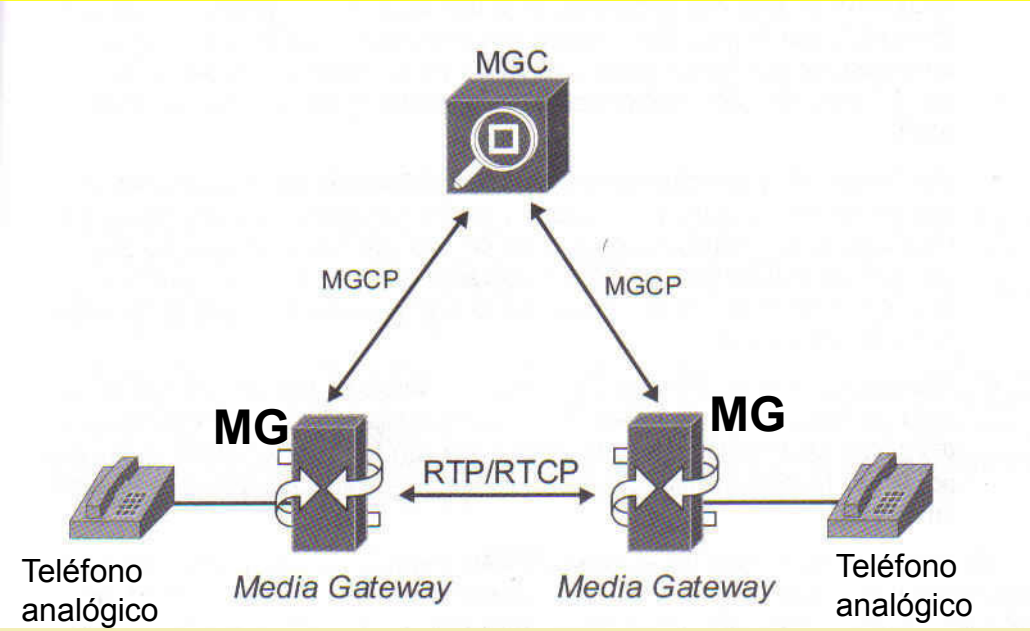
Hasta aquí H.323

Seguiremos ahora con el estudio de otros protocolos de telefonía IP

Los protocolos MGCP y MEGACO / H.248 que estudiaremos a continuación fueron diseñados para proveer una arquitectura donde los servicios y el control de las llamadas pueden ser agregados a una red de datos existentes, **en forma centralizada.**

En este sentido, una arquitectura que usa MGCP ó MEGACO / H.248, se parece a la arquitectura y a los servicios de la PSTN.

5.2.3 Protocolo MGCP (IETF ITU-T)



MG: Media Gateway. Entidades con poca inteligencia, esclavas de MGC. Corresponde a la entidad Gateway del protocolo H.323

MGC: Media Gateway Controller. Servidor que controla uno o más MG, en modalidad cliente-servidor

MGCP: Media Gateway Control Protocol es el **protocolo** para la comunicación entre MGC y MG

El modelo MGCP simplifica a máximo las entidades que realizan la función gateway, aquí denominada MG

Las funciones de los MG se limitan a:

- Enviar SEÑALES al MGC, para reportar los eventos que ocurren en los terminales. Las ***señales*** son mensajes a través de los cuales los MG transmiten información al MGC que los controla.
- Ejecutar los COMANDOS que recibe del MGC. Los ***comandos*** son mensajes con órdenes que el MGC envía a los MG
- Interface entre la red IP y la red TDM de conmutación de circuitos

El protocolo MGCP es simple. Define una cantidad reducida de SEÑALES y COMANDOS

- En el desarrollo del protocolo Media Gateway Control Protocol (MGCP) se han aprovechado esfuerzos del IEFC y de la ITU-T

- MGCP permite controlar y administrar externamente dispositivos que cumplen la función Media Gateway (MG): interface entre redes disímiles (entre una red TCP/IP y la red telefónica pública con conmutación de circuitos)

- MGCP fue diseñado específicamente para la comunicación, a través de redes TCP/IP, entre Media Gateways y el Media Gateway Controller (MGC) del cual dependen.

- Los mensajes MGCP usan protocolo de transporte UDP

COMANDOS MGCP

EndPointConfiguration	MGC configura el terminal, por ej. estableciendo el tipo de CODEC a utilizar
NotificationRequest	MGC solicita a MG notificar eventos
PollNotify	MGC solicita comprobar la notificación
AuditEndPoint	Solicita configuración e información de estado de un terminal
AuditConnection	Solicita información del estado de una conexión
CreateConnection	Crea conexión entre terminales
ModfyConnection	Modifica parámetros de una conexión existente
DeleteConnection	Libera conexión

SEÑALES MGCP

Notify	MG avisa a MGC que ha ocurrido algún evento
DeleteConnection	MG avisa a MGC que se liberó la conexión
RestartInProgress	MG informa que uno o más terminales están pasando a estado fuera de servicio

Los comandos y señales MGCP incluyen parámetros.

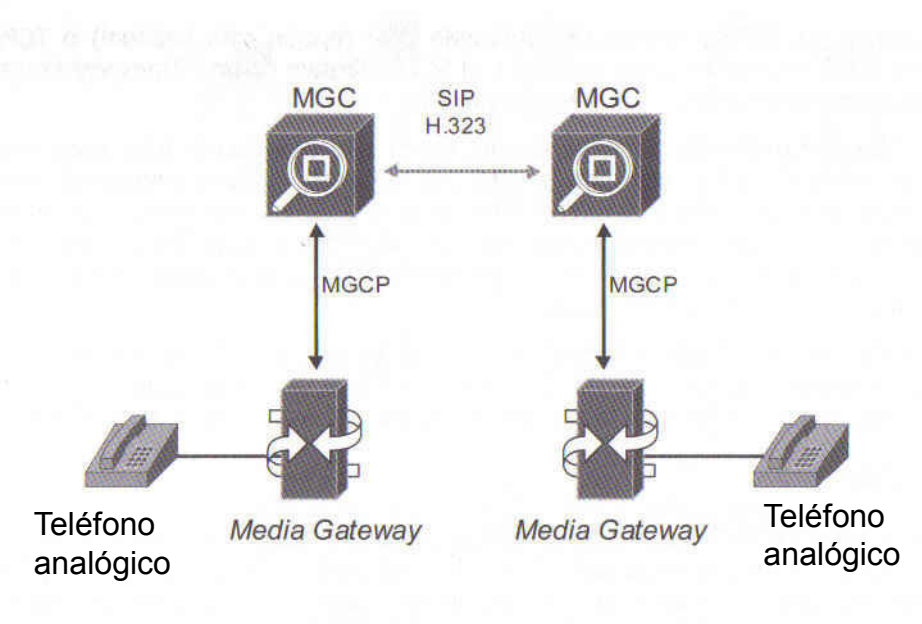
Los parámetros contienen la información específica que se transfiere entre MG y MGC

Para mayores detalles ver RFC 2705

- MGCP puede ínter operar con H.323 y SIP para crear conexiones entre Media Gateways, permitiendo una conexión extremo-extremo a través de redes disímiles

- MGCP no es alternativa de SIP ni de H.323. En realidad SIP y H.323 proveen el control de la comunicación mientras que MGCP controla los Media Gateways involucrados en dicha comunicación

- MGCP incluye norma alternativa a H.323 para la conversión de audio TDM a paquetes IP



Se tiene entonces que en la modalidad MGCP

- Un Media Gateway (MG) típico es el adaptador ATA, que permite el uso de teléfonos POTS en telefonía IP. Otro MG típico es el que realiza la función interface entre redes PSTN y TCP/IP
- Los Media Gateway realizan la función de convertir las señales analógicas tradicionales en formato paquetes y viceversa, durante las fase de señalización y conversación de una comunicación telefónica.
- El MG actúa como esclavo del MGC, al que informa la aparición de eventos en los terminales, enviando mensajes llamados señales, por ejemplo señal de que el teléfono descuelga.
- El MGC instruye al MG sobre las acciones que debe realizar, enviándole comandos a través de la red IP, por ejemplo poner tono de marcar al usuario
- El protocolo MGCP especifica la forma en que se realiza la comunicación tipo maestro-esclavo, y garantiza que el terminal tonto y el centro de inteligencia (MGC) se comuniquen adecuadamente
- Cuando el MGC decide la participación de otro MGC u otro servidor de llamadas como lo es una PBX IP, entonces utiliza protocolo SIP ó H.323 para dialogar con estos dispositivos.

Teléfono A descuelga

MG A informa a MGC que A solicita atención

MGC acepta la notificación y ordena poner dial tone

MG A envía a MGC dígitos

MGC ordena a MG A crear conexión con MG B

MG A acepta crear conexión

MGC ordena a MG B crear conexión con MG A

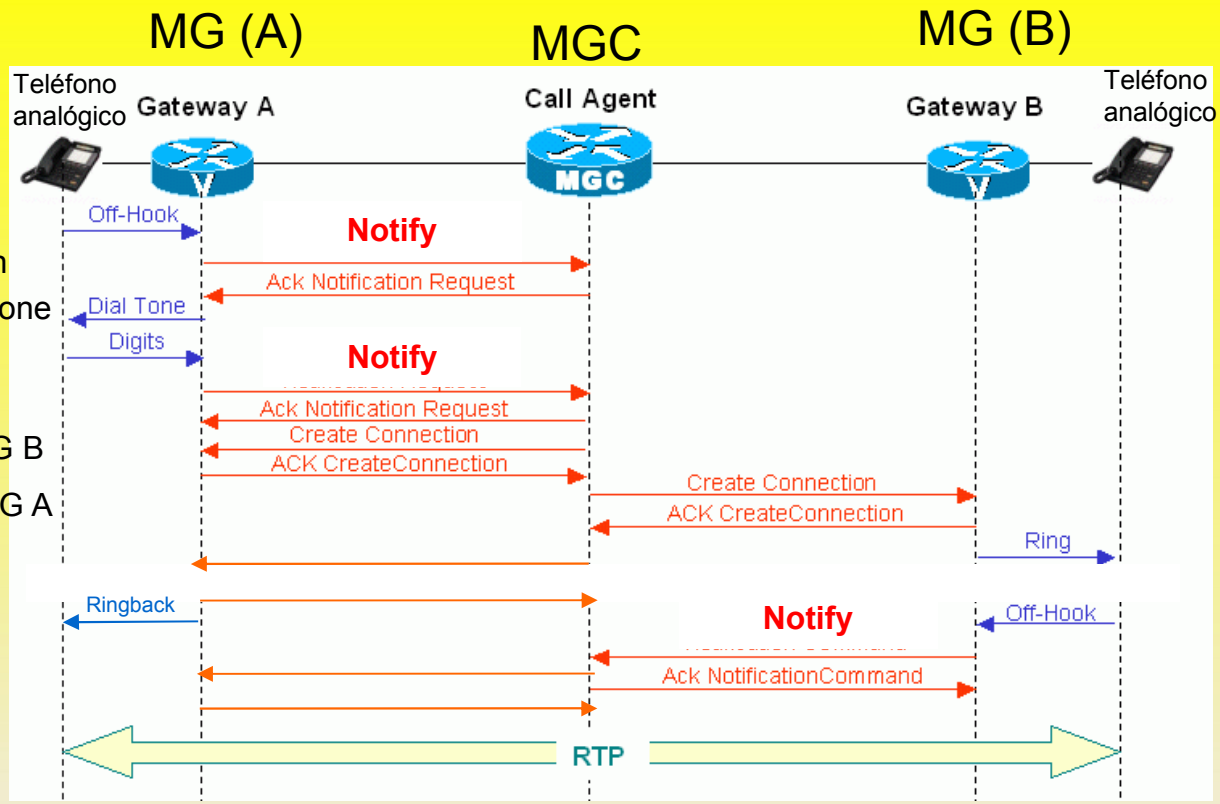
GW B acepta crear conexión

MGC ordena a MG A poner ringback

B descuelga

MGC ordena a MG A quitar ringback

Conversación: flujo RTP



Comunicación con protocolo MGCP

ENTIDAD SG Y PROTOCOLO SIGTRAN

Como se dijo, en el modelo MGCP se simplifican a máximo las funciones asignadas a los Gateways (MG).

Por esta razón se hace conveniente distinguir una nueva entidad a la que se asigna la funcionalidad de GATEWAY de SEÑALIZACION (SG).

Esta nueva entidad SG, es capaz de entender los protocolos de señalización:

a) SS7 utilizado en red telefónica tradicional de circuitos y

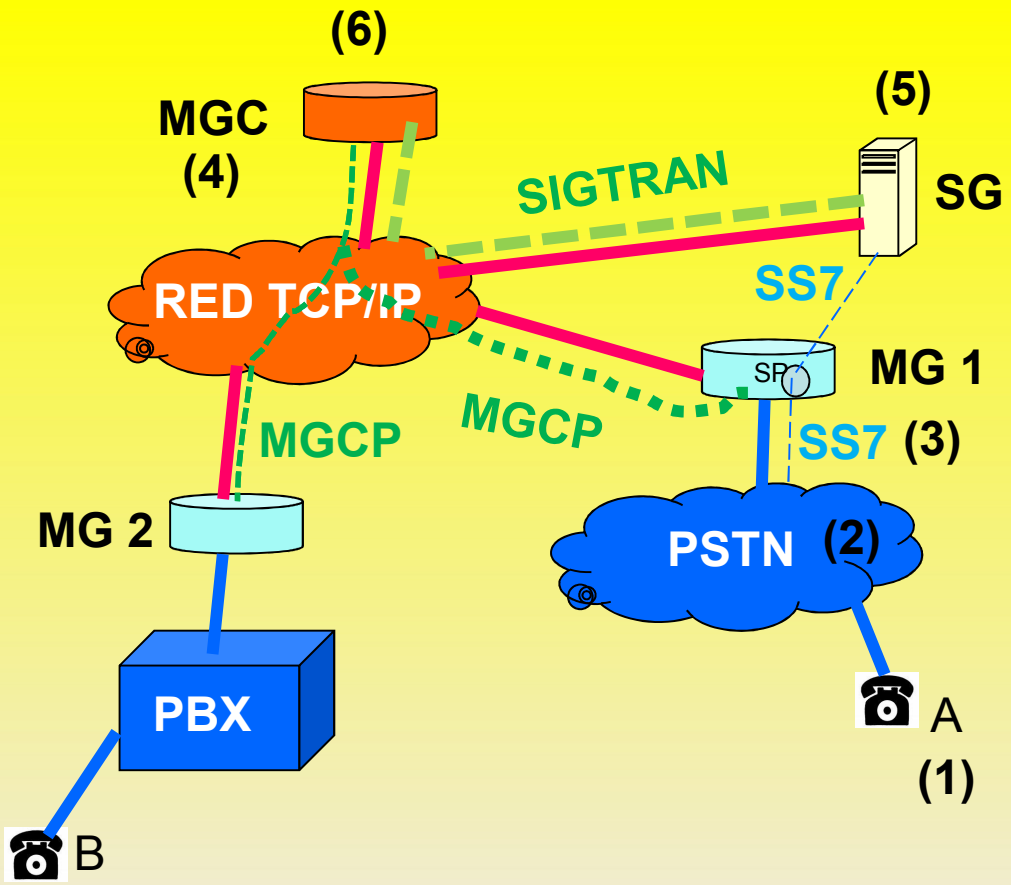
b) un protocolo adecuado a redes TCP/IP utilizado en los MGC

El protocolo indicado en b) corresponde a SIGnalling TRANsport, tradicionalmente conocido como SIGTRAN.

SIGTRAN a partir de los mensajes SS7 recibidos de la red de circuitos, genera paquetes IP que envía a MGC, y viceversa.

SIGTRAN utiliza en la capa de transporte TCP ó SCTP (Stream Control Transport Protocol)

Se suele decir que SIGTRAN corresponde a SS7 sobre IP.



1) A descuelga, es atendido por la PSTN

2) La red PSTN determina que en el establecimiento de la llamada debe participar el Signalling Point (SP) del MG 1 e inicia el envío de mensajes SS7 a dicho SP

3) El MG 1 no es capaz de traducir los mensajes SS7 al protocolo MGCP, con el cual se comunica con su MGC

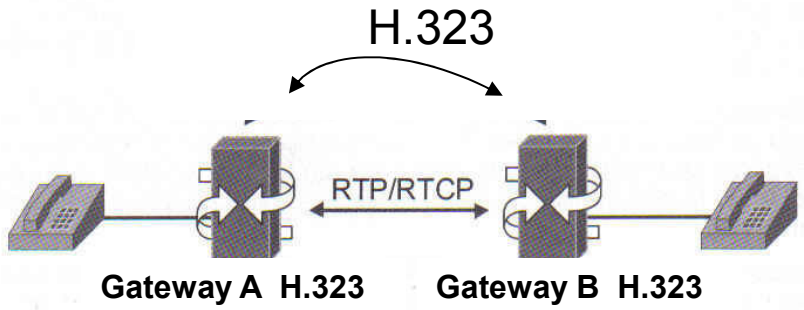
4) MGC ordena al MG 1 enviar los mensajes SS7 al SG

5) SG dialoga en SS7 con el SP de MG 1. Para dialogar con MGC traduce SS7 a SigTran y viceversa.

6) MGC a partir de la información entregada por SG, envía comandos y recibe señales MGCP a MG 1 y MG 2 asociado en sus bases de datos con el Nº B recibido desde SG

Diferencias H.323 --- MGCP

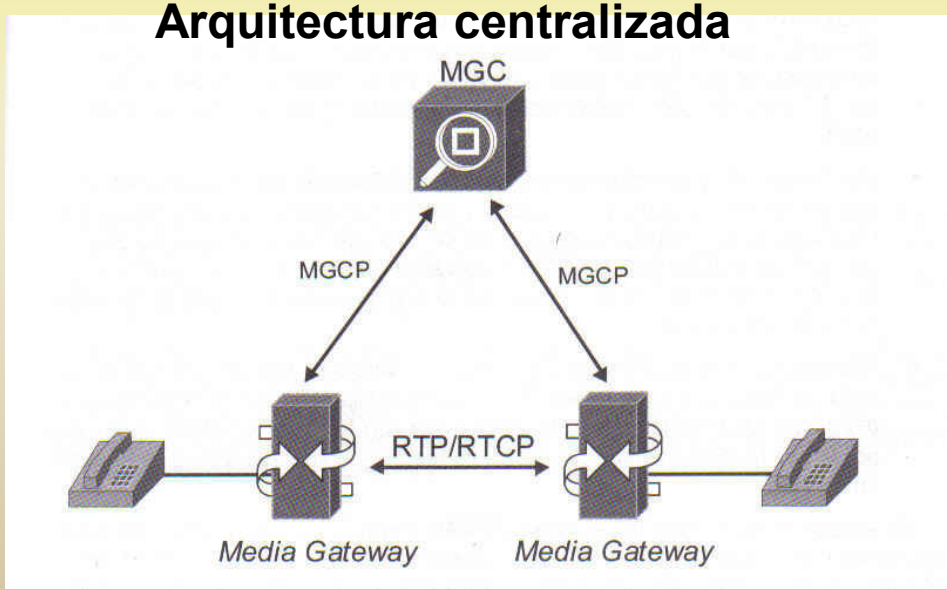
H.323: Gateways inteligentes
Peer-peer
Arquitectura descentralizada



El Gateway A determina la forma en que se enrutará la llamada. En caso que exista GK como entidad separada, GW A cuenta con su ayuda.

Los GW negocian la configuración de los terminales. Teniendo como base la información H.323 intercambiada, el Gateway B decide llamar al abonado B.

MGCP: MG sólo hacen funciones básicas
Maestro / esclavo
Arquitectura centralizada



MG de origen notifica a MGC

MGC determina como será cursada la llamada, las configuraciones de los terminales, etc. y envía comandos MGCP a ambos MG

5.2.4 Protocolo MEGACO / H.248 (IETF ITU-T)

- MEGACO (MEdia GAteway COntrol) se ha desarrollado a partir de MGCP, en forma conjunta por la ITU-T y por IETF. Es una versión más avanzada de MGCP (mayor cantidad de comandos)

- La ITU-T lo denomina H.248 mientras que IETF lo llama MEGACO (RFC 3525)

- MEGACO, al igual que MGCP permite la comunicación de MG y MGC a través de redes de paquetes IP, pero además por redes basadas en celdas (ATM)

- MEGACO es parte de la solución de protocolo Call Setup:
  - Controla el Call Setup en la comunicación entre MGC y MG
  - En caso de requerirse comunicación entre MGC, se emplea SIP, H.323 u otro

5.2.5 Protocolo SIP (IETF)

SIP = Session Initiation Protocol

- Los diseñadores del protocolo SIP trataron de responder preguntas como: ¿Para qué utilizar un protocolo pesado como el H.323 cuando para realizar bien el trabajo la mayor parte del tiempo basta un protocolo más liviano?

- El protocolo SIP actualmente es muy importante en la industria de las telecomunicaciones. Lo utilizan CISCO, Nortel y Microsoft. Hay sistemas operativos Windows de MS con interfaces cliente SIP

- SIP, al contrario de MGCP y MEGACO que se basan en configuración maestro-esclavo (MGC/MG), apuesta a una configuración de inteligencia distribuida en los Gateways, lo que tiende a eliminar la necesidad de MGC

SIP es un protocolo multimedia que fue diseñado pensando en aprovechar la experiencia existente en cuanto a arquitectura y a la forma de los mensajes, en las aplicaciones típicas que utilizan Internet como red de transmisión.

Es así como SIP utiliza arquitectura distribuida, mensajes basados en texto y denominación por URL.

> URL es acrónimo de Uniform Resource Locator y especifica como encontrar un recurso en Internet. La denominación URL no solo representa una dirección de Internet sino que apunta a un recurso concreto dentro de esa dirección (archivo, programa,..)

El protocolo SIP solo define la forma en que las sesiones se establecen y terminan.

Debe entonces apoyarse en otros protocolos IETF para definir otros aspectos de la telefonía IP y de las sesiones multimedia, tal como SDP para intercambiar aptitudes (tipo de Codec, jitter aceptable, etc.), URL para direccionar, Domain Name System (DNS) para localizar y Telephony Routing over IP (TRIP) para enrutar las llamadas.

El protocolo TRIP (RFC 3219) provee un medio para que los nodos de la red TCP/IP, a través de servidores de localización (Location Servers), ubiquen el Gateway adecuado. TRIP es un protocolo diseñado para ser usado entre operadores. Permite conocer la accesibilidad, negociar las aptitudes y especificar los atributos de los Gateways que participan en la comunicación.

Aunque el IETF ha hecho grandes progresos definiendo nuevas especificaciones (extensiones del SIP) que permiten que SIP interactúe con redes PSTN tradicionales, la motivación que se tuvo para diseñarlo fue crear un ambiente que soporte comunicaciones de próxima generación, que utilicen la red y las aplicaciones Internet.

Como es un protocolo que usa arquitectura distribuida, permite a los operadores construir grandes redes escalables, flexibles y redundantes.

Provee mecanismos para la interconexión con otras redes TCP/IP, ya sea agregando inteligencia y nuevas funcionalidades a los terminales o a los Servidores SIP Proxy o a los Servidores de Redirección.

ARQUITECTURA SIP

- Es una arquitectura distribuida en que se distinguen
  - AGENTE USUARIO CLIENTE (UAC)
  - AGENTE USUARIO SERVIDOR (UAS)
- Los UAC hacen PETICIONES (request) al servidor.
- Los UAS procesan las peticiones y envían RESPUESTAS (response)
- El diálogo entre CLIENTE y SERVIDOR es mediante el intercambio de mensajes de texto, durante una SESION que se establece entre ellos.
- Los mensajes tanto de peticiones como de respuestas son de texto y tienen una estructura sencilla, muy semejante a los utilizados por HTTP.

AGENTE USUARIO

Los Agentes Usuario son aplicaciones que residen en los terminales SIP.

Un Agente Usuario puede actuar tanto de Cliente como de Servidor

Un Agente Usuario típico es un teléfono SIP. Este actúa como UAC cuando inicia una llamada y como UAS cuando es la parte llamada en una comunicación telefónica.

También existen Agentes Usuario Recíprocos (B2BUA), que corresponden a aplicaciones que actúan como intermediarias entre dos partes, realizando simultáneamente las funciones UAS/UAC para procesar consultas durante sesiones

Los dispositivos SIP pueden comunicarse directamente entre ellos cuando conocen el URL del otro, sin embargo normalmente deben apoyarse en SERVIDORES SIP CENTRALES que proporcionan una infraestructura para servicio de registro, autenticación, autorización, ruteo.

SERVIDORES SIP CENTRALES

SERVIDOR PROXY

Es una entidad intermedia que recibe peticiones que puede contestar inmediatamente o tomar el rol de intermediario, caso en que actúa como cliente de otro servidor al que traspasa la petición.

De esta forma un Proxy puede actuar como Cliente y como Servidor, pero solamente durante el establecimiento y disolución de la comunicación.

SERVIDOR DE LOCALIZACION (o de ubicación)

Contiene información sobre la localización de los usuarios (enlaces URL)

SERVIDOR DE REDIRECCION

Recibe peticiones SIP para conocer direcciones nuevas del usuario llamado. Las mapea y devuelve como respuesta estas direcciones al cliente. Este servidor nunca inicia peticiones.

SERVIDOR DE REGISTRO

Provee servicios de registro de localización

- El protocolo SIP (Session Initiation Protocol) se usa para iniciar, modificar y terminar sesiones entre uno o más usuarios

  Sesión: Cualquier comunicación interactiva mediante datos, que se intercambian a través de Internet. La comunicación puede ser de voz, mensajes instantáneos, video, etc.

- El protocolo SIP fue desarrollado por IETF y es muy parecido al protocolo HTTP

  HTTP (HyperText Transfer Protocol): Este protocolo es ampliamente utilizado en la world wide web. Funciona enviando mensajes de tipo petición / respuesta para conectar usuarios con páginas web. Por Ej. al tipear www.subtel.cl el usuario envía una petición al servidor en que está la página web de Subtel. Como respuesta dicho servidor transmite de vuelta la página

- En forma similar, una petición SIP puede solicitar conexión con:
  sip:nombredelcomputador@ind.tiger.com
  sip:+7074440123@gateway.com
  sip:+7074440123
  Es así como a veces se requiere la ayuda de un servidor de resolución de dominio Domain Name Server (DNS)

- Tanto SIP como HTTP usan direcciones URL (Universal Resource Locator).
- Las direcciones URL describen la ubicación de la información en la web, por Ej. www.subtel.cl
- Cuando se usa SIP, incluso los números telefónicos son convertidos a direcciones URL
- Dada la similitud que tiene SIP con HTTP, es muy adecuado para ambiente IP
- Además tiene la ventaja que los expertos en HTTP lo pueden programar sin necesidad de estudiar un nuevo lenguaje
- Los mensajes SIP generalmente usan **UDP** como capa de transporte. Puerto 5060 UDP.
- Sin embargo también pueden usar como capa de transporte TCP ó SCTP
- Previo al establecimiento de la sesión entre cliente y servidor, estos deben ponerse de acuerdo sobre el tipo de sesión que se establecerá. Para esta funcionalidad se emplea una capa de nivel más alto que SIP: Session Description Protocol (SDP)

ESTRUCTURA DE LOS MENSAJES SIP

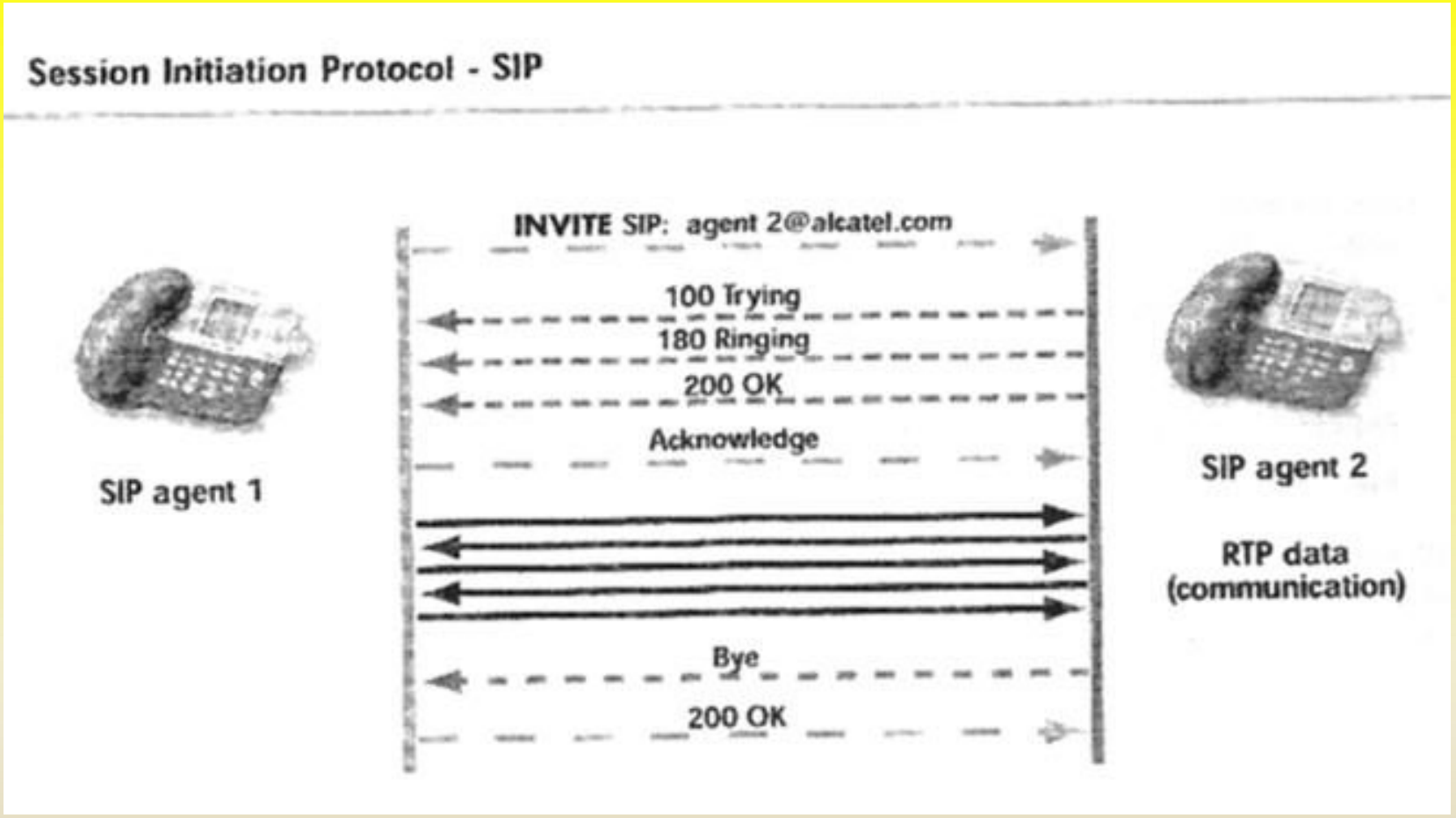
Start line	Indica tipo de petición o respuesta, versión SIP
General header	Contiene **Call-Id** propio de cada llamada para identificarla, **CSeq** número aleatorio para identificar cada request, **From** dirección de origen de la llamada, **To** dirección de destino de la llamada, etc.
Additionals	Campos adicionales con información como **expire**, **priority**, etc.

PETICIONES SIP

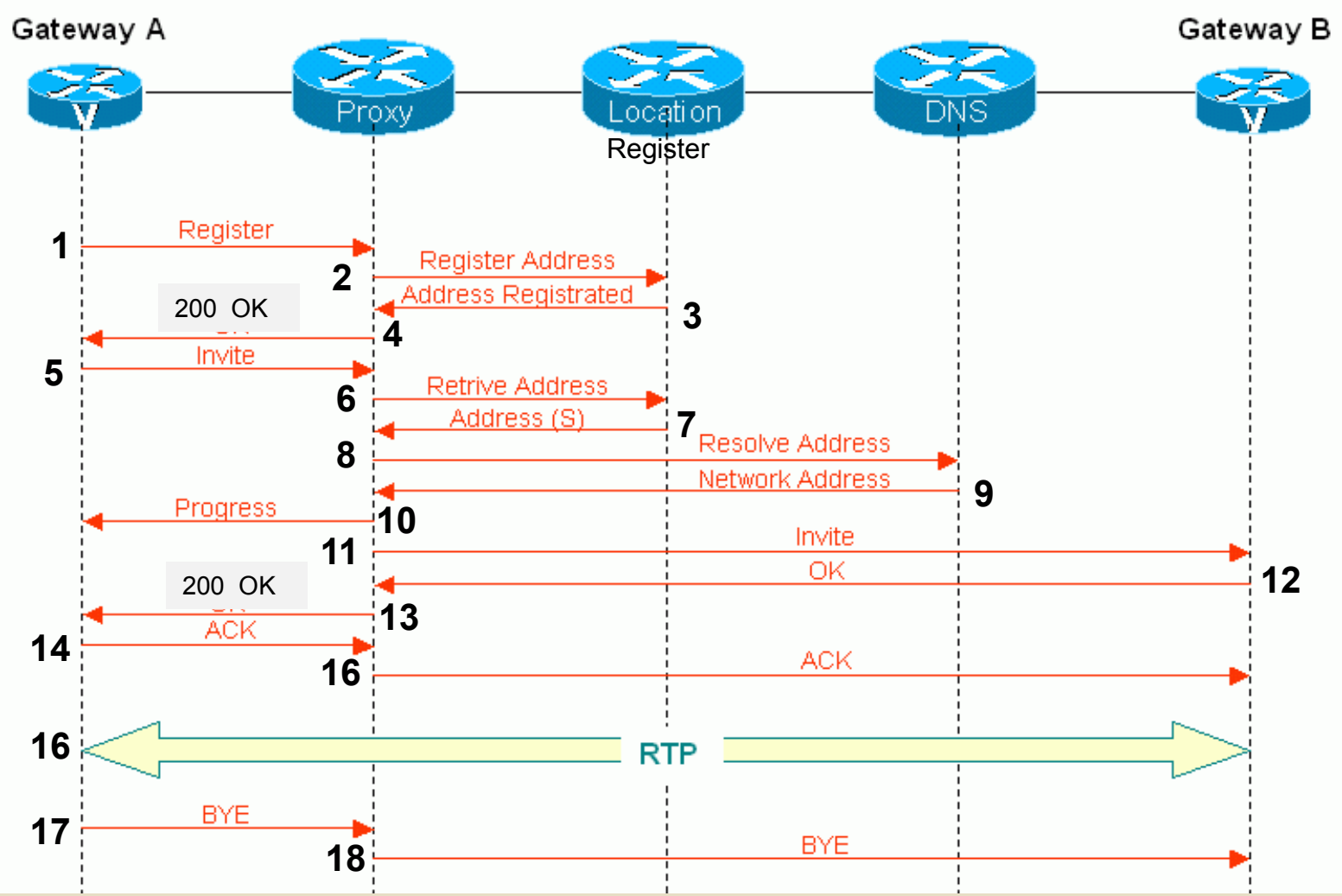
INVITE	Mensaje inicial que envía el llamante: Contiene direcciones de origen y destino
ACK	Confirma inicio sesión
BYE	Mensaje de terminación enviado por uno de los participantes
CANCEL	Mensaje que cancela una petición pendiente
REGISTER	Mensaje para registrar la dirección actual de contacto
OPTIONS	Mensaje a un cliente para solicitar sus capacidades (por ej. CODEC)
INFO	Mensaje con información como por ej. dígitos DTMF

RESPUESTAS SIP

1xx	Mensajes de información
2XX	Éxito
3XX	Mensajes de desvío
4XX	Error en la petición
5XX	Error en el servidor
6XX	Error general



Ejemplo de comunicación SIP. Caso simple, en que el llamante conoce el URL del llamado



Ejemplo de Comunicación SIP. Caso en que intervienen servidores centrales

1) Gateway A acude al Proxy para hacer su registro
2) Proxy hace petición de registro al servidor de registro
3) Servidor de registro comunica a Proxy que éste se realizó
4) Proxy informa al Gateway que el registro se realizó OK
5) Gateway envía a Proxy el mensaje inicial INVITE con direcciones origen y destino
6) Proxy acude al servidor de localización para recuperar la dirección del llamado
7) Servidor de localización envía la dirección al Proxy
8) Proxy acude al servidor DNS para obtener la dirección de red del llamado
9) DNS envía al Proxy la dirección de red del llamado
10) Proxy informa a Gateway que la comunicación está en progreso
11) Proxy envía INVITE a Gateway B
12) Gateway responde a Proxy OK
13) Proxy retransmite OK a Gateway A
14) Gateway A reconoce al Proxy el OK con ACK
15) Proxy retransmite ACK a Gateway B
16) Se inicia el traspaso RTP de muestras de voz correspondiente a la fase conversación
17) Gateway A finaliza la llamada y envía BYE al proxy
18) Proxy retransmite BYE a Gateway B

5.2.6 Futuro de los protocolos Call Setup

- Aunque la familia H.323 de protocolos Call Setup es la más utilizada actualmente, se prevé que los otros irán siendo cada vez más utilizados

- En efecto, el reporte Insight Research citado anteriormente predice que los cuatro protocolos que hemos discutido (H.323, MGCP, Megaco y SIP), dentro de pocos años serán utilizados aproximadamente en la misma proporción

- Con la fuerte penetración de la tecnología de telefonía IP CISCO, cada vez se hace más popular el protocolo SCCP de este proveedor

5.3 Protocolo RTP para la fase de conversación

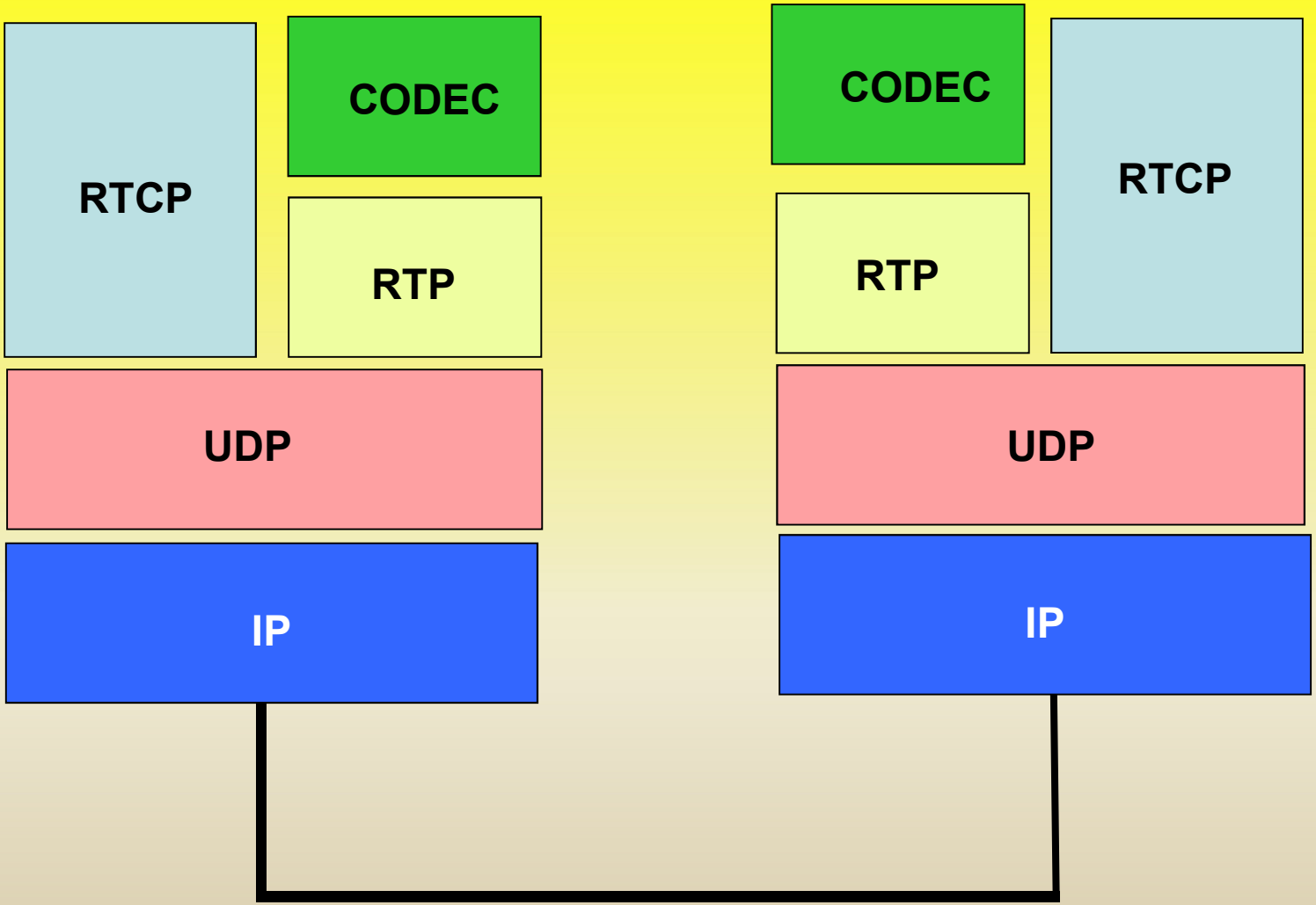
- El intercambio de los datos que corresponden a la voz digitalizada, ocurre después del Call Setup (y antes del Call Takedown)

- Los datos a intercambiar provienen de los CODEC. Corresponden a los datagramas que producen los CODEC durante el proceso de muestreo y digitalización de la voz

- Estos datos son intercambiados mediante dos flujos de datos – uno en cada dirección – haciendo así posible que ambos participantes en la conversación telefónica hablen al mismo tiempo (existen dos “canales lógicos para la voz”)

- Para cada uno de estos dos flujos se usa un protocolo de capa alta, llamado **Real-time Transport Protocol (RTP**), el que es encapsulado en UDP para su viaje por la red

- El protocolo RTP se conoce también como protocolo IETF RFC 1889


RTCP
CODEC
RTP
UDP
IP
CODEC
RTP
RTCP
UDP
IP

5.3.1 Real-time Transport Protocol (RTP)

- RTP es ampliamente usado para transportar flujos de datos correspondiente a audio (datagramas generados por CODEC G.7XX) y video (datagramas generados por CODEC H.26X) .
- Está diseñado para aplicaciones que envían datos en una dirección sin señal de reconocimiento (sin acknowledgement)
- El encabezamiento de cada datagrama RTP contiene un “timbre” con la hora (timestamp). Este “timestamp” permite que la aplicación en el extremo receptor reconstruya exactamente el “timing” de la información original
- El encabezamiento también contiene un número secuencial, que permite al extremo receptor detectar y tomar medidas cuando los datagramas sufren pérdida, duplicación o deterioro

- Los dos flujos RTP, es decir la conversación bi-direccional misma, son elementos importantes que determinan la calidad de la llamada, en lo que se refiere a la calidad de la voz durante la conversación.

- Veremos la composición de las unidades de datos RTP cuya carga útil o payload corresponde a la voz codificada en forma de datos

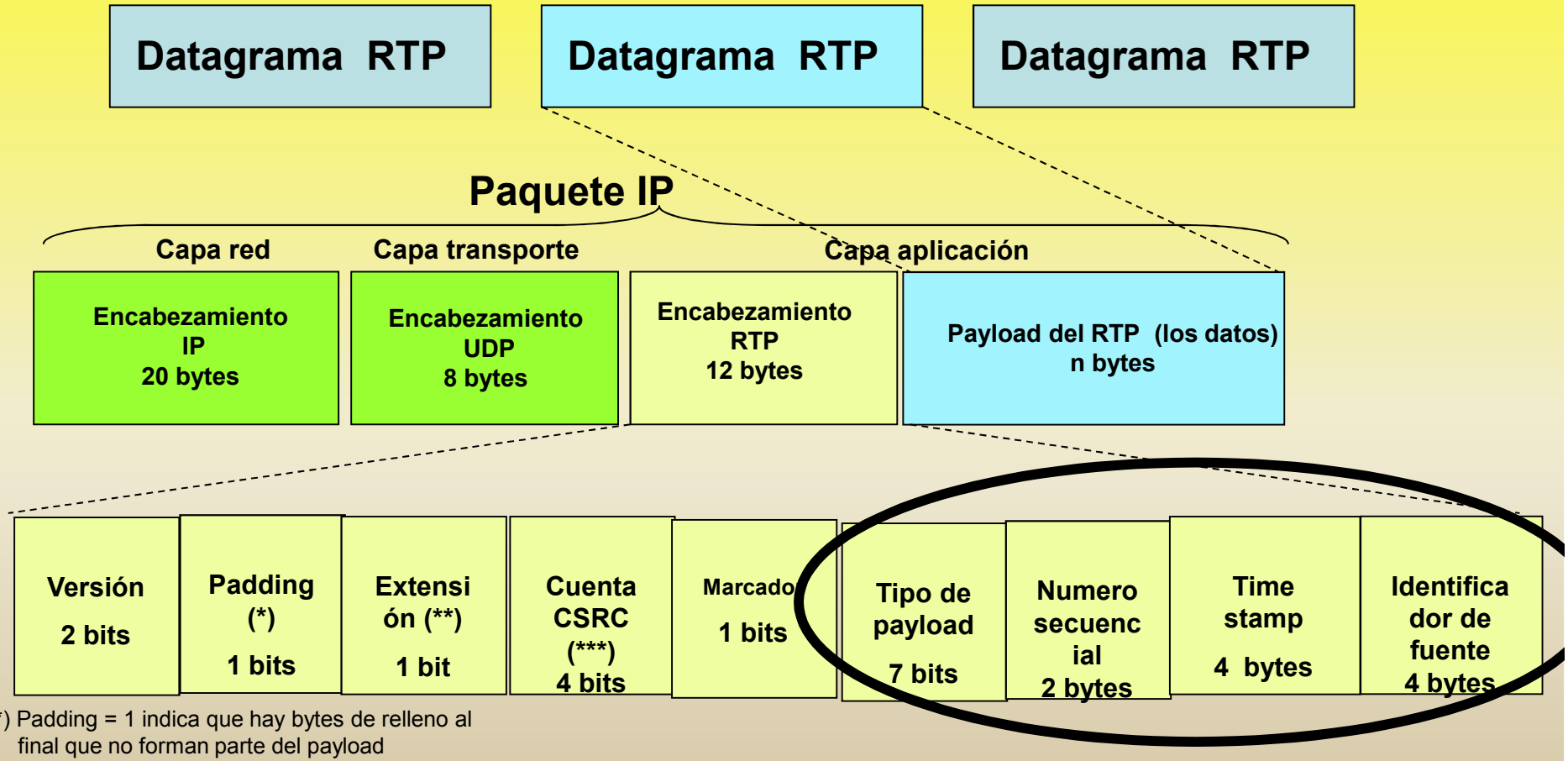
- Cada datagrama más un encabezamiento RTP, se encapsula en un segmento UDP, y éste a su vez se encapsula en un paquete IP

- El encabezamiento del RTP lleva la información necesaria para el correcto reensamblado y decodificación del payload

- Un campo del encabezamiento IP indica a los dispositivos de la red que necesitan esta información, que la transferencia de la unidad RTP se está haciendo mediante protocolo UDP

- Como ya lo vimos, el header IP contiene la información necesaria para que el paquete “viaje” correctamente por la red. Parte de dicha información corresponde a las direcciones de origen y destino del paquete

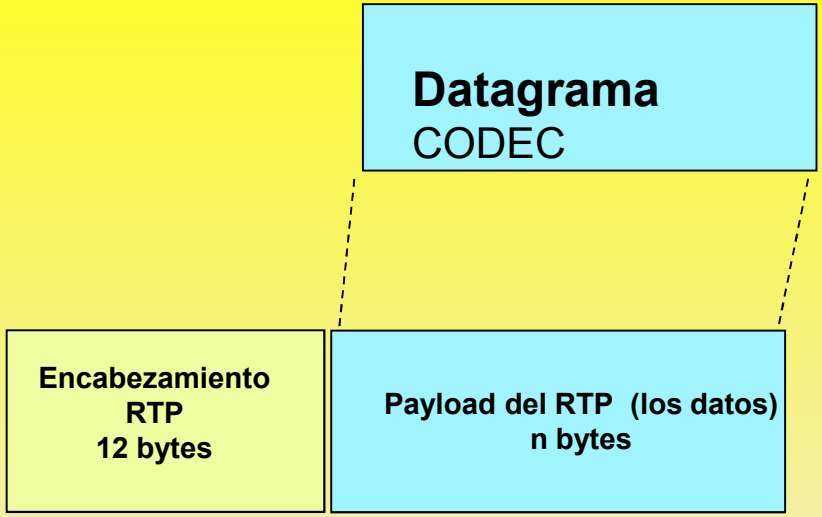
En el paquete IP el encabezamiento de RTP va a continuación del encabezamiento de UDP y éste a continuación del encabezamiento de IP



(*) Padding = 1 indica que hay bytes de relleno al final que no forman parte del payload

(**) Extensión = 1 indica que el encabezamiento fijo va seguido de extensión (Rec. H 225 Anx A.5.3)

(***) Indica la cantidad de identificadores de fuente que siguen al encabezamiento fijo



- La unidad de información del **R**eal time **T**ransport **P**rotocol corresponde a un datagrama entregado por el CODEC más el encabezamiento de RTP
- Veremos el encabezamiento RTP

5.3.2 Campos en el encabezamiento de los RTP

- La unidad RTP está anidada como la carga útil (payload) del UDP

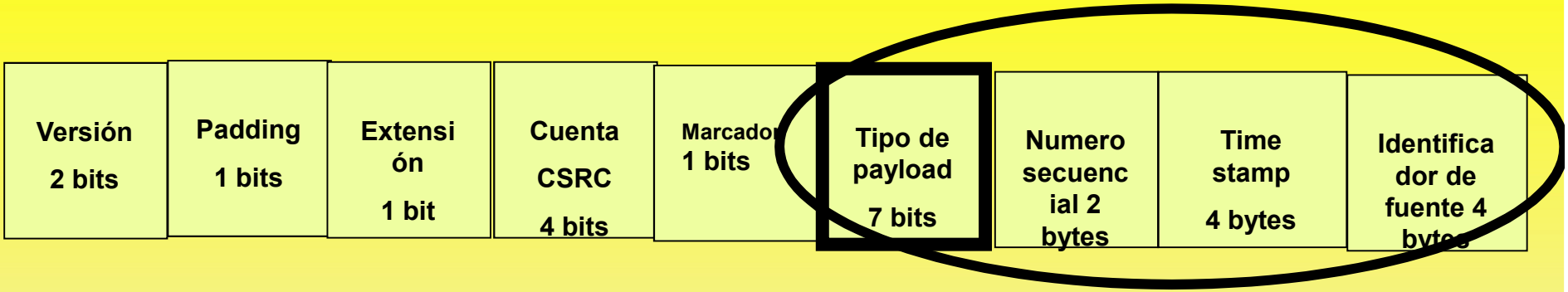
- El software que ejecuta RTP es una aplicación. No forma parte del stack de protocolos TCP/IP

- Este software de aplicación tiene como parte de sus funciones, agregar (en lado origen) y reconocer (en extremo receptor) el header del RTP, constituido por 12 bytes

- En el encabezamiento del RTP hay cuatro campos que son los más importantes

- Los campos del encabezamiento del RTP son llenados en el extremo de envío

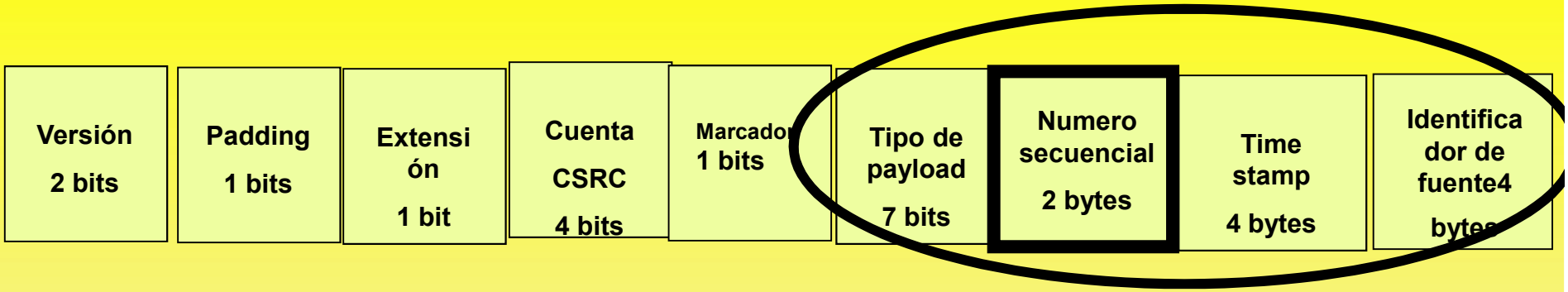
Encabezamiento RTP



Campo Tipo de Payload

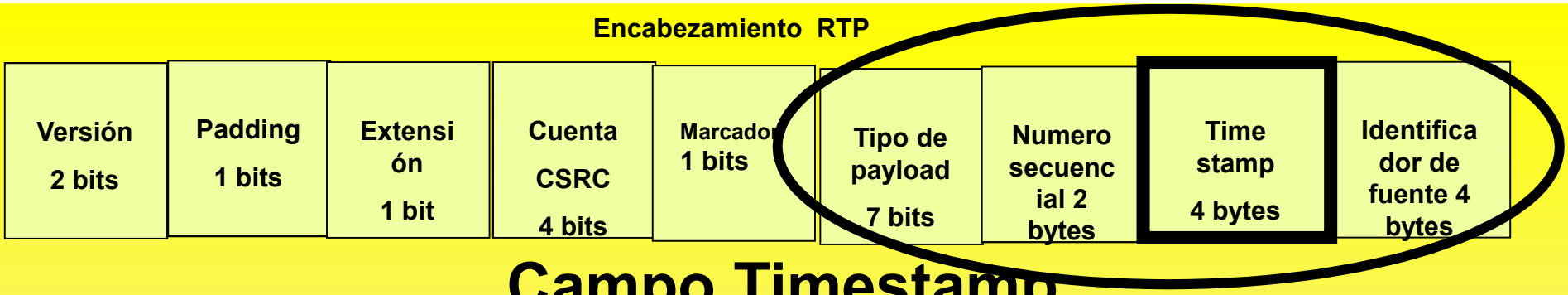
- Indica que tipo de CODEC debe ser usado para decodificar la voz
- Indica el tipo de datos que transporta: puede ser voz, audio o video.
- También indica cómo está codificado.

Encabezamiento RTP



Campo Número Secuencial

- Ayuda al lado receptor en el reensamblado de la información y en la detección de datagramas perdidos, datagramas estropeados y datagramas duplicados



Campo Timestamp

- Se utiliza para reconstruir el timing del audio (o video) original

- También ayuda al lado receptor en la determinación del jitter (diferencia en los tiempos de llegada provocada por la variación de retardo)

- El timestamp realmente valida el RTP

- El enviador de RTP pone un timestamp en cada unidad RTP que envía

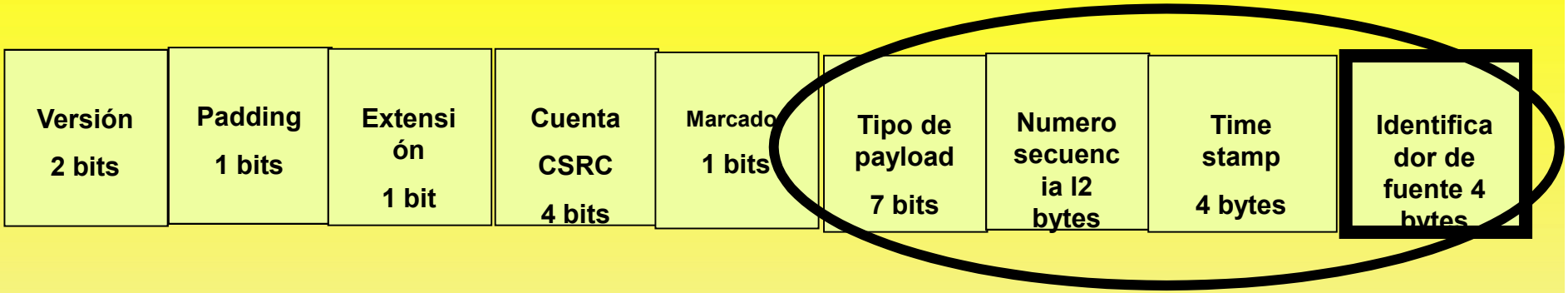
- El extremo receptor de RTP registra los instantes de llegada de los datagramas. Luego compara las diferencias de tiempos de llegada registrados entre datagramas con la diferencia entre los timestamps correspondientes. De esta forma el extremo receptor puede calcular el jitter que introduce la red

- Para dos unidades RTP, si la resta de la diferencia de los instantes de llegada y la diferencia de sus timestamp es nula, es indicación de que ambas unidades RTP tuvieron una variación de retardo 0. Si el valor resultante es, por ej., + 5 mseg, indica que la 2ª unidad RTP demoró 5 mseg. más que la 1ª unidad RTP.

Ejercicio de cálculo de Jitter mediante el campo Time Stamp del encabezamiento de los RTP (Ver transparencia al final Parte I. Usar D y S)

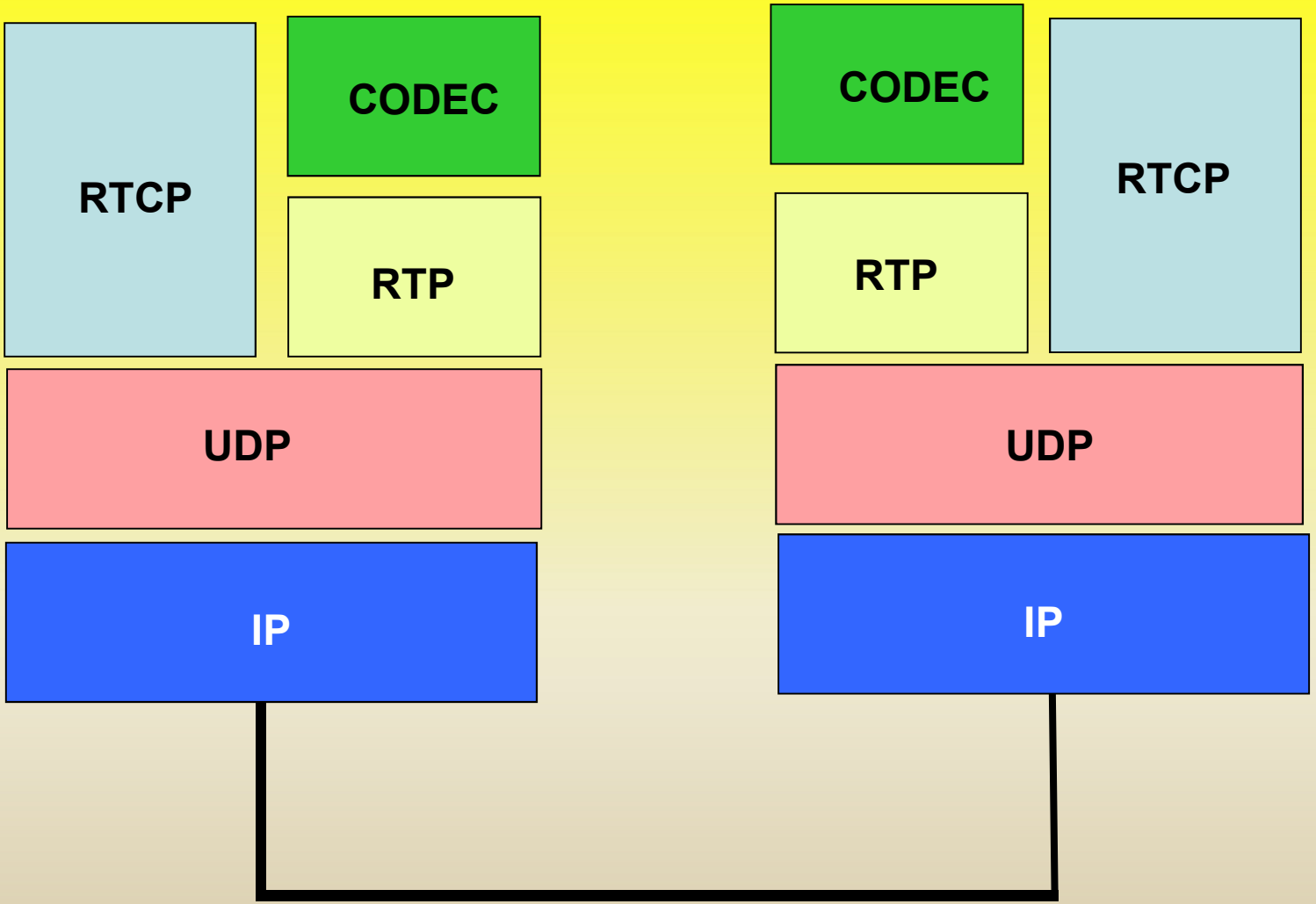
								CALCULO DEL JITTER EN LADO RECEPTOR			
1	2		3		4	5		6	7	8	9
Nº datagrama	Reloj lado emisor (Time Stamp)		Retardo introducido por la red		Variación de retardo (Jitter)	Diferencia entre relojes		Reloj lado receptor (instante de llegada)	Diferencia entre Time Stamps	Diferencia entre instantes de llegada	Variación de retardo (Jitter)
i	TS		Ret		$Ret_{i+1} - Ret_i$	Constante		ILL = (2) + (3) + (5)	$TS_{i+1} - TS_i$	$ILL_{i+1} - ILL_i$	(8) - (7)
1	0		2			10		12			
					1				3	4	**1**
2	3		3			10		16			
					1				2	3	**1**
3	5		4			10		19			
					-2				2	0	**-2**
4	7		2			10		19			
					2				3	5	**2**
5	10		4			10		24			
					-4				2	-2	**-4**
6	12		0			10		22			
					1				2	3	**1**
7	14		1			10		25			

Encabezamiento RTP



Campo Identificador de fuente (Source ID)

- Permite que el extremo receptor distinga entre los múltiples y simultáneos flujos que está recibiendo


RTCP
CODEC
RTP
UDP
IP
CODEC
RTCP
RTP
UDP
IP

RTP usa número de puerto UDP dinámico, ya que un mismo usuario puede estar recibiendo varios flujos simultáneamente.
El número de puerto UDP que usa RTP es siempre par y en el rango 1024 – 65535.
El número impar siguiente es el puerto UDP asignado a RTCP.

RTCP de cierta manera controla el flujo RTP, lo que se hace mediante el envío periódico de paquetes de control con información que envían los participantes

ver: http://es.kioskea.net/contents/internet/rtcp.php3

RTCP (Real-time Transport Control Protocol)

- Describe el intercambio de mensajes de control relacionados con la QoS: retardo, jitter, tasa de pérdidas, etc.
- Su uso es opcional, pero recomendable ya que entrega información del estado de la comunicación en lo referente a la QoS
- No tiene mecanismos para mejorar la QoS
- Entrega además otros servicios como sincronización entre medios

cRTP (compressed RTP)

Con el fin de aumentar la eficiencia en el uso del ancho de banda, este protocolo utiliza el procedimiento de comprimir los encabezamientos RTP. Sin embargo el precio que se paga no es bajo: mayor retardo introducido por los procesamientos de compresión y descompresión

6 CODEC: Funcionamiento, Especificaciones, Ancho de banda

6.1 Principios de funcionamiento de los CODEC usados en telefonía

Una de las funciones de los codec es ahorrar Ancho de Banda en la red de datos por la que se transmitirá la información, y ahorrar espacio de almacenamiento en los dispositivos en que eventualmente se decida grabar la información.

Para realizar esta función el diseño de los CODEC tiene en cuenta que los archivos de datos en que está codificada la información contienen bytes que se pueden clasificar como REDUNDANTES (información repetitiva y fácil de predecir), otros que son IRRELEVANTES (por ej. frecuencias inaudibles, ruido de fondo durante silencios), y por último otros bytes que corresponden a la información básica o RELEVANTE (la necesaria para reconstruir la información).

La compresión puede ser:

SIN PERDIDAS REALES: Se elimina la información redundante.

SIN PERDIDAS SUBJETIVAS: Se elimina la información redundante y también la irrelevante

CON PERDIDAS: Se elimina la información redundante, irrelevante y parte de la básica. En este caso se obtiene una información semejante a la original con cierta degradación de su calidad.

Técnicas para codificar, comprimir y evitar degradación de calidad

Los CODEC usan técnicas sofisticadas para codificar y para comprimir, respaldadas por modernas teorías matemáticas y estadísticas, que están fuera del alcance de este curso.

Sus nombres indican la forma en que se realiza el trabajo:

Multi-Pulse Maximum Likelihood Quantization (MPMLQ)

Algebraic Code Excited Linear Predictive (ACELP). Disponible para G.729 y G.723.1

La técnica de ocultamiento de pérdida de paquetes (packet loss concealment) (PLC) es una característica adicional disponible en los CODEC G.711u y G.711a.

Como las conexiones VoIP son en tiempo real con protocolo de transporte UDP, no es posible usar técnicas de control de errores como ARQ (*Automatic Repeat-reQuest),* por lo que se recurre al enmascaramiento de los paquetes perdidos.

Packet Loss Concealment (PLC), es una técnica para enmascarar los efectos de la pérdida de paquetes en comunicaciones VoIP.

PLC realiza las siguientes acciones para enmascarar las pérdidas:

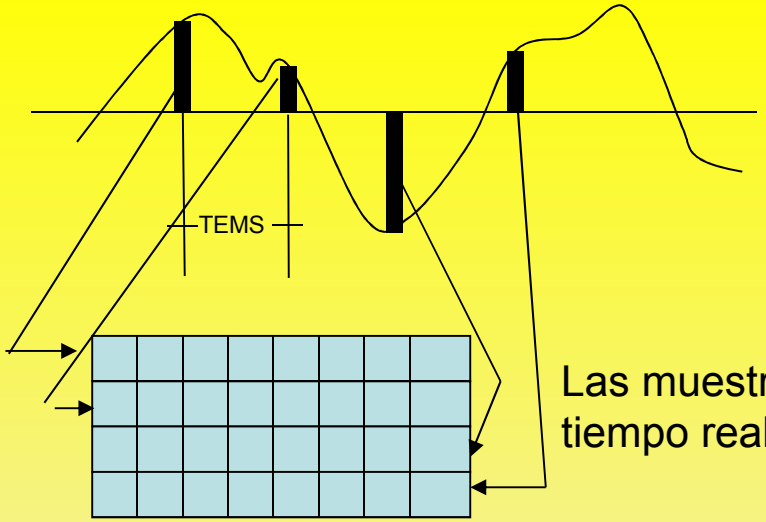
- **Inserción de ceros**: Los payload perdidos se reemplazan por ceros

- **Sustitución de forma de onda:** Los elementos faltantes se reconstruyen repitiendo una porción ya recibida de la voz. La forma más simple es repetir el último payload recibido. Sin embargo hay otras técnicas más elaboradas, que consideran la frecuencia fundamental, la duración del gap , etc. Los métodos de sustitución de forma de onda son populares por su simplicidad para entenderlos y para implementarlos. Un ejemplo de estos algoritmos se encuentra en el Apéndice I de la recomendación G.711

- **Métodos basados en modelos**: Constantemente se están desarrollando nuevos algoritmos que basados en modelos matemáticos, permiten interpolar y extrapolar la voz a fin de generar los elementos perdidos en forma más aproximada a la realidad.

- PLC no agrega retardo ni otros problemas secundarios, pero encarece los Codec.

En las figuras siguientes se resumen los procesos y funciones que realizan los CODEC utilizados en telefonía.



Se toman muestras de la señal de voz analógica cada TEMS seg.

TEMS = Tiempo Entre Muestras Sucesivas de la señal de voz analógica

Las muestras se cuantizan, codifican y con ellas se va creando en tiempo real un archivo digital que contiene la información de la voz

ALGORITMOS DE COMPRESION

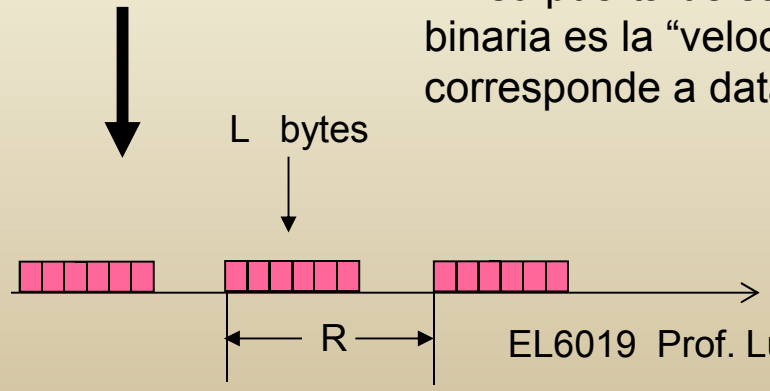
R =

V_{Codec}

Con el fin de ahorrar Ancho de Banda, el archivo se somete a algoritmos que eliminan la información correspondiente a silencios y la información redundante.

Los procesos a que se somete la información se configuran fijando diversos parámetros, entre los que destaca R

En su puerta de salida el CODEC entrega un flujo binario cuya tasa binaria es la "velocidad nominal del CODEC" (V_{codec}). El flujo corresponde a datagramas de L bytes entregados cada R seg.



- Cada cierto tiempo TEMS se toma una muestra de la señal de audio analógica y se somete a varios procesos: PAM, cuantización, codificación, compresión, etc.[1] con el fin de crear bloques de bits que contienen la información correspondiente a muestras de voz, a los que se denomina datagramas.
- Los datagramas se transmiten por la red al CODEC corresponsal, donde se realiza el proceso inverso.
- Cada datagrama tienen L bytes y se envía al CODEC corresponsal cada cierto intervalo de tiempo R.
- Cada datagrama corresponde a una "porción" de información digital que constantemente generan los procesos antes indicados.
- El tiempo requerido por el CODEC para colectar y procesar la información correspondiente a las muestras de voz analógica que se codifican en los datagramas, provoca el "retardo de paquetización" que introduce el CODEC

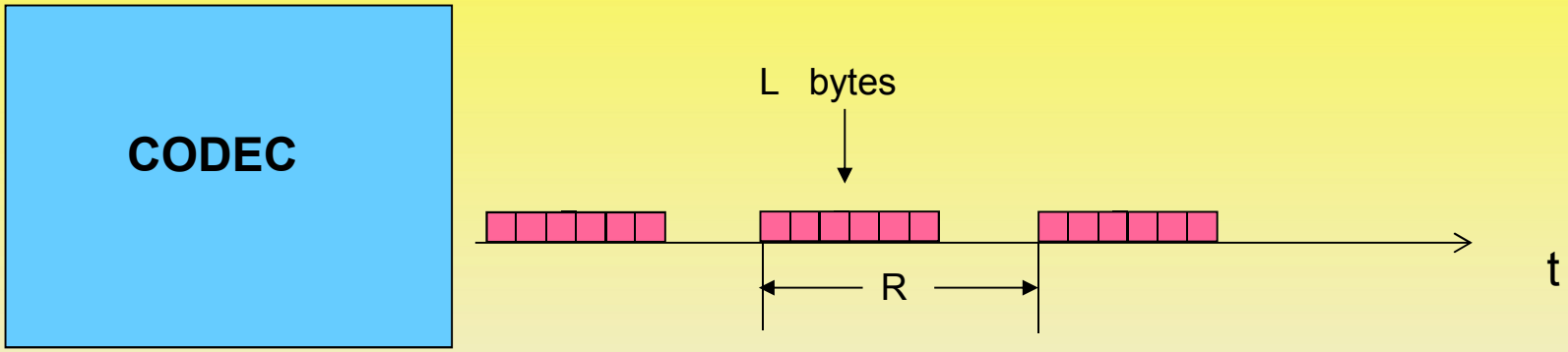
.

(1) Otro algoritmo que se aplica en algunos CODEC permite discriminar si la señal analógica de voz corresponde a voz propiamente tal o si corresponde a tonos, como por ej. DTMF o de equipos FAX o MODEM

Datagramas entregados por el CODEC

Relación entre V_{Codec} , R y L

El CODEC entrega la información cada cierto período de tiempo R fijo (pero ajustable), en forma de datagramas de tamaño L



V_{Codec} = Tasa de datos nominal del CODEC ó velocidad del CODEC (bits/seg.)

R = Tiempo o período entre dos datagramas sucesivos (seg.)

L = Tamaño del datagrama (bytes)

1 / R = Frecuencia de los datagramas [seg $^{-1}$]

La frecuencia de los datagramas, o sea la cantidad de datagramas por segundo es:

$$\text{Frecuencia} = \frac{1}{R} \quad [\text{seg.}^{-1}]$$

El flujo binario, o sea la cantidad de bits por segundo es:

$$V_{Codec}\ (\text{bps.}) = \frac{1}{R} * L\ [\text{bytes}] * 8\ [\text{bits}]$$

El largo de los datagramas, o sea la cantidad de bytes de los datagrama es:

$$\mathbf{L = \frac{V_{Codec} * R}{8}}$$

En que V_{Codex} se expresa en (bits/seg.) = bps.

L en bytes y

R en seg.

Para una V_{Codec} dada, si se aumenta el tiempo R entre datagramas, aumenta el largo L del datagrama, ya que en un segundo el transporte de la misma cantidad de bits, se realiza en menor número de envíos (con menor frecuencia).

Así por ejemplo, si para el CODEC G.711 el tiempo R entre datagramas aumenta de 0,020 seg. a 0,030 seg., el largo del datagrama aumenta de 160 a 240 bytes.

Expresión “Retardo entre paquetes” (delay between packets) ó “Largo de los paquetes de voz” (speech packet lenght) ó “Duración del paquete” (packet duration)

- Algunos teléfonos IP permiten ajustar el “retardo entre paquetes” (delay between packets) o el “largo de los paquetes de voz” (speech packet length) o la “duración del paquete” (packet duration). ¡Cuidado con la jerga!: La unidad utilizada en los tres casos es el mseg.

- Las tres expresiones indican lo mismo y se refieren al intervalo de tiempo entre dos datagramas, o sea corresponde al período de tiempo R entre entregas de datagramas consecutivos. Su valor inverso es la frecuencia de los datagramas.

- Por ejemplo, si la tasa de salida del CODEC enviador es 64 Kbps, y el ajuste se pone en “datagrama de voz 0,020 seg.”, se tendrá que el extremo enviador creará y entregará a la red datagramas cada 0,020 seg.
  Por lo tanto en este caso el largo L del datagrama resultará:
  $L = (V_{Codec} * R) / 8 = 160$ bytes

6.2 Otras especificaciones de los CODEC usados en telefonía

Velocidad nominal del CODEC y retardo que introduce

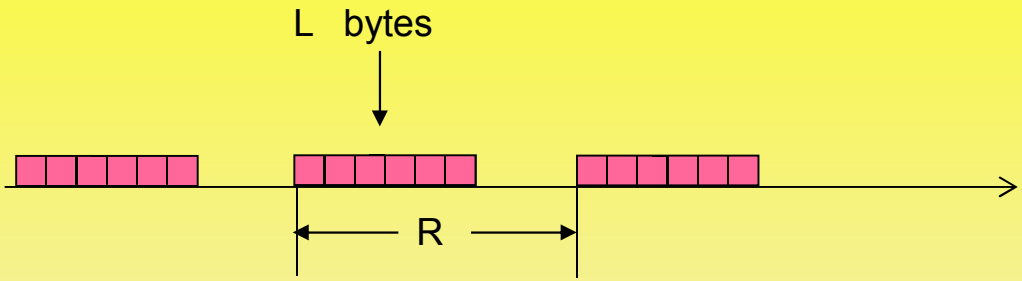
Como vimos anteriormente, los CODEC utilizados en telefonía realizan las funciones de muestrear a intervalos regulares la señal analógica de voz, cuantizar las muestras en valores discretos, codificar, comprimir, producir bytes de 8 bits y ensamblarlos en datagramas para que sean transmitidos por la red de datos.

La velocidad nominal a que el CODEC entrega los datagramas en su salida es uno de los factores determinantes del ancho de banda que se ocupa en la red de datos para transmitir los datagramas. De aquí que sea atractivo diseñar CODEC con bajas velocidades de salida. Velocidades de salida bajas se logran mediante procesamientos más complejos que consumen mayor tiempo provocando delay, el que afecta en parte la calidad del audio.

La tabla de la página siguiente muestra comparativamente estas características para los CODEC más utilizados.

CODEC	Velocidad nominal de salida (Kbps)	Calidad del audio	Complejidad de los procesamientos	Retardo (ms)
G.711	64	Excelente	Muy baja	Despreciable
G.723.1	5,6	Buena	Muy alta	Importante
G.723.1	6,4	Buena	Muy alta	Importante
G.726	32	Buena	Baja	Despreciable
G.728	16	Buena	Media	Despreciable
G.729 (A)	8	Buena	Alta	Apreciable

Período R entre datagramas y consumo de ancho de banda en la red de datos



Como vimos R corresponde al período de tiempo entre dos entregas consecutivas de datagramas, por lo que su valor recíproco corresponde a la frecuencia de los datagramas.

Por ejemplo si R = 0,020 seg. el CODEC entrega 1 / 0,02 = 50 datagramas por segundo

La selección del valor a utilizar para la frecuencia de los datagramas es un compromiso entre requerimiento de calidad y consumo de ancho de banda.

Si se decide alta frecuencia de datagramas, ellos resultarán cortos (pocos bits) y la pérdida de algunos datagramas durante la transmisión hasta el CODEC receptor no afectará mayormente a la calidad. Pero el costo que pagamos es que al existir muchos datagramas, habrá muchos encabezamientos que suben el overhead requiriéndose mayor ancho de banda, como lo veremos más adelante.

El valor más utilizado para R es 0,020 seg., salvo para los CODEC G.723.1 en que se utiliza R = 0,030 seg.

El valor R = 0,020 seg. es utilizado en los ejemplos que Internet Engineering Task Force incluye en la RFC1889

Período TEMS entre toma de muestras de la señal analógica de voz

Una de las características importantes de cada CODEC es el intervalo de tiempo que transcurre entre la toma de dos muestras sucesivas de la señal analógica de voz (TEMS).

Para los principales CODEC se tiene:

CODEC		Tiempo entre toma de muestras sucesivas (TEMS)
G.711	PCM	0,000125 seg. = 0,125 ms.
G.723.1	ACELP	0,030 seg. = 30 ms.
G.723.1	MP-MLQ	0,030 seg. = 30 ms.
G.726	ADPCM	0,000125 seg. = 0,125 ms.
G.728	LD-CELP	0,000625 seg. = 0,625 ms.
G.729 (A)	CS-ACELP	0,010 seg. = 10 ms.

R / TEMS

A veces se utiliza el parámetro **R / TEMS,** que corresponde al cuociente entre el tiempo R entre datagramas sucesivos y el tiempo entre tomas de muestras sucesivas de la señal analógica de voz.

La tabla siguiente indica el valor de este parámetro para algunos casos:

CODEC	TEMS [ms.]	R [ms.]	R / TEMS
G.711	0,125	20	160
G.711	0,125	30	240
G.723.1 ACELP	30	60	2
G.726	0,125	20	160
G.726	0,125	30	240
G.728	0,626	20	32
G.728	0,626	30	48
G.729(A)	10	20	2
G.729(A)	10	30	3

Retardo de Paquetización

Como hemos visto, los CODEC realizan una serie de tratamientos a la información: toman muestras a intervalos regulares de la señal analógica de voz, cuantizan las muestras en valores discretos, codifican, comprimen, producen bytes de 8 bits y los ensamblan en datagramas, que finalmente entregan a su salida para ser transmitidos por la red de datos hasta el CODEC corresponsal, donde se realizan los procesos inversos hasta recuperar la señal de voz.

El tratamiento que los CODEC hacen a la información, desde que se toman las muestras a la señal de voz analógica hasta que se obtiene en su puerta de salida el datagrama correspondiente a ellas, obliga a ocupar tiempos de almacenamiento en buffers, los que junto a los tiempos de procesamiento provocan lo que se conoce como el retardo total introducido por el CODEC o “retardo de paquetización”. Este retardo, que es fijo, se introduce tanto por el CODEC transmisor como por el CODEC receptor. Los retardos introducidos por los CODEC se suman a los propios de la red de datos, pudiendo llegarse a valores de latencia que degradan la calidad.

La tabla siguiente muestra los retardos de paquetización introducidos por los CODEC más comunes usados en telefonía IP.

Retardos de paquetización que introducen los CODEC más comunmente usados para VoIP

Nombre del CODEC	Velocidad de salida nominal (V_{Codec})	Retardo de paquetización (*)
G.711u	64,0 Kbps.	1,0 ms.
G.711a	64,0 Kbps.	1,0 ms.
G.726-32	32,0 Kbps.	1,0 ms.
G.729	8,0 Kbps.	25,0 ms.
G.723.1 MPMLQ	6,3 Kbps.	67,5 ms.
G.723.1 ACELP	5,3 Kbps.	67,5 ms.

(*) Retardo fijo debido a los tiempos que se necesita para los procesos PAM, cuantización, codificación, compresión y otros. El retardo es introducido tanto por el CODEC transmisor como por el CODEC receptor.