

1- INTRODUCCIÓN A VOIP.....	4
1.1 REVISIÓN DE LAS REDES TRADICIONALES DE VOZ.....	5
<i>Introducción a la Sección 1.1.....</i>	5
<i>Señalización.....</i>	5
<i>Sistema de Señalización Número 7 (SS7).....</i>	7
<i>Direccionamiento.....</i>	8
<i>Encaminamiento.....</i>	9
1.2 REVISIÓN DE CONCEPTOS SOBRE LAS REDES DE DATOS	10
<i>Introducción a la Sección 1.2.....</i>	10
<i>Señalización.....</i>	10
<i>Direccionamiento.....</i>	12
<i>Resolución de direcciones.....</i>	13
<i>Encaminamiento.....</i>	14
<i>Modelos de Voz sobre redes de paquetes.....</i>	15
1.3 VOZ SOBRE ATM (VoATM)	17
<i>Introducción a la Sección 1.3.....</i>	17
<i>Introducción.....</i>	17
<i>Señalización en VoATM.....</i>	19

<i>Direccionamiento en VoATM</i>	21
<i>Encaminamiento en VoATM</i>	23
<i>VoATM y el Retardo</i>	24
1.4 VOZ SOBRE FRAME RELAY (VoFR).....	25
<i>Introducción a la Sección 1.4</i>	25
<i>Señalización</i>	25
<i>Direccionamiento y diseño en VoFR</i>	26
<i>VoFR y el Retardo</i>	27
1.5 VOZ SOBRE IP (VoIP).....	28
<i>Introducción a la Sección 1.5</i>	28
<i>Introducción</i>	28
<i>Historia</i>	30
2- ESCENARIOS Y RETOS PARA VOIP	32
2.1 ESCENARIOS Y RETOS EN VOIP	33
<i>Introducción a la Sección 2.1</i>	33
<i>Escenarios posibles en VoIP</i>	33
<i>¿Por qué VoIP?</i>	36
<i>Retos para VoIP</i>	38
3- CONSIDERACIONES TÉCNICAS	40
3.1 CONSIDERACIONES TÉCNICAS	41
<i>Introducción a la Sección 3.1</i>	41
<i>El reto del tiempo real</i>	41
<i>La transmisión informática</i>	43
<i>La transmisión informática (II)</i>	44
<i>Codificación y compresión de voz</i>	45
<i>Retardo y Jitter</i>	47
<i>El tiempo de encaminamiento</i>	48
<i>El tiempo de tratamiento de los equipos terminales</i>	50
<i>El retardo total</i>	52
<i>Una transmisión asíncrona y no síncrona</i>	53
<i>Orden y camino</i>	54
<i>La red no es fiable</i>	55
<i>Primer balance</i>	56
4- APLICACIONES VOIP	57
4.1 INTRODUCCIÓN.....	58
<i>Introducción a la Sección 4.1</i>	58
<i>El enfrentamiento entre dos mundos</i>	58
<i>La cuestión de la tarificación</i>	59
4.2 EVITANDO LA RED TELEFÓNICA TRADICIONAL.....	61
<i>Introducción a la Sección 4.2</i>	61
<i>Llamadas PC-a-PC</i>	61
<i>Aplicaciones utilizadas en las llamadas PC-a-PC</i>	63
<i>Llamadas PC-a-teléfono</i>	65
<i>Llamadas teléfono-a-teléfono</i>	67
<i>Pasarela (gateway) corporativa</i>	69
<i>PABX (Centralita) IP</i>	70
4.3 SUSTITUYENDO LA RED TELEFÓNICA TRADICIONAL	71
<i>Introducción a la Sección 4.3</i>	71
<i>Introducción</i>	71
<i>El Softswitch o la Sustitución de las centrales de tránsito</i>	72
<i>Red de Acceso Integrada</i>	73
<i>Equipos de Acceso Integrados</i>	74
4.4 SERVICIOS DE VALOR AÑADIDO	75
<i>Introducción a la Sección 4.4</i>	75

<i>Proporcionar Servicios de Valor Añadido VoIP</i>	75
5- MODELO DE RED Y PROTOCOLOS	77
5.1 MODELO DE RED	78
<i>Introducción a la Sección 5.1</i>	78
<i>La Falta de Estandarización en el Modelo de Red</i>	78
<i>Elementos del Modelo de Red</i>	80
5.2 INTRODUCCIÓN A LOS PROTOCOLOS DE VOIP	82
<i>Introducción a la Sección 5.2</i>	82
<i>Visión General de los Protocolos de VoIP</i>	82
<i>UDP vs TCP: El dilema continuidad-fiabilidad</i>	84
<i>La necesidad de herramientas complementarias</i>	86
5.3 RTP (REAL-TIME TRANSPORT PROTOCOL)	88
<i>Introducción a la Sección 5.3</i>	88
<i>¿Qué hace RTP?</i>	88
<i>El feedback RTCP</i>	89
<i>Características Principales</i>	90
5.4 VISTA PREVIA DEL PLANO DE CONTROL.....	92
<i>Introducción a la Sección 5.4</i>	92
<i>El Plano de Control</i>	92
<i>Protocolos de Señalización</i>	94
<i>Arquitectura de Protocolos SS7</i>	96
5.5 PROTOCOLO MEGACOP (MEDIA GATEWAY CONTROL PROTOCOL)	98
<i>Introducción a la Sección 5.5</i>	98
<i>Descripción</i>	98
<i>Funciones de MEGACOP</i>	99
<i>Escenario de llamada con MEGACOP</i>	100
5.6 EL ESTÁNDAR H.323.....	102
<i>Introducción a la Sección 5.6</i>	102
<i>Descripción de H.323</i>	102
<i>Elementos de la Arquitectura H.323</i>	103
<i>Funciones Obligatorias y Opcionales en un Gatekeeper H.323</i>	105
<i>Arquitectura de Protocolos H.323</i>	106
<i>Escenario de Llamada Básica sin Gatekeepers en H.323</i>	108
<i>Llamadas PC-a-teléfono</i>	110
5.7 PROTOCOLO SIP	112
<i>Introducción a la Sección 5.7</i>	112
<i>Definición e Historia</i>	112
<i>Funcionalidad de SIP</i>	114
<i>Características de SIP</i>	116
<i>Escenario SIP</i>	117
5.8 PROTOCOLO SIGTRAN (SIGNALLING TRANSPORT)	119
<i>Introducción a la Sección 5.8</i>	119
<i>Definición y Modelo Funcional</i>	119
<i>Ejemplo de Implementación de Llamada con SIGTRAN</i>	121



Bienvenido al capítulo:

Introducción a VoIP



1.1 Revisión de las redes tradicionales de voz

Introducción a la Sección 1.1

Vas a comenzar el apartado 1.1:

Señalización

Introducción



Vaya, vaya, vaya... Así que intentando adentrarse en el mundo de Voz sobre IP, ¿no? En fin, pues habría que empezar por el principio, repasando algunos conceptos muy utilizados en las redes de transmisión de voz. Sin ir más lejos, empezamos por el **concepto de señalización**....

Propósito de la señalización

El **propósito de la señalización** en una red de voz es el establecimiento de la conexión. Existe señalización en el acceso a la red para la toma de línea, en el establecimiento del camino a través de la red y, en el extremo remoto, en el reconocimiento de la llamada.

Fases de señalización

Para completar una llamada telefónica, se necesitan varias fases de señalización:

Primero, en el momento en que se descuelga el teléfono, se envía la señal de "descuelgue" a la PBX. La PBX responde con el tono de invitación a marcar. Acto seguido, el teléfono envía los dígitos hacia la PBX.

A este intercambio que tiene lugar entre la PBX y el teléfono se denomina **Señalización del Bucle de Abonado** (la señalización que se origina en la central local y que provoca que suene el timbre del teléfono también forma parte de la Señalización del Bucle de Abonado). La transmisión de dígitos desde el teléfono hacia la PBX puede verse también como una forma de direccionamiento, como veremos posteriormente.

Una vez que la PBX ha recibido los dígitos, todas las decisiones se toman en la propia PBX. En aquellos casos de dirigir la llamada hacia la central telefónica necesitamos otro tipo de señalización entre la PBX y la central que permita a la PBX la toma de un "trunk" hacia la central y el envío de los dígitos.



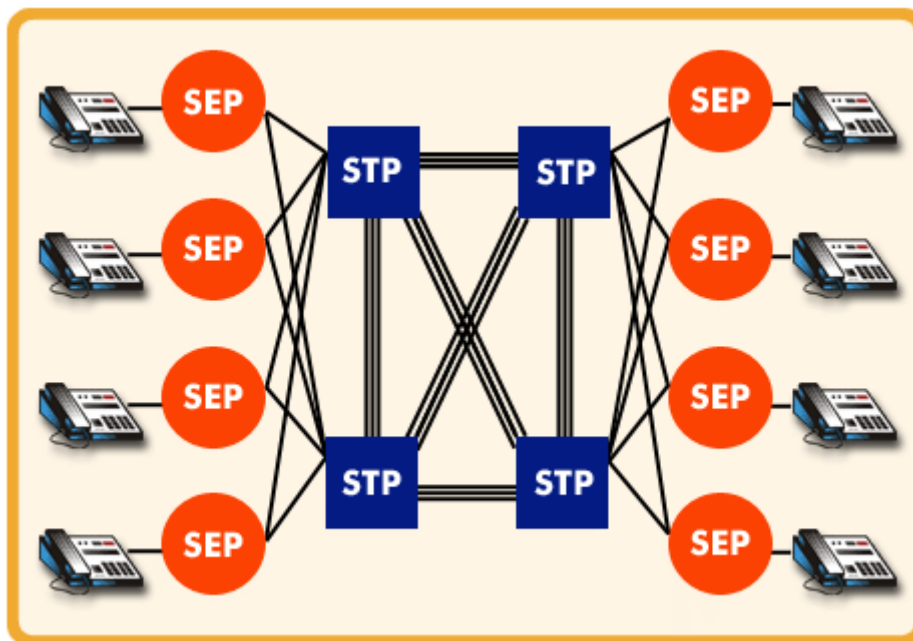
Tipos de señalización

¿Y qué **tipos de señalización** existen en la actualidad?

Pues hoy día, en que los enlaces son digitales, podemos distinguir diferentes métodos de señalización:

- Señalización por canal asociado (**CAS** – *Channel Associated Signalling*): la información de señalización es transportada dentro del canal de voz “robándole” un bit de cada canal para la información de señalización.
- Señalización por canal común (**CCS** – *Common Channel Signalling*): en la trama T1 o E1 (24 o 32 timeslots, respectivamente) se reserva uno de los timeslots como canal de señalización.

Sistema de Señalización Número 7 (SS7)



Pero de los tipos existentes, en telefonía se utiliza un único sistema de señalización, ¡el famoso Sistema de Señalización Número 7!

En las redes de voz de hoy en día, la ruta para una llamada telefónica se establece en un sistema de señalización separado de las rutas de transmisión usadas para las llamadas. El sistema de señalización Número 7 (SS7 – Signalling System 7) utiliza un método de señalización fuera-de-banda (señalización por canal común) para establecer la ruta adecuada para la llamada.

Punto de Señalización (SP – Signalling Point): cualquier nodo de la red de señalización.

Punto final de señalización (SEP – Signalling End Point): son los nodos fuente o destino del tráfico de señalización.

Punto de transferencia de señalización (STP – Signalling Transfer Point): son los nodos de tránsito para la información de señalización.

Point Code: identificador único de 14 bits para cualquier punto de señalización.

Direccionamiento



Pero no todo es señalización exclusivamente, claro...

Para que cualquier red telefónica pueda funcionar, cada teléfono debe estar identificado por una dirección única.

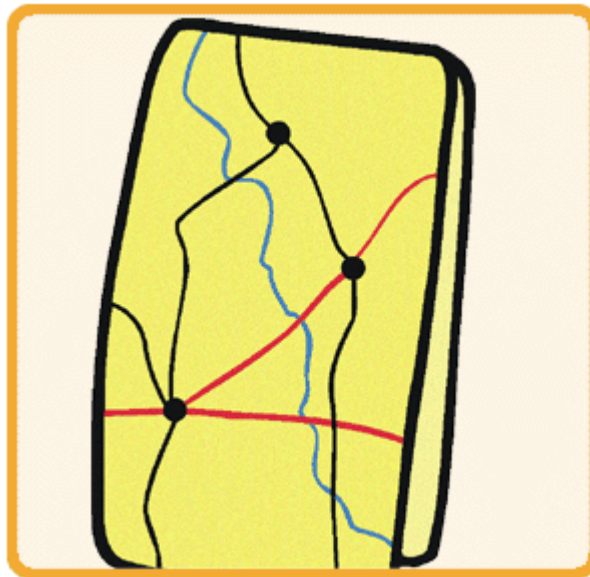
El direccionamiento de las redes de voz se basa en una combinación de estándares nacionales e internacionales y normas de las compañías telefónicas locales.

¡Claro que existe un plan internacional de numeración para evitar ambigüedades en un tema tan importante!

De hecho, las recomendaciones que definen ese plan de numeración internacional son:

- La recomendación E.164 de ITU-T define el plan internacional de numeración para ISDN.
- El plan de numeración del servicio telefónico internacional es un subconjunto del plan E.164.

Encaminamiento



El encaminamiento está estrechamente ligado al plan de numeración y señalización descrito anteriormente.

Permite el establecimiento de una llamada desde un teléfono origen a otro destino.

Pero eso no es todo; la mayor parte de los procedimientos de encaminamiento son bastante más complejos, permitiendo a los abonados seleccionar servicios, desviar llamadas a otros abonados, ...

¿Y cómo funciona el proceso de encaminamiento?

Pues de una manera bastante simple...

El encaminamiento tiene lugar como resultado de la existencia de una serie de tablas en cada nodo conmutador.

Cuando una llamada llega a un conmutador, éste obtiene el camino para llegar al destino de dicha llamada, así como los servicios que requiere, de dicha tabla.

1.2 Revisión de conceptos sobre las Redes de Datos

Introducción a la Sección 1.2

Vas a comenzar el apartado 1.2:

Señalización

Introducción



Algo que te debe quedar claro es que los conceptos nombrados anteriormente no son exclusivos de las redes de transmisión de voz, sino que son comunes a todas las redes. Por ejemplo, podemos tomar el caso del concepto de señalización en las redes de datos.

Cualquier discusión sobre señalización debe hacer notar las diferencias en comportamiento de las **redes orientadas a conexión** frente a las **no orientadas a conexión**.

Redes orientadas a conexión

Las redes orientadas a conexión son aquellas en las que se establecen conexiones, entendiendo como conexión a un camino lógico entre las estaciones finales fuente y destino.

El término circuito virtual (VC) se utiliza a menudo para describir este tipo de conexión. Ejemplos de circuitos virtuales son la utilización de time-slots en una red TDM y una conexión establecida en una red ATM utilizando circuitos virtuales permanentes (PVCs).

Para establecer una conexión se necesitan una ruta y unos requisitos para dicha conexión. Dichos requisitos son un conjunto de peticiones que la estación final hace a la red. Por ejemplo, en una red ATM, una petición de circuito virtual puede especificar una tasa de datos media, una tasa de datos máxima y un porcentaje de pérdida de datos. La red intentará construir el VC especificado, si es que hay recursos disponibles.

Redes no orientadas a conexión

Las redes no-orientadas a conexión, al contrario que las redes orientadas a conexión, no necesitan sesiones de establecimiento y liberación de conexiones.



Los encaminadores de estas redes aceptan todo el tráfico e intentan enviarlo basándose en la filosofía “best-effort”. Los encaminadores pueden priorizar el tráfico, pero no tienen un conocimiento global sobre el estado de la red.

Algunos protocolos de redes no-orientadas a conexión, como RSVP (Resource Reservation Protocol) comunican los requisitos de sesión al núcleo de la red a la manera en que los requerimientos de una conexión se comunican en una red orientada a conexión.

Direccionamiento



Si comenzamos a centrarnos en el tipo de red que nos interesa en este curso, podríamos repasar el concepto de direccionamiento de las redes IP.

Los arquitectos originales de Internet diseñaron un protocolo y un esquema de direccionamiento que hiciera abstracción de las tecnologías subyacentes.

Esta interoperabilidad permite a los usuarios comunicarse unos con otros sin tener en cuenta la red a la que están conectados.

Por ejemplo, el esquema de direccionamiento y los protocolos TCP/IP permiten a un usuario en una estación Ethernet comunicarse, a través de una red X.25, con otra estación final en una LAN Token Ring.

Si se utiliza IP como ejemplo de direccionamiento de Nivel 3, lo que destacan son los conceptos de red y de host.

Este esquema de direccionamiento incrementa la flexibilidad y la escalabilidad de las redes de datos.

Ejemplos de aproximaciones a direccionamientos por niveles los hay tanto en redes de área local como de área amplia.

Es importante destacar que los esquemas de direccionamiento por niveles presentan grandes diferencias frente a los esquemas de direccionamiento utilizados en las redes de voz.

Resolución de direcciones

Es importante destacar cómo se traducen las direcciones de Nivel 3 a direcciones de Nivel 2, ya que este concepto es ajeno a las redes de voz.

Vamos a intentar explicar tres métodos diferentes de traducción o resolución de direcciones.



Difusión (Broadcast)

En las redes que comparten un medio común, una aproximación evidente es la utilización de los mecanismos de difusión.

En este caso, cuando una estación conoce la dirección de destino IP pero no la dirección Ethernet subyacente a dicha dirección IP de destino, la propia estación fuente difunde una petición dirigida a todos los que comparten dicho medio. Todos los nodos recibirán el mensaje pero sólo una estación, la propietaria de la dirección IP que se quiere resolver, responderá a la fuente con su dirección Ethernet.

Servidores de resolución de direcciones

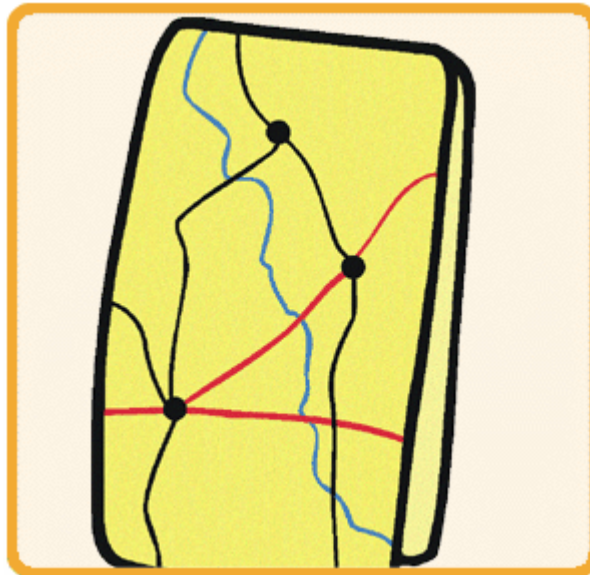
El mecanismo de difusión es muy eficiente en LANs no-orientadas a conexión, y con medio compartido, pero no es adecuada en redes orientadas a conexión. En el caso de ATM, se utiliza un servidor para resolver la dirección ATM a una dirección IP, en lo que se conoce como "Classical IP over ATM".

Todas las peticiones de direcciones desconocidas de nodos ATM se dirigirán al servidor de direcciones que responderá con la dirección subyacente ATM correcta. Después de recibir esta dirección subyacente ATM, la fuente se comunica directamente con la estación de destino.

Tablas locales de configuración

Las redes pequeñas pueden ahorrarse cualquiera de los dos tipos anteriores de resolución de direcciones, si en cada estación final se configuran tablas locales que contengan las correctas asociaciones de direcciones de Nivel 3 y direcciones de Nivel 2.

Encaminamiento



Por último, la determinación de una ruta consiste en el proceso de encontrar el “mejor” camino desde la estación fuente a la estación destino.

El encaminamiento se utiliza tanto en protocolos de Nivel 2 como de Nivel 3.

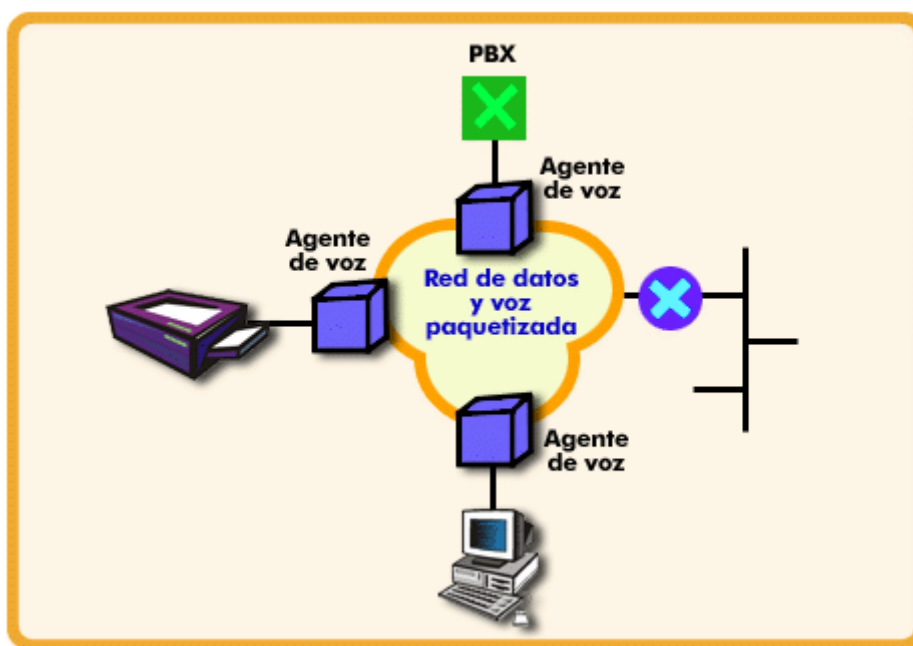
Para determinar una ruta es posible la utilización de tablas estáticas pre-programadas en cada conmutador o en cada encaminador, así como la utilización de protocolos de encaminamiento dinámico.

Modelos de Voz sobre redes de paquetes

¿Y si comenzamos a profundizar en el tema que nos interesa?

¿Qué tal si comenzamos con una visión genérica de cómo se puede transmitir la voz “paquetizada” (contenida en paquetes de datos) sobre redes específicas de datos?

Bueno, pues el modelo general es el que se utiliza en la figura...



La red de transporte de voz paquetizada puede estar basada en IP, Frame Relay o ATM.

Las fronteras de dicha red son equipos que denominaremos “Agentes de voz”.

La misión de estos equipos es cambiar la información de voz desde su forma tradicional telefónica a un formato adecuado para su transmisión en paquetes.

La red podrá entonces dirigir los paquetes de voz hacia otros agentes de voz de destino.

Existen dos modelos básicos para la integración de la voz sobre los datos, Transporte frente a Traducción.

El modelo de Transporte supone el soporte transparente de la voz sobre las actuales redes de datos.

Un buen ejemplo es la simulación de líneas dedicadas sobre ATM utilizando la emulación de circuitos.

La Traducción supone que la infraestructura de datos es capaz de soportar las funciones de voz tradicionales.



Por ejemplo, la interpretación de la señalización de voz en las redes de datos actuales y la creación de conexiones virtuales conmutadas (SVCs) con ATM.

Las redes que siguen este modelo de Traducción son mucho más complejas que las que siguen el modelo de transporte, y su implementación está en plena discusión en varios comités de estandarización.



1.3 Voz sobre ATM (VoATM)

Introducción a la Sección 1.3

Vas a comenzar el apartado 1.3:

Introducción

Introducción

Hombre, ya empezamos a hablar de tecnologías concretas...

¿Cómo es posible la transmisión de voz haciendo uso de redes ATM?

Pues utilizando especificaciones que definieron el ATM Forum y el ITU de las diferentes clases de servicio existentes para representar los distintos tipos de tráfico posibles.

CBR Y VBR

Primeramente diseñados para comunicaciones de voz, las clases **CBR** (*Constant Bit Rate*) y **VBR** (*Variable Bit Rate*) se utilizan en el tráfico de tiempo real, y garantizan un cierto nivel de servicio.

El parámetro CBR, en particular, permite especificar, durante el establecimiento de la llamada, el ancho de banda, el retardo extremo a extremo y la variación permitida de dicho retardo.

UBR Y ABR

Los parámetros **UBR** (*Unspecified Bit Rate*) y **ABR** (*Available Bit Rate*) son más apropiados para aplicaciones de datos. En particular, UBR no garantiza la entrega del tráfico de datos.

AAL1

Así, el método de transporte de canales de voz sobre redes ATM depende de la naturaleza del tráfico.

Se han especificado varios tipos de adaptación a ATM, cada uno de ellos con sus ventajas y desventajas.

La Capa de Adaptación **AAL 1** es el método más utilizado con servicios CBR.

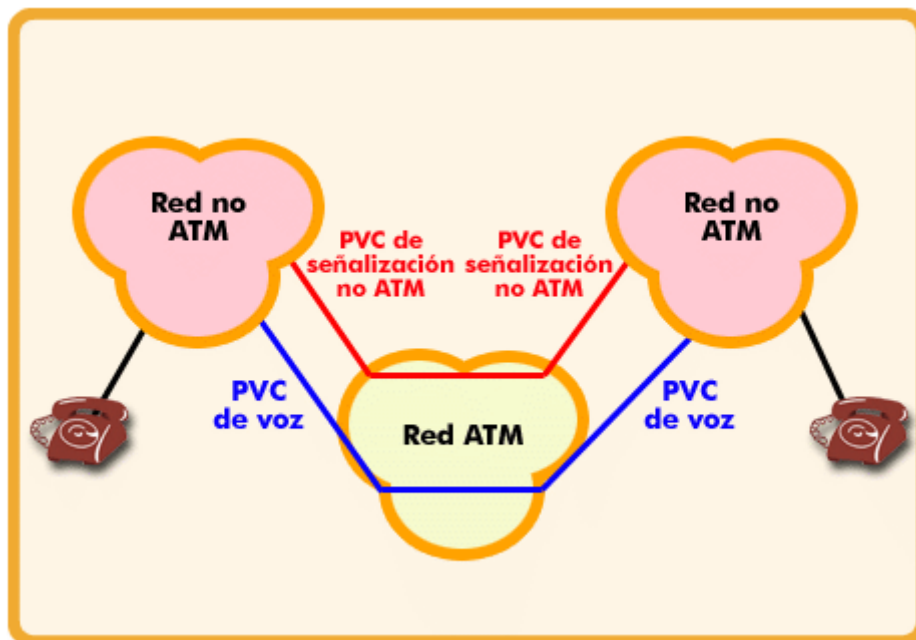


¿Que cómo funciona AAL1? AAL1 no estructurado toma un flujo continuo de bits y lo coloca en celdas ATM. Se trata de un método de adaptación muy utilizado para soportar un flujo de extremo a extremo.

El problema que presenta es que hay que enviar el flujo completo, sin tener en cuenta la cantidad actual de canales de voz en uso dentro de él.

Señalización en VoATM

Dentro de la VoATM, si usamos el modelo de Transporte, hay que crear diferentes PVCs para el transporte transparente de la voz y de la señalización.



Primero, los mensajes de señalización son transportados transparentemente sobre la PVC denominada "Señalización no-ATM", desde una estación final a otra.

Después, la coordinación entre los sistemas finales permitirá la selección de otra PVC para transportar la voz entre ellos.

Como puede deducirse fácilmente, la red ATM no participa en ningún momento en la interpretación de la señalización que tiene lugar entre las estaciones finales.

Sin embargo, como característica de valor añadido, puede destacarse que algunos equipos sí son capaces de entender la señalización CAS (señalización en canal asociado) y pueden evitar el envío de celdas vacías de voz cuando las estaciones finales han "colgado".

Por el contrario, si usamos el modelo de Traducción, la red ATM interpreta la señalización tanto desde los equipos no ATM como desde los ATM.

Se crearán conexiones virtuales permanentes (PVCs) entre las estaciones finales y la red ATM.

Recordemos que en el modelo de Transporte, las PVCs se transportan transparentemente por la red ATM.

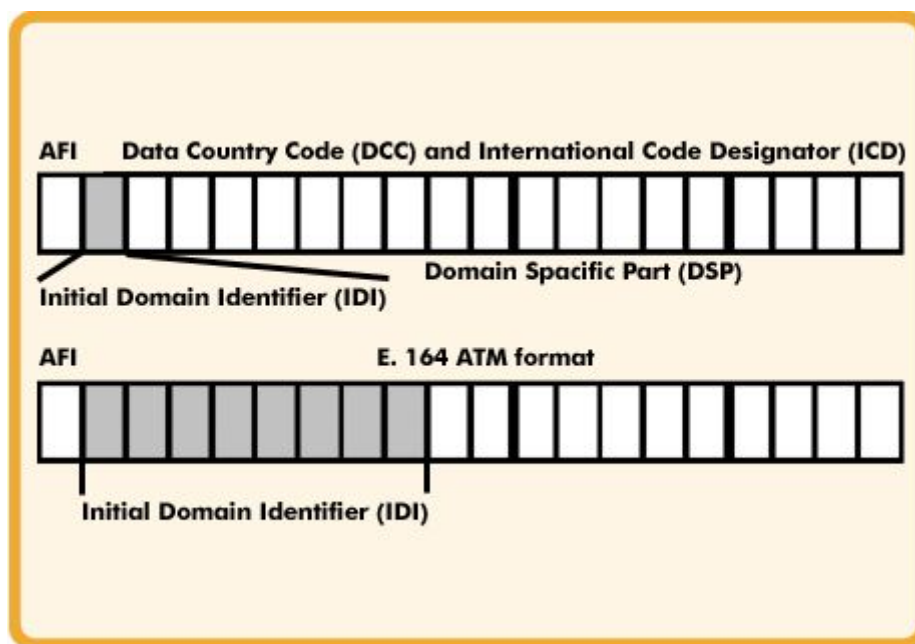
Una petición de señalización desde una estación final provocará que la red ATM cree un circuito virtual conmutado (SVC) con la calidad de servicio (QoS) apropiada, dependiendo de los deseos de dicha estación final.

La creación de una SVC, frente a las PVCs del modelo anterior, ofrece más ventajas desde tres puntos de vista:



- Las SVCs utilizan más eficientemente el ancho de banda.
- Los criterios de QoS no necesitan ser constantes; en las PVCs debían mantenerse constantes.
- La posibilidad de conmutación de las llamadas dentro de la red ATM puede llevarnos a la sustitución de las PBX de tránsito, e incluso de las de frontera.

Direccionamiento en VoATM



¿Cómo hacemos el direccionamiento en VoATM?

Pues los estándares ATM soportan ambos esquemas de direccionamiento, público y privado.

Ambos esquemas de direccionamiento tienen una longitud de 20 octetos. Los principales campos de direccionamiento son los siguientes:

El AFI (*Authority and Format Identifier*) identifica el formato de direccionamiento empleado.

Actualmente, existen tres identificadores especificados:

DCC (*Data Country Code*), ICD (*International Code Designator*) y E.164.

Cada uno de los tres formatos está estandarizado por su comité correspondiente.

La segunda parte de la dirección es el IDI (*Initial Domain Identifier*), que únicamente identifica la red del abonado.

El esquema E.164 posee un IDI mayor, puesto que se corresponde con los 15 dígitos del número ISDN.

La parte final, DSP (*Domain Specific Part*) identifica grupos lógicos dentro de estaciones finales ATM.

¿Y dentro de los modelos que hemos visto, cómo se utilizan estos formatos?

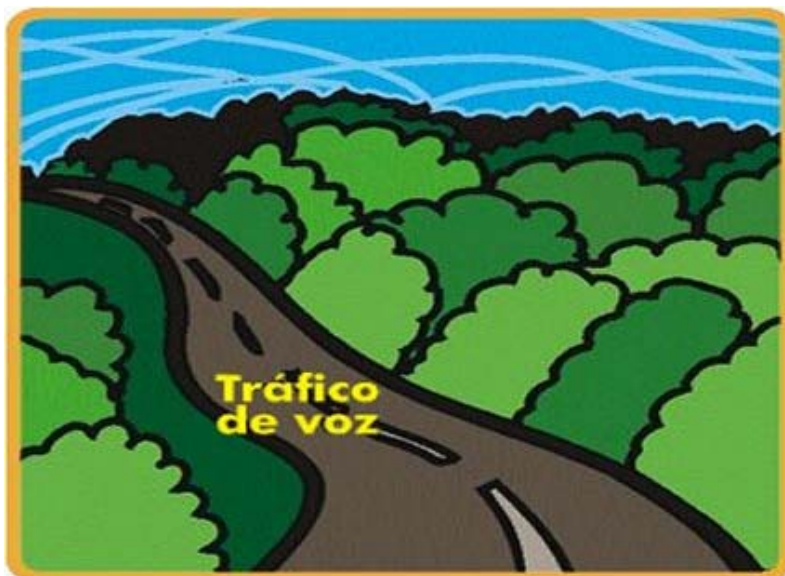
En el modelo de *Transporte* no es necesario preocuparse del direccionamiento subyacente de la red de voz.

Sin embargo, en el modelo de Traducción, la posibilidad de comunicar equipos no-ATM con equipos ATM implica un cierto nivel de correlación de direcciones.



Afortunadamente, ATM soporta el esquema de direccionamiento E.164, el mismo sistema empleado por las redes telefónicas en todo el mundo, solucionándose ese problema.

Encaminamiento en VoATM



En cuanto al último de los conceptos fundamentales, el de encaminamiento, ATM utiliza PNNI (Private Network to Network Interface), un protocolo de encaminamiento "enlace-estado" jerárquico que es escalable para uso global.

Además de poder determinar la accesibilidad y el encaminamiento en las redes ATM, también es posible el establecimiento de llamadas.

De este modo, una petición de circuito virtual (VC) provocará una conexión, con ciertos requerimientos de QoS, hacia la red ATM.

La ruta a través de la red se determina por el conmutador ATM fuente, basándose en lo que él determina como "mejor" camino a través de red, partiendo de la información que obtuvo del protocolo PNNI y de los requerimientos de QoS.

Cada conmutador a lo largo de la ruta es chequeado para comprobar si dispone de los recursos apropiados para la conexión.

Una vez que la conexión está establecida, el tráfico de voz fluirá entre las estaciones finales, exactamente igual que si existiese una línea dedicada entre ellas.

Es importante destacar que la especificación PNNI sólo es apropiada en el ámbito de las redes privadas.

Si hablamos de redes públicas, el protocolo entre conmutadores se denomina B-ICI.

VoATM y el Retardo



Como último comentario sobre esta tecnología, añadir que ATM ofrece diversos mecanismos para el control del retardo y de la variación del retardo o jittering.

Las capacidades de QoS en ATM permiten especificar peticiones de tráfico de flujo de bits constante (constant bit rate), con ancho de banda y variación del retardo garantizados.

El uso de conexiones virtuales (VC) permite que cada tipo de tráfico sea gestionado en colas diferentes, y sea tratado con independencia.

En el caso del tráfico de voz, puede utilizarse una cola de alta prioridad para dicha transmisión.

Además, la utilización de pequeñas celdas de tamaño fijo reducirá el retardo en las colas y la variación en dicho retardo asociada a las longitudes variables de los paquetes.

¿Te apetece un resumen rápido?.

ATM es una arquitectura orientada a conexión. Fue creado para, entre otras cosas, manejar tráfico sensible al retardo, como la voz.

Sus procedimientos de señalización, direccionamiento y encaminamiento nos permiten la construcción de una red que siga el modelo de Traducción.

La función de encaminamiento, en particular, es lo bastante "robusta" como para permitir la construcción de conexiones basadas en el acuerdo previo sobre un cierto retardo y variación del retardo.

1.4 Voz sobre Frame Relay (VoFR)

Introducción a la Sección 1.4

Vas a comenzar el apartado 1.4:

Señalización



¿Un pequeño repaso a Frame Relay? Venga...

Frame Relay es una tecnología ampliamente difundida, utilizada generalmente en el ámbito de las redes de datos corporativas por su flexibilidad en la utilización del ancho de banda, accesibilidad a nivel mundial, soporte a mezclas de tráfico diversas y madurez de la tecnología.

El servicio Frame Relay está basado en la utilización de conexiones virtuales permanentes (PVCs).

¿Podemos transmitir voz sobre este tipo de tecnología?

Por supuesto que sí. De hecho, VoFR es una progresión lógica para las empresas que ya estaban utilizando Frame Relay en su transporte de datos.

Históricamente, el establecimiento de llamadas con Frame Relay ha sido una solución propietaria de cada fabricante. Esto ha significado que los productos de diferentes fabricantes no interoperaran entre sí.

Pero se está trabajando en una solución a este inconveniente, como ya te habrás imaginado. El documento FRF.11 del Frame Relay Forum establece un estándar para el establecimiento de llamadas, los tipos de codificación y los formatos de los paquetes para transmitir voz sobre Frame Relay, y proporcionar la base para la interoperabilidad futura entre los fabricantes.

Direccionamiento y diseño en VoFR



¿Y qué ocurre con el direccionamiento en este caso? En VoFR la configuración de direcciones se gestiona a través de tablas estáticas: dígitos marcados se corresponden con PVCs específicas.

El encaminamiento de la voz depende del tipo de protocolo de encaminamiento utilizado para establecer las PVCs y del hardware utilizado en la red Frame Relay.

El encaminamiento puede basarse en límites de ancho de banda, número de saltos, retardos, o combinaciones de estos criterios, pero la mayoría de las implementaciones de encaminamiento se basan en la maximización de la utilización del ancho de banda.

En cuanto al diseño, un par de notas generales...

Una red completamente mallada de PVCs de voz y datos para minimizar el número de saltos en el tránsito por la red, y para maximizar la capacidad para establecer diferentes calidades de servicio.

Una red diseñada de esta forma minimiza el retardo y mejora la calidad de la voz, pero ejemplifica la red de más alto costo.

Muchos proveedores de Frame Relay tarifican basándose en el número de PVCs utilizadas.

Para reducir el costo, ambos segmentos de voz y datos pueden configurarse para que utilicen la misma PVC; reduciendo por tanto el número de problemas potenciales derivados de la creación de un salto en el tránsito cuando la voz necesita ir de una oficina remota a la otra.

Sin embargo, esto impide la compresión/descompresión que tiene lugar cuando utilizamos una PBX de tránsito.

VoFR y el Retardo

VoFR y el Retardo



Existen mecanismos para minimizar el retardo y la variación del retardo en una red Frame Relay. La presencia de grandes tramas de datos en un enlace Frame Relay de baja velocidad puede causar retardos inaceptables para tramas sensibles al tiempo. Para minimizar este problema, algunos fabricantes implementan tamaños pequeños de tramas para ayudar a reducir el retardo y la variación del retardo.

También, los métodos para priorizar las tramas de voz frente a las de datos ayudan a reducir el retardo y la variación del retardo. El problema es que tanto estos métodos, como los que potencian la utilización de pequeños tamaños de tramas son soluciones propietarias de cada fabricante. Para asegurar la calidad de la voz, el CIR (*Committed Information Rate*) en cada PVC debe establecerse convenientemente para asegurar que las tramas de voz no serán descartadas.

¿Volvemos a hacer un resumen de esta otra tecnología? Creo que sí, ¿no?

Resumen

Frame Relay está bastante difundido y resulta comparativamente asequible. Además, está ampliamente disponible en todo el mundo.

Por desgracia, su carencia de un completo sistema de señalización, direccionamiento y encaminamiento evitará, seguramente, la implementación de modelos de *Traducción*, teniéndonos que conformar con los de *Transporte*.

Las redes Frame Relay del futuro proporcionarán señalización SVC para el establecimiento de llamadas, y pueden permitir, incluso, que los DTEs Frame Relay hagan peticiones de calidad de servicio para una llamada, lo que mejorará la calidad de la voz sobre Frame Relay.

1.5 Voz sobre IP (VoIP)

Introducción a la Sección 1.5

Vas a comenzar el apartado 1.5:

Introducción



Y ya que hemos hablado de otras tecnologías, ¿qué te parece si nos centramos en el objeto de estudio del presente curso?

Voz sobre IP (VoIP) puede definirse como una tecnología que permite el transporte de señales de voz sobre datagramas IP, ofreciendo un servicio al usuario de comunicación de voz en tiempo real.

Cuando se habla de VoIP, mucha gente piensa en comunicaciones de voz sobre Internet.

Sin embargo, VoIP es una tecnología que puede implementarse en cualquier tipo de red privada que use el protocolo IP para interconectar sus sub-redes.

El concepto de VoIP no debe confundirse con telefonía sobre IP.

La telefonía sobre IP se refiere al uso de terminales IP directamente sobre las propias redes IP; estos terminales pueden ser ordenadores, teléfonos IP, ...

Sin embargo, cuando hablamos de VoIP nos estamos refiriendo a un concepto mucho más amplio, incluyendo comunicaciones entre teléfonos "normales" (POTS), los cuales utilizarán la red IP en alguna parte de su comunicación.

Tampoco debe confundirse el término VoIP con el de "Voice over Packet".

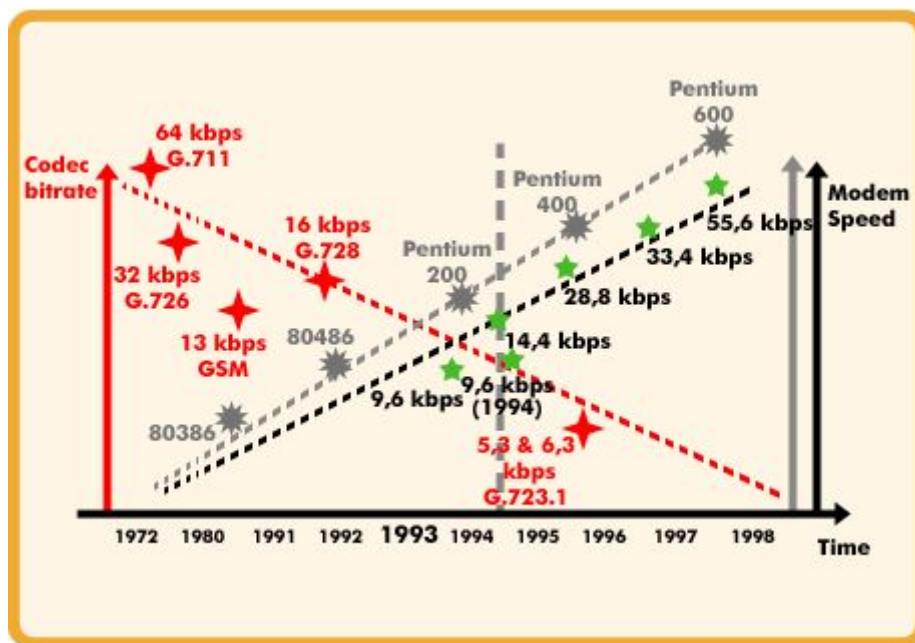


Con éste último término nos estamos refiriendo al transporte de voz sobre cualquier red de paquetes: IP, ATM o Frame Relay.

Aunque la tecnología suele denominarse "Voz sobre IP", incluye también el transporte de datos "Multimedia" sobre redes IP.

Los estándares de VoIP contemplan ambos tipos de transporte de datos (por ejemplo, la videoconferencia), ya que los dos necesitan un servicio de comunicaciones en tiempo real.

Historia



Los comienzos de Internet se remontan a **1970**. Pronto se convirtió en la herramienta de trabajo favorita de los investigadores de todo el mundo. Rápidamente experimentaron la necesidad de comunicarse de un modo más “humano”, más directo.

Para seguir conferencias orales de grupo, implementaron en sus encaminadores el direccionamiento multipunto, que racionaliza el envío simultáneo de un mensaje a varios destinatarios.

El conjunto de estas máquinas representa la red overlay MBONE, sobre la que se han realizado ya las primeras experiencias de transmisión de vídeo y audio.

Las aplicaciones de telefonía o de difusión de audio para microordenadores aparecieron a finales de 1994, el año en que Internet explotó en los medios y entre el público gracias al desarrollo de las páginas web y los “navegadores”.

Estas aplicaciones aprovechan los recursos de las tarjetas de sonido para la digitalización de la señal y su restitución en forma analógica. Ha sido pues necesario esperar a que el parque de ordenadores multimedia fuera lo suficientemente amplio como para incitar a los informáticos a crear nuevas herramientas para el gran público.

La compresión de la señal es otra condición necesaria para el desarrollo de la comunicación en tiempo real en Internet. Un canal de telefonía en la red digital RDSI dispone de un flujo de 64 kbps para el transporte de sonido codificado bajo 8 bits a una secuencia de 8 kHz. ¿Cómo hacer pasar este flujo a través de módems que limitan la velocidad de salida a 28,8 kbps o incluso a 14 kbps? Los algoritmos de compresión son cada vez más complejos y eficaces. Utilizan los recursos incesantemente crecientes de los procesadores digitales de señal, los DSP, motores de todos los dispositivos de sonido o vídeo del mercado.

El “gigante” del procesador de propósito general, Intel, no se ha estado quieto. El Pentium y más aún el Pentium Pro saben reservar cada vez más recursos a los

tratamientos de señales y preservan la viabilidad de soluciones enteramente por software.

Todo coincidía, a partir de 1995, en la aparición del tiempo real en Internet: una población de internautas consecuente, un parque de ordenadores multimedia significativo y los recursos de máquinas, aplicaciones y módems necesarios.

El año 1995 asiste a la multiplicación de las ofertas. Numerosas empresas han abierto una tienda en la red, ofreciendo la descarga gratuita o a prueba de soluciones de telefonía. Algunas han desaparecido ya. Desafortunadamente, todas las aplicaciones de telefonía proponen soluciones propietarias que rivalizan en astucia técnica para resolver los desafíos del tiempo real. En ausencia de especificaciones estandarizadas, los protocolos de transporte, de control y de codificación siguen siendo, generalmente incompatibles. El argumento comercial común a todos estos productos era la economía de tarifas realizada al utilizar Internet, con frases como: "¡Llame al otro extremo del mundo por el precio de una llamada local!".

Fruto de los trabajos en MBONE, se han propuesto soluciones. Si el emisor recibe regularmente informes de escucha de su o sus destinatarios, conocerá casi en tiempo real el estado de la red; así como modular su flujo de salida. Conmutará su codificador para pasar de una señal poco comprimida y de alta fidelidad a una señal más comprimida pero menos onerosa en cuanto a recursos. Un difusor de información multimedia en tiempo real ya no emitirá a ciegas, soltando paquetes al viento de la red. Es él quien dominará el atasco de los nodos y las ramas.

Los paquetes llevarán información que facilitará la reconstrucción de la señal y de su base temporal; convertirán la red en un contenedor digno de un servicio en tiempo real. La sincronización del paquete precisa la hora exacta de su creación; será fácilmente reordenado, y su desaparición se reordenará con rapidez. Una etiqueta indicará el tipo de datos enviados en el paquete y un número de secuencia lo colocará instantáneamente en el flujo de datos. Todas estas especificaciones y otras muchas se encuentran en RTP, el *Real-time Transport Protocol*, adoptado como estándar por el IETF.

La estructura y las especificaciones del IP de nueva generación, el protocolo de red básico de Internet, también se han estandarizado.

El IPv6 se desplegará progresivamente al conjunto de encaminadores en el transcurso de los próximos años. La cabecera IPv6 contiene un campo de prioridad que permite tratar los datos en tiempo real con el cuidado que merecen.

El encaminador es quien tomará la iniciativa de destruir los paquetes de baja prioridad, preservando el tránsito de la señal más prioritaria. Y por si todo esto no basta, un tercer tipo de arma está en reserva. El receptor podrá elegir él mismo el nivel de calidad y la comodidad de la recepción en la señal que desee captar, programa de radio, cadena de televisión, ... Más allá de un cierto umbral de exigencia, podrían encontrarse pagando por los recursos que consuma; es la base para beneficiarse de un servicio a la carta. Es el protocolo de reserva de recursos, RSVP (*Resource reSerVation Protocol*), que transmite la demanda de reserva a todos los encaminadores partiendo del receptor y remontando hasta la fuente.

Las herramientas están a punto, y se integrarán en las próximas generaciones de aplicaciones o de encaminadores, a medida que se reemplacen o se actualicen.



Bienvenido al capítulo:

Escenarios y Retos para

VoIP

2.1 Escenarios y Retos en VoIP

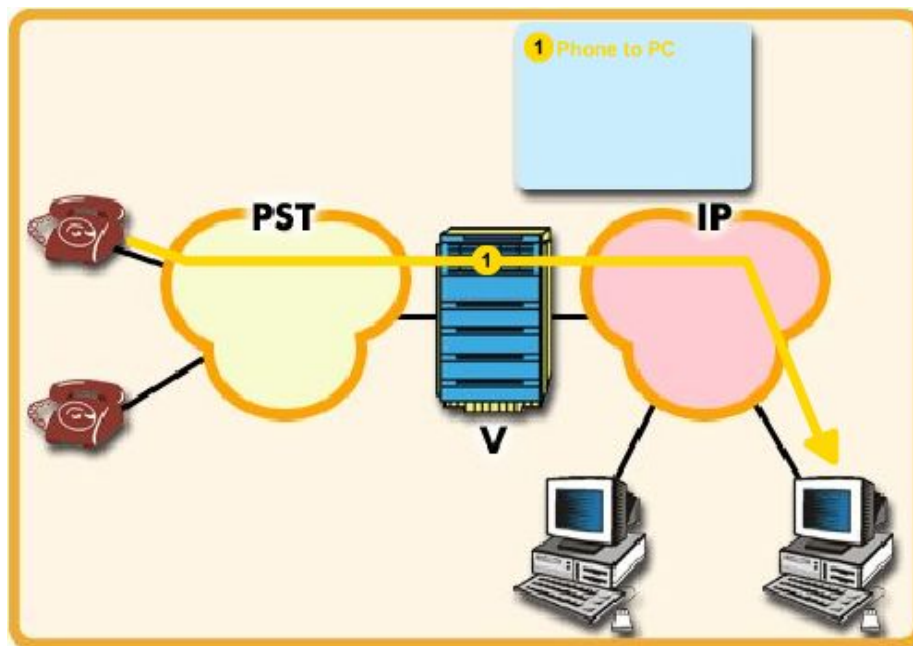
Introducción a la Sección 2.1

Vas a comenzar el apartado 2.1:

Escenarios posibles en VoIP

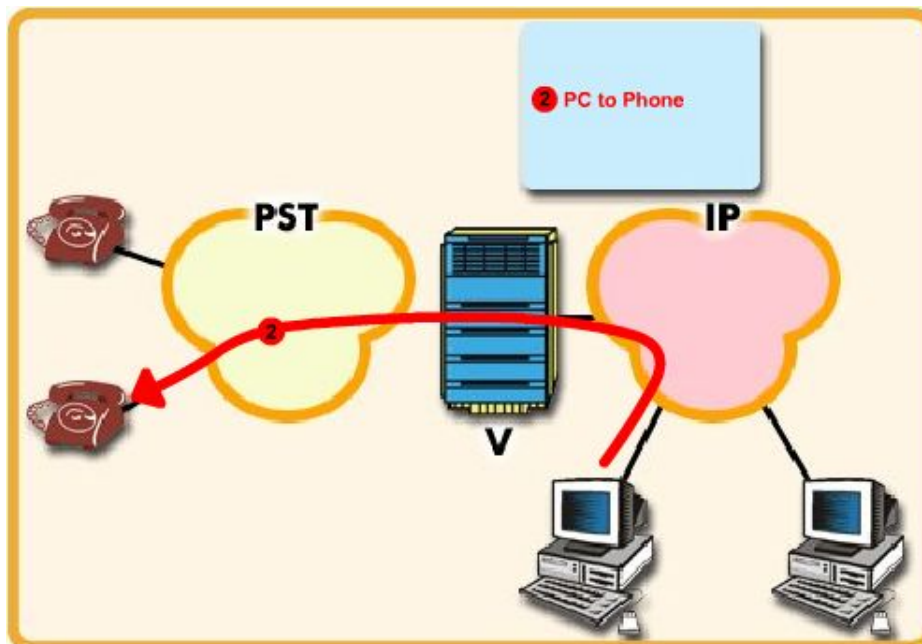
¿Cuáles son los posibles escenarios que podemos plantearnos en VoIP? Pues básicamente, existen cuatro escenarios posibles:

- Teléfono a PC



Este escenario, de gran interés para los ISPs, permitiría, por ejemplo, llamar a un usuario que está navegando por Internet.

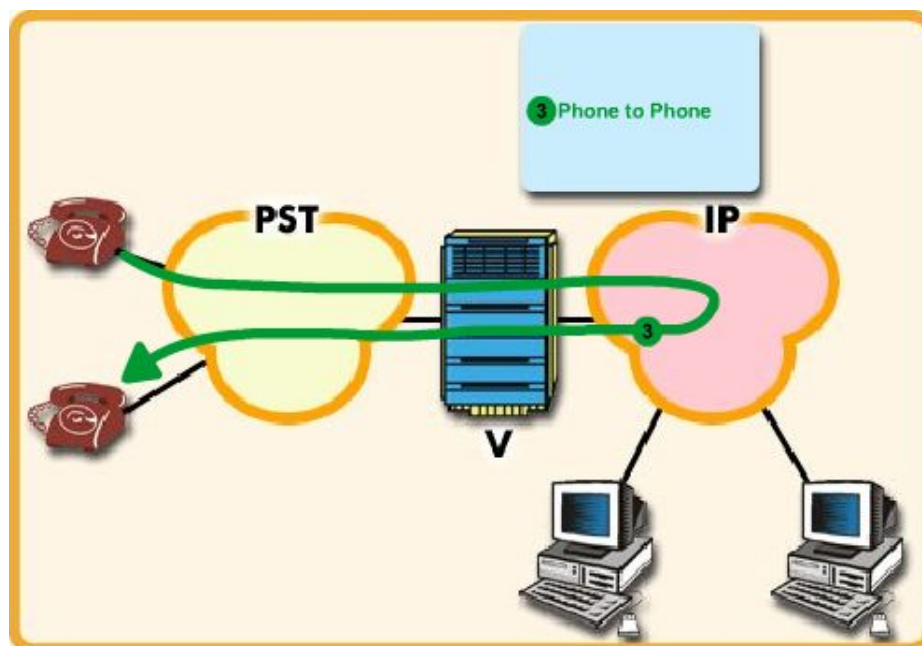
- **PC a teléfono**



Este escenario, también de gran interés para los ISPs, también es conocido por los nombres “click-to-dial” o “surf-and-talk”.

Permitiría a un usuario llamar, por ejemplo, a su ISP, y recibir respuestas a sus preguntas, mientras continúa navegando por las páginas web.

- **Teléfono a teléfono**



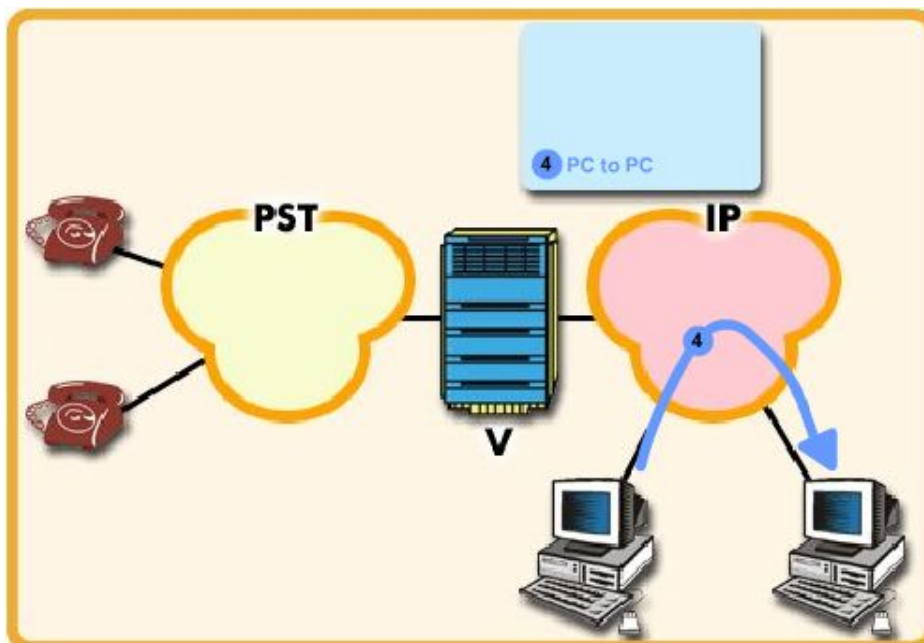
Escenario muy interesante para los operadores telefónicos establecidos.

Puesto que estos operadores ya poseen una gran red de conmutación de circuitos, les puede resultar atractiva la instalación de un Gateway de telefonía IP, que les permita transportar voz sobre un backbone IP como medio de abaratar los costes de las llamadas de larga distancia.

Por ello, este escenario es también conocido por el nombre *"Telephony toll bypass"*.

- **PC a PC**

Este escenario está particularmente pensado para videoconferencias entre dos o más usuarios.



¿Por qué VoIP?



La pregunta del millón es ¿por qué VoIP?

Bueno, podemos dar una respuesta tecnológica a esta pregunta: la capacidad de hacer llamadas de voz sobre una red de datos basada en IP.

Pero, una vez dada la respuesta, también podemos argumentar en su contra que, a priori, no parece la mejor tecnología para transportar el tráfico de voz.

Sin ir más lejos, tenemos un candidato ideal en ATM.

ATM es una tecnología multimedia y multiservicio; por tanto, parecería un candidato idóneo para el transporte de tráfico de voz y multimedia; al menos, más indicado que IP.

Recientemente, han surgido especificaciones destinadas al tráfico de voz sobre ATM (métodos como Constant Bit Rate, vía AAL1, o Variable Bit Rate, vía AAL2).

Sin embargo, ATM no está ampliamente difundido, especialmente entre las pequeñas empresas, y es relativamente caro.

Por el contrario, las redes IP están ampliamente difundidas en el mundo empresarial, por lo que parece más interesante el despliegue de la voz sobre la tecnología IP.

El gran impulso que está teniendo VoIP no se debe tanto a un interés tecnológico como a un interés de mercado.

En el pasado, el mercado de las telecomunicaciones europeo estaba cerrado por los monopolios nacionales.

Sin embargo, la situación ha cambiado en la actualidad: un mercado liberalizado está emergiendo con una plétora de nuevos operadores.

El problema con el que se encuentran ahora los nuevos operadores es que no poseen una infraestructura de telecomunicaciones.

Por tanto, para ellos VoIP representa un punto de entrada más fácil al mercado, ya que les facilita el despliegue de una única red que sea capaz de prestar servicios de "voz" y de "datos".

¿Y cómo es rentable esto? Gracias a que las regulaciones actuales consideran VoIP como tráfico de datos, no como tráfico de voz, lo cual permite considerar como llamada local cualquier llamada de larga distancia cursada a través de redes IP.

De este modo, de cara a estos operadores, el desarrollo de una red IP permitirá tener una red "all-in-one", que posibilite un menor coste de infraestructuras y una mejor utilización del ancho de banda de dicha red.

Ya te imaginarás que los operadores nacionales ya establecidos (los antiguos monopolios) no se han quedado cruzados de brazos.

Y, al contrario de lo que se podría pensar en un principio, no ven en VoIP una amenaza a sus intereses, sino todo lo contrario.

Los operadores de telecomunicaciones establecidos también ven las ventajas de redes VoIP, ya que no sólo representan una buena opción de reducción de costos en su infraestructura, sino una oportunidad para ofrecer nuevos servicios que no son posibles sobre redes de circuitos conmutados (por ejemplo, Click-to-talk en aplicaciones de e-commerce).

Retos para VoIP



En fin, ya hemos alcanzado la convicción de que la mejor tecnología o, mejor dicho, la más conveniente actualmente, para transportar voz en paquetes de datos es mediante el uso de redes IP.

Es decir, ya hemos llegado a la conclusión de que la tecnología en la que debemos centrar nuestros esfuerzos de desarrollo es VoIP.

Sin embargo, la tecnología VoIP debe afrontar algunos desafíos antes de poder ofrecer un servicio de calidad a los usuarios.

No debemos dormirnos en los laureles, ya que quedan muchas cosas por hacer.

- Las nuevas redes VoIP deben permitir la comunicación con las redes telefónicas tradicionales. De no ser así, no habrá interconectividad total, y los usuarios de la red telefónica tradicional no podrían ser atendidos por el nuevo servicio, ni los usuarios del nuevo podrían comunicarse con los usuarios de las redes tradicionales.
- Pero, no sólo hace falta interconectividad con las redes tradicionales de voz; ésta debe ser transparente al usuario. Por ejemplo, debe ser posible llamar desde un teléfono a un PC sin que el llamante tenga que conocer la dirección IP del PC; debería bastar con la simple marcación a un número de directorio telefónico. De hecho, el llamante no tendría que saber si el llamado es un teléfono "normal" o un PC.
- Evidentemente, el uso de una nueva tecnología, como VoIP, no debería implicar una pérdida de la funcionalidad ofrecida por las redes tradicionales (por ejemplo, el desvío de llamada).



- La calidad de servicio ofrecida por las redes VoIP debería ser similar a la ofrecida por las redes telefónicas de conmutación de circuitos.
- Finalmente, se necesitan estándares que posibiliten la compatibilidad entre los diferentes suministradores de equipos.



Bienvenido al capítulo:

Consideraciones Técnicas

3.1 Consideraciones Técnicas

Introducción a la Sección 3.1

Vas a comenzar el apartado 3.1:

El reto del tiempo real



¿Cómo puede representar una banal conversación telefónica un reto mayúsculo para la triunfante tecnología digital?

¿Por qué no podemos reproducir, en estas famosas “autopistas multimedia” de promesas infinitas, gestos que para nuestros padres eran ya naturales?

Sin duda, el teléfono ha conocido una época de puesta a punto.

Lentamente, el eco que molestaba al usuario ha disminuido para desaparecer en los filtros de los circuitos; el ruido que, a menudo, hacía inaudible o lejana la voz del interlocutor, ha dejado paso a una señal clara y próxima.

El retardo de transmisión también se ha hecho discreto; cortar la palabra a un amigo en el otro extremo del mundo sigue siendo descortés, pero ahora es fácil.

¿Hemos vuelto a los años oscuros?

¿Para qué sirve presumir en multitud de artículos del placer de pasear por la red si no se puede ni telefonear por ella?

¿Sería más fácil telefonear a la luna?

Nuestro satélite se encuentra a 384.000 km de nosotros y la señal tarda apenas un segundo para atravesar el espacio.

¡Un rendimiento que envidiarían las sedes en el ciberespacio!

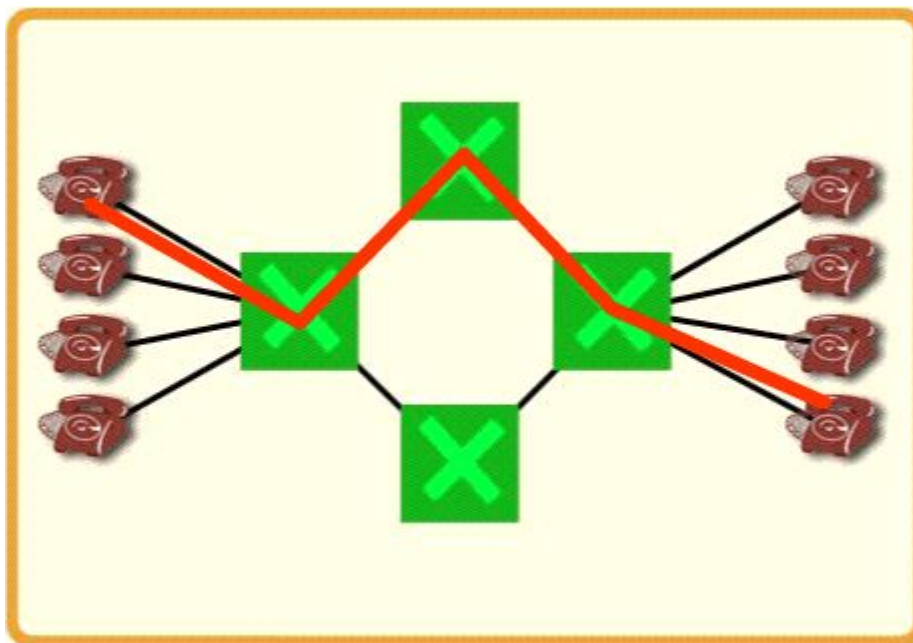


¿Han olvidado algo los “inventores” de Internet?

El problema se explica si consideramos la red Internet como lo que es, una interconexión de máquinas informáticas y no de seres humanos.

Los ordenadores están lejos de comunicar como nosotros; no tienen la misma “conciencia” del tiempo.

La transmisión informática



¿Y en qué consiste esa diferencia en la comunicación entre ordenadores y las personas?

La comunicación oral en tiempo real no es algo natural para una red informática.

La red telefónica es quien cumple esta función; establece una verdadera conexión, en forma de un circuito físico que se mantiene abierto a lo largo de toda la conversación.

Resumiendo, para conectar a los usuarios, la red telefónica conmuta los circuitos.

Su punto fuerte es asegurar el transporte, en tiempo real, de un flujo continuo de palabras garantizando el tiempo, la velocidad y la entrega.

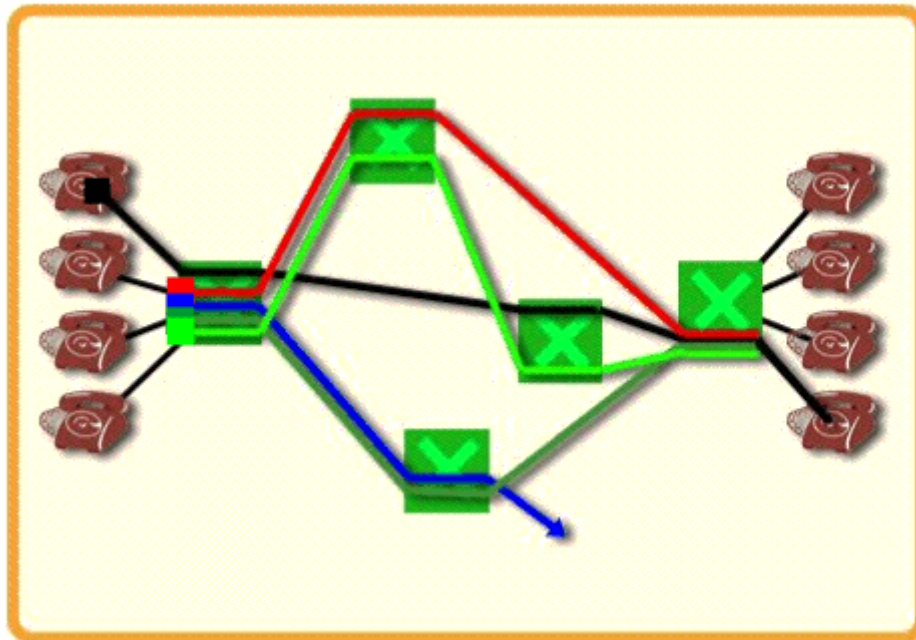
Esta fiabilidad tiene un coste: un circuito físico con recursos dedicados en exclusiva mientras dure la conversación.

El enlace no se libera hasta el fin del diálogo.

Las infraestructuras deben calibrarse para asegurar la misma Calidad de servicio (QoS – Quality of Service) y una misma disponibilidad en los momentos punta.

Los recursos inmovilizados en previsión de los momentos de fuerte tráfico pesan notablemente sobre los costes de amortización y funcionamiento.

La transmisión informática (II)



La red IP no está sometida al mismo tipo de requisitos. Su única misión es enlazar máquinas con el fin de intercambiar información.

Sin embargo, debe dar cumplida respuesta a ciertas imperativos:

- La primera exigencia es la "disponibilidad" de la red. Ésta debe ser capaz de satisfacer a un número cada vez mayor de usuarios. Jamás debe rechazar una petición de conexión, sino al contrario, acomodar a los recién llegados.
- Los datos no se transmiten en un flujo continuo, lo que monopolizaría un "circuito" durante todo el tiempo de transmisión. La red debe compartir sus recursos y servir a todos los clientes.
- El archivo que se desea transmitir se fragmenta, en forma de paquetes, que se conmutan en el interior de la red. El protocolo IP constituye paquetes de unos cientos de bytes; éstos pueden ser fraccionados a su vez, por un nodo de la red, en paquetes más pequeños, si su tamaño es demasiado importante para atravesarlo.
- La otra especialidad de la red IP es su capacidad de difusión de grupo (multidifusión). Un mismo mensaje, texto o datos, puede dirigirse a una lista de destinatarios, o incluso, enviarse en difusión (broadcast) a todos los miembros de la red.

La conmutación de paquetes IP está perfectamente adaptada a las comunicaciones entre ordenadores.

Esto da un gran rendimiento a un entorno compartido. Es económico, simple, eficaz en su utilización de los recursos, y especialmente para la difusión simultánea hacia varios destinos.

Pero... la red IP privilegia el resultado, en detrimento de la velocidad.

Codificación y compresión de voz

Método de compresión	Estándar ITU	Ratio de conversión	Puntuación MOS	Retardo
PCM	G.711	64 kbps	4.4	0.75 ms
ADPCM	G.726	32 kbps	4.2	1 ms
LD-ACELP	G.728	16 kbps	4.2	3-5 ms
CS-ACELP	G.729	8 kbps	4.2	10 ms

CALIDAD

Los métodos de codificación y compresión de la voz son los primeros factores que, potencialmente, pueden afectar a la calidad de la voz.

El término codificación hace referencia al proceso completo de conversión de la señal de voz analógica a formato digital. El estándar de codificación de voz a 64 Kbps se denomina PCM (Pulse Code Modulation).

Denominamos compresión al método por el cual se reduce la cantidad de información digital por debajo de los tradicionales 64 kbps.

Los avances en los algoritmos de compresión han mejorado considerablemente la calidad de la voz comprimida. Múltiples conversiones analógico-digitales o cambios en los esquemas de compresión pueden perjudicar la calidad de la señal de voz original.

Cuando hablamos de compresión de voz, siempre hay que llegar a un acuerdo entre el nivel de calidad de la voz transmitida y el ahorro en ancho de banda.

Pulse Code Modulation (PCM) es el referente de la calidad de voz esperada de una red telefónica.

PCM opera a 64 kbps, no proporciona métodos de compresión y, por lo tanto, no ofrece la oportunidad de ahorros en el ancho de banda.

Adaptive Differential Pulse Code Modulation (ADPCM) proporciona tres niveles de compresión.

La disminución de calidad es, prácticamente, imperceptible comparada con PCM a 64 kbps. Se aprecia alguna pérdida de fidelidad cuando la compresión aumenta.

Dependiendo de la mezcla de tráfico, los ahorros pueden llegar al 25% para ADPCM a 32 kbps, 30% para ADPCM a 24 kbps y 35% para ADPCM a 16 kbps.

El algoritmo *Low-Delay Code-Excited Linear-Prediction* (LDCELP) imita la voz humana.

Dependiendo de la mezcla de tráfico, el ahorro puede llegar al 35% para LDCELP a 16 kbps.

El método *Conjugate-Structure Algebraic-Code-Excited Linear-Prediction* (CS-ACELP) proporciona un ahorro de ancho de banda 8 veces superior a PCM y, por lo tanto, 4 veces sobre ADPCM a 32 kbps.

CS-ACELP también está diseñado específicamente para la voz humana y consigue una calidad equivalente a LDCELP y a ADPCM a 24 kbps. También, dependiendo de la mezcla de tráfico, el ahorro puede llegar al 40% para CS-ACELP a 8 kbps.

¿Cómo se mide **la calidad** de la voz en los distintos métodos de compresión?

La utilización del índice MOS (Mean Opinión Score) está ampliamente difundida como un índice subjetivo de medida de dicha calidad de voz.

La puntuación máxima es 5, aunque valores entre 4 y 5 son considerados como de muy alta calidad.

Retardo y Jitter



Por desgracia, ya sabemos que no sólo la compresión de la voz afecta a la calidad de la misma. De hecho, dos efectos muy habituales que pueden afectar también a la calidad de la voz son el retardo y la variación del retardo, éste último también conocido como jitter.

El retardo puede causar dos perjuicios potenciales a la voz.

Por su parte, el jitter causa ausencias de voz, lo que se traduce en conversaciones "espasmódicas". La calidad de la línea también afecta a la calidad de la voz, pero esto escapa al propósito de este estudio.

- Grandes retardos en una conversación pueden causar que el receptor comience a hablar antes de que el transmisor haya finalizado.
- El retardo incrementa el problema del eco, es decir, de la reflexión de la señal original hacia el emisor. El eco es indiscernible en condiciones de bajo retardo.

El tiempo de encaminamiento

El panorama es menos favorable cuando nos interesamos por la capacidad de la red para transportar una señal en tiempo real.

La noción de tiempo real supone que la emisión y la recepción de la señal sean "casi" simultáneas.

El contenido de este "casi" varía con las restricciones de cada aplicación.

Retardo en un sentido	Descripción
0 – 150 ms	Aceptable por la mayor parte de aplicaciones de usuario
150 – 400 ms	Aceptable siempre que las administraciones sean conscientes del impacto del tiempo de transmisión en la calidad de la transmisión de las aplicaciones de usuario.
Más de 400 ms	Inaceptable para propósitos de planificación general de redes; sin embargo, se asume que, en algunos casos excepcionales, pueda excederse este límite.

En el caso del transporte de voz, el tiempo de tránsito debe ser inferior a 150 ms, con una tolerancia que va hasta los 400 ms.

Cuanto más se alarga el tiempo, más importante es el fenómeno de eco, que se tendrá que suprimir electrónicamente.

Pero, ante todo, es la interactividad, base de la conversación entre dos seres humanos, lo que no se respeta.

Se hace imposible quitar la palabra al interlocutor.

Contrariamente a lo que pueda pensarse, el principal factor que influye en el tiempo de encaminamiento no es la distancia entre los nodos finales de la red.

La distancia no es un factor más preponderante que en la red telefónica.

La velocidad de circulación de los electrones por un cable se acerca a los 200.000 km/s, lo que supone 6 microsegundos por cada kilómetro.

En Internet, la duración del trayecto activo es casi siempre despreciable en relación a la de los procedimientos de tránsito debidos a la conmutación de paquetes en los encaminadores.

El tiempo de transporte en una red como Internet dependerá estrechamente del número de nodos intermedios atravesados.

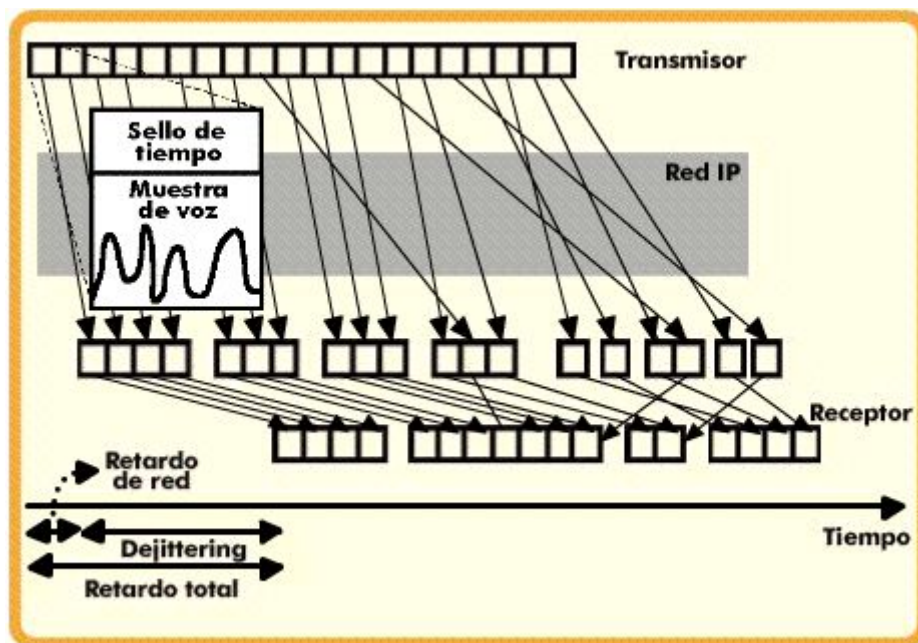
Los paquetes son desviados por los encaminadores hacia la rama siguiente según van llegando.

Se colocan, en función de su orden de llegada, en colas de espera de partida.

El tiempo de tránsito en estos encaminadores estará en función del tráfico al que se vean sometidos en un momento dado.

Dependiendo del número de encaminadores atravesados, podemos encontrarnos bastante lejos de las restricciones del tiempo real.

El tiempo de tratamiento de los equipos terminales



Otro factor muy influyente es el tiempo que tardan en procesarse los paquetes en los distintos equipos de la red.

En los equipos terminales, este tiempo se debe a:

- **El emisor:** digitalización, compresión, división en paquetes:

Otra diferencia fundamental separa a Internet de la red telefónica. El equipo terminal de telecomunicaciones, el teléfono, no efectúa ningún tratamiento. Se limita a restituir una señal analógica o digital al interlocutor. El único retraso notable viene dado por el transporte. Por el contrario, el terminal de la red IP tiene que asumir una pesada tarea. La voz se recibe a través de un micrófono, y después se digitaliza en una tarjeta de sonido.

La señal digital en bruto, se comprime mediante algoritmos matemáticos complejos para que ocupe el menor espacio posible, antes de ponerse en paquetes y transmitirse. La compresión en tiempo real es la más exigente en recursos de CPU; cuanto más potente sea un ordenador, mas rápido la hará.

El tiempo de tratamiento por el emisor puede requerir, según la máquina, de 50 ms a varios cientos de milisegundos.

- **El receptor:** el búfer de resincronización.

Pero para el terminal de recepción, el tratamiento es aún superior. Los paquetes pueden llegar en desorden y con un espaciado importante y variable.

Hay que dar a la señal una velocidad constante, restituirle la fluidez. El flujo tiene que recuperar las referencias de tiempo en vigor en el momento de su creación; tiene que resincronizarse.

La aplicación tiene que temporalizar, "bufferizar"; contará con algunas centésimas de segundo suplementarias para disponer del número de paquetes necesario para

la reconstrucción del flujo, lo que le permitirá compensar las variaciones en el retardo (dejittering) de encaminamiento que pueden sufrir los paquetes.

Sólo entonces los paquetes seguirán el tratamiento de restitución: reintegración, descompresión, conversión en señal analógica, amplificación y difusión por los altavoces.

Si la señal recibida está muy dañada, tendrá que sufrir un verdadero trabajo de restauración que aumentará aún más el tiempo de tratamiento.

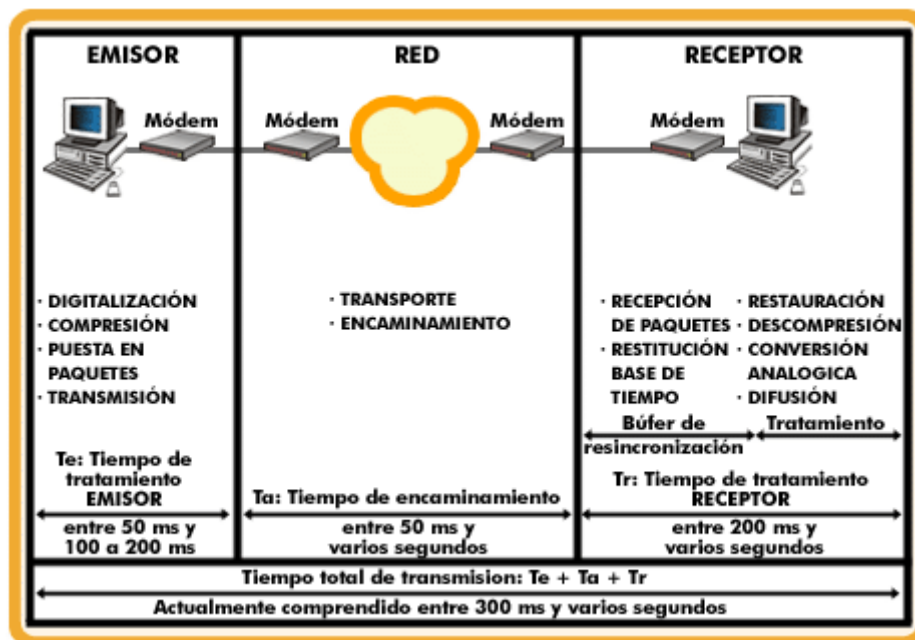
El ordenador destinatario intentará reemplazar los paquetes que faltan por un silencio, un ruido en blanco, o un valor estimado o calculado.

Según la potencia de los ordenadores y la importancia y el tamaño del búfer, el tiempo de tratamiento ocupará de 200 ms a más de un segundo.

El retardo total

Comenzamos, pues, a resumir los aspectos anteriormente vistos.

En cuanto al retardo, debemos considerar que hay que sumar el tiempo de tratamiento por parte de los terminales de los extremos a la demora de encaminamiento para obtener el retardo total entre la fuente y el receptor.



Pero, ¿de verdad que no puede haber algún factor adicional que incremente dicho retardo?

Desafortunadamente, no podemos responder afirmativamente a esa pregunta.

Por ejemplo, en caso de congestión persistente, es decir, de sobrecarga y atasco en la red, estos dos tiempos, desgraciadamente, se desvían a la vez.

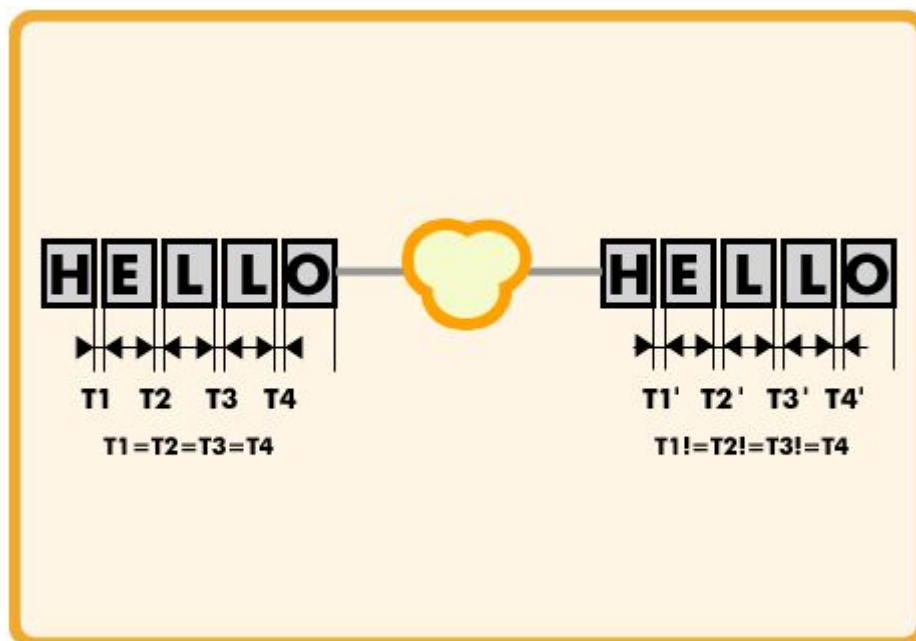
Una red cargada, inducirá tiempos de transporte prolongados y una variación de la cadencia importante (jitter), que habrá que corregir aumentando el tamaño de los búfer (dejittering).

La fuente intentará disminuir la velocidad de salida aumentando la compresión y, por tanto, su tiempo de tratamiento.

Este retardo total es el que debe ser inferior, si es posible, a 150 ms y nunca superior a 400 ms, para permitir la interactividad, el full-duplex.

Más allá de este valor, se hablará de "casi tiempo real"; un modo suficiente para los servidores de medios, radio, archivos de audio, o el trabajo cooperativo en half-duplex.

Una transmisión asíncrona y no síncrona



Además, si consideramos otro nuevo factor, no sólo pueden ser prolongadas las demoras, sino que, además, no son constantes. Mantener a lo largo de todo el camino un mismo espaciado reducido entre los paquetes no forma parte de las preocupaciones de la red.

El transporte es asíncrono. El ritmo de emisión de los paquetes por la fuente no se respeta en el transporte. No hay relación de tiempo entre el emisor y el receptor

El transporte sería sincronizado si hubiera una relación fija entre el ritmo de emisión de los paquetes y el de su recepción. El transporte en tiempo real exige que esta relación sea igual a uno, es decir, que las demoras de salida y llegada sean iguales y constantes. Una red de este tipo se denomina isócrona.

Bueno, pues las redes IP son redes donde el transporte es asíncrono, con lo que tenemos una nueva preocupación extra para la transmisión de voz.



Orden y camino

¿Creías que habíamos terminado? No, aun quedan algunos flecos por considerar...

Los encaminadores están conectados a varias sedes que les ofrecen una gran variedad de caminos posibles para orientar un paquete hacia una dirección dada. La red no es determinista. No hay un camino obligatorio, sino un amplio abanico de opciones.

Los itinerarios se actualizan sin cesar en las tablas de encaminamiento en función de criterios "económicos"; el algoritmo de cálculo de estas tablas efectúa un arbitraje permanente en función de la carga y el tráfico en cada camino, o en función del número de "saltos" encontrados. Este arbitraje se hace para cada paquete individual, sin tener en cuenta el "histórico".

En el caso de un flujo de audio, todos los paquetes debieran sucederse y seguir rigurosamente el mismo itinerario. No es éste el caso, y los paquetes de una misma conversación pueden, teóricamente, tomar rutas totalmente diferentes según la situación instantánea de la red.

En este aspecto, aún brilla una pequeña luz de esperanza en el caso de redes IP, ya que en la práctica, se percibe que el itinerario presenta una cierta estabilidad; es la estrategia del camino más corto la preponderante hasta un cierto umbral de congestión de la red.

Una ruta relativamente estable se establece de un nodo hacia el mismo destino. Sin embargo, ruta única y respeto por el orden de llegada no vienen garantizados nunca por la red.

La red no es fiable



Por último, no olvidemos que el viaje de un paquete por Internet presenta peligros.

- **Destrucción por un encaminador escaso de recursos**

Los encaminadores no tienen capacidad ilimitada. Cuando la memoria reservada a la gestión de los archivos de espera de emisión está saturada, entran en congestión y los paquetes que se presentan a su puerta son ignorados y, simplemente, se destruyen.

- **Tiempo de vida limitado**

El paquete cuenta también con una duración de vida limitada que disminuye a cada paso por un nodo. Un trayecto demasiado largo podrá consumir la totalidad del crédito, y el paquete se destruirá.

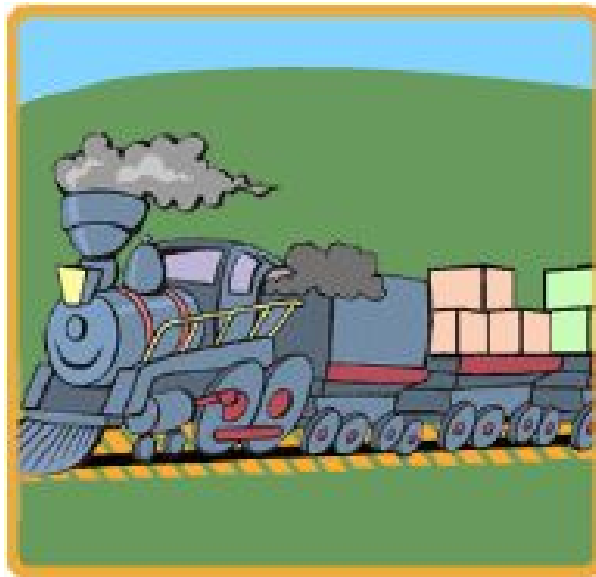
- **Llegada tardía**

Un paquete puede llegar sano y salvo a su destino, pero presentar un retraso demasiado importante y superior al tamaño de la memoria intermedia del búfer de resincronización (dejittering). El flujo de tiempo real no espera; se difundirá a pesar de la ausencia del paquete retrasado. Dicho paquete, ahora inútil, se destruirá.

- **Resumiendo**

Resumiendo, la red IP no es una red fiable que garantice la llegada a tiempo o simplemente la mera llegada a su destino de los paquetes que transporta. Los equipos de los extremos pueden implementar protocolos de transporte fiables como TCP, que establece una conexión punto-a-punto e implementa un mecanismo de confirmación y reenvío de paquetes perdidos. Pero tales sistemas imponen idas y venidas de paquetes de control y de contenidos entre el emisor y el destinatario que son incompatibles con las restricciones de demora del tiempo real. Un mecanismo con fiabilidad punto-a-punto multiplica, como mínimo, por dos la demora unitaria de transmisión; al tiempo de encaminamiento del primer paquete, habrá que añadir el del paquete de control (el reconocimiento).

Primer balance



La primera conclusión que se puede extraer de esta enumeración de dificultades está lejos de ser negativa.

Internet es estructuralmente capaz de transportar datos en tiempo real.

La práctica demuestra que la demora de transporte puede ser llevada dentro de límites compatibles con la interactividad de una conversación.

La fiabilidad no se garantizará nunca, de acuerdo, pero las tasas de pérdidas inferiores al 5% son asumibles; el terminal receptor puede "llenar" los agujeros y "restaurar" la señal mediante diversos tratamientos digitales.

Por el momento, la red es poco eficaz. Pero todos los defectos son coyunturales.

"Basta" con aumentar el ancho de banda y "basta" con disponer de recursos para curar todos los males.



Bienvenido al capítulo:

Aplicaciones VoIP

4.1 Introducción

Introducción a la Sección 4.1

Vas a comenzar el apartado 4.1:

El enfrentamiento entre dos mundos



Antes de nada, veamos una polémica que ha afectado durante los últimos años a la integración de las dos principales mundos en que se divide el área de las telecomunicaciones: los servicios de voz y los de datos...

Los ingenieros del "mundo de la voz" y los del "mundo de los datos" no se comprenden. Se acusan mutuamente de menosprecio recíproco.

La telefonía es una vieja dama. Ha introducido la rigidez en la práctica de la comunicación vocal en una carcasa de reglas y planificación.

Y ésta es una evolución natural para una actividad que ha llegado a la madurez y se ha visto elevada al rango de servicio público.

Su objeto, la comunicación entre personas, es también cada vez más el de la informática multimedia, que pasa del tratamiento local de la información a la era de la conectividad universal.

Aún hoy – pero, ¿por cuánto tiempo? – comparten el espacio en el despacho el teléfono y el terminal informático.

El primero ya no evoluciona, mientras que el segundo transmite ya la voz, por red local o global, y la integra naturalmente con los datos.



La cuestión de la tarificación

¿Y en qué se traduce principalmente la diferencia entre ambos mundos? Pues en el coste que llevan asociado...

Sea cual sea su país de origen, el abonado al servicio telefónico está acostumbrado a pagar sus comunicaciones en función de la distancia y de la duración. No se ofusca por ello. Este modo de facturación es natural; es un calco del transporte terrestre y corresponde a una percepción intuitiva de la utilización de las infraestructuras.

1994

Su sorpresa fue mayúscula cuando, a partir de **1994**, descubrió Internet y su aparente gratuidad.

¿Quién podía pagar por cargar una página Web desde los Estados Unidos? Progresivamente, el principio de la red informática y su acceso por tiempo de uso ha entrado en las costumbres. Pero el contraste se ha hecho flagrante entre el coste marginal, próximo a cero, del transporte de paquetes por Internet, y el precio anormalmente elevado, y a menudo incoherente, de las llamadas internacionales.

1995

Cuando aparecieron las primeras aplicaciones de conversación vocal en el mercado, a principios de **1995**, fue para atacar frontalmente el “monopolio” de los operadores de telefonía. Una picadura de mosquito en la piel de los grandes paquidermos. La telefonía por Internet toma sus primeras armas y la señal aún está lejos de los estándares de calidad de los operadores tradicionales. Estos últimos tienen aún unos años prósperos por delante, antes de que una red IP federe definitivamente todas las comunicaciones del planeta.

DESREGULACIÓN

Pero ese tiempo ya pasó; se abre la veda en los países que mantienen los viejos monopolios, y comienza un proceso de **desregulación** que afecta a todos los países, firmando el fin de los monopolios y de una era en la telefonía. Los recursos son cada vez más abundantes a medida que la fibra óptica se extiende a lo largo de las autopistas, las vías férreas y las canalizaciones de agua. Nuevos operadores las empiezan a utilizar, apostando por tarifas atractivas para conquistar a los abonados.

Ahora bien, en el secreto de los estados mayores, los operadores tradicionales conocen la salida a esta confrontación. Algunos se están preparando con estrategias de crecimiento basadas en el transporte de datos.



Veamos ahora algunas estrategias encaminadas a la evolución gradual hacia una convergencia de redes, en la que el objetivo último es utilizar una única red tanto para voz como para datos.

4.2 Evitando la Red Telefónica Tradicional

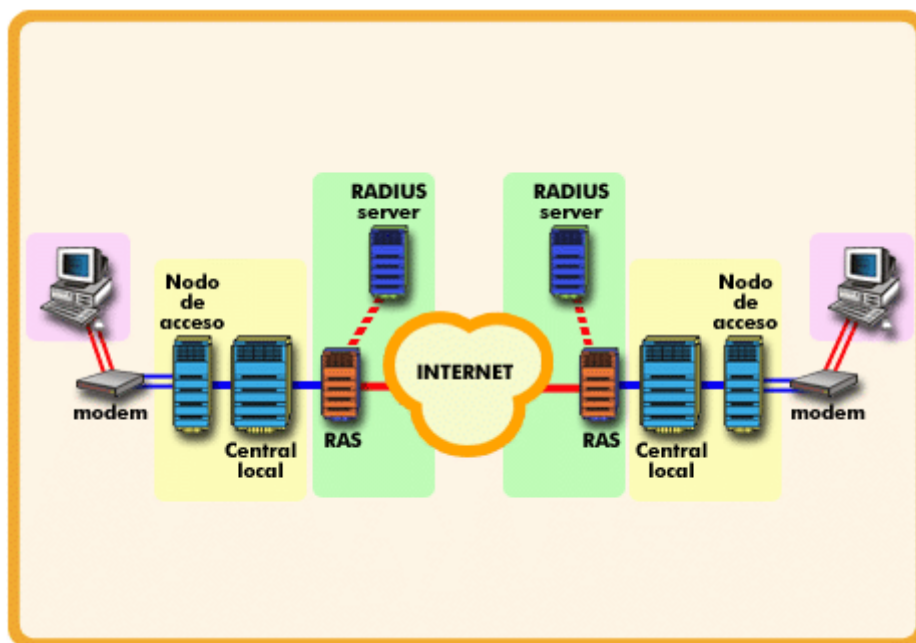
Introducción a la Sección 4.2

Vas a comenzar el apartado 4.2:

Llamadas PC-a-PC

La primera estrategia que se nos ocurre a la hora de converger ambas redes es una coexistencia entre las mismas, pero procurando en la medida de lo posible, evitar al máximo la utilización de aquella red que pensamos sustituir, es decir, la red telefónica.

Dentro de este caso, nos podemos encontrar con varios escenarios posibles...



La primera idea es muy simple; se basa en utilizar la red Internet para las comunicaciones de voz PC-a-PC, evitando a la red telefónica tradicional (las centrales de tránsito), de manera que nuestra conversación sea tratada como un acceso "normal" a Internet, y sólo sea tarificada con el coste de una llamada local.

Este escenario requiere que los dos interlocutores estén previamente conectados a Internet a través de sus respectivos RAS, con sus ISPs correspondientes.

Es decir, no podemos pensar en escenarios parecidos a los de las llamadas en la telefonía "normal" porque un usuario no podrá ser notificado de que tiene una "llamada entrante" a menos que esté previamente conectado a Internet y utilizando alguna aplicación que le permita acceder a este servicio.

Por lo tanto, todo el procesamiento relativo a VoIP tendrá lugar en los propios PCs, y no hay necesidad de ningún otro nodo intermedio que incorpore mecanismos propios de VoIP.



Las primeras aplicaciones comerciales de telefonía aparecieron en el mercado a principios de 1995.

Pero la infancia de la telefonía en Internet no ha durado más que una primavera.

En el primer semestre de 1996, Netscape y Microsoft se lanzan a la batalla.

Aplicaciones utilizadas en las llamadas PC-a-PC



Los productos de telefonía en el mercado están todos estructurados de manera parecida.

Presentan un panel de control que sirve para acceder a las principales funciones de telefonía y proporciona acceso a los menús de configuración y de opciones.

- Ajuste de los niveles del terminal: la primera operación consiste en regular el nivel de sensibilidad del micrófono y del equipo multimedia, tarjeta de sonido y altavoces. El panel de control permite definir un umbral de silencio por debajo del cual la aplicación no registrará los sonidos. El ruido de fondo tampoco se tendrá en cuenta y ningún flujo inútil molestará a la red. Un umbral de silencio demasiado elevado puede traducirse en una degradación de la señal; las partes de algunas palabras pronunciadas en voz demasiado baja pasarán por debajo del umbral y se considerarán como ruido, con lo cual, la palabra será cortada sin que la red ni el ancho de banda tengan la culpa. En caso de recepción defectuosa, el primer reflejo será pues solicitar al interlocutor que baje el umbral de silencio de su aplicación.
- La velocidad de salida: El usuario debe fijar la frecuencia de muestreo de la señal en la tarjeta de sonido.

Cuanto más elevada sea, la calidad será mejor, pero mayor será la frecuencia de salida. Esta frecuencia puede limitarse por la velocidad del módem, o por las condiciones de tráfico de la red.

Debe ajustarse al principio de la conversación y, posteriormente, en el transcurso de la comunicación si cambian las condiciones. La señal muestreada se comprime fuertemente mediante algoritmos de compresión.

- Procedimientos de llamada y opciones: todos los productos se relacionan con los IRC que dan la lista de las personas que utilizan la misma aplicación y están conectadas en directo.

Según el producto, un menú permite también pasar una llamada a una dirección IP identificada, permanente y correspondiente a una máquina ya conectada a la red. La encriptación de conversaciones vocales puede incluirse en el producto.

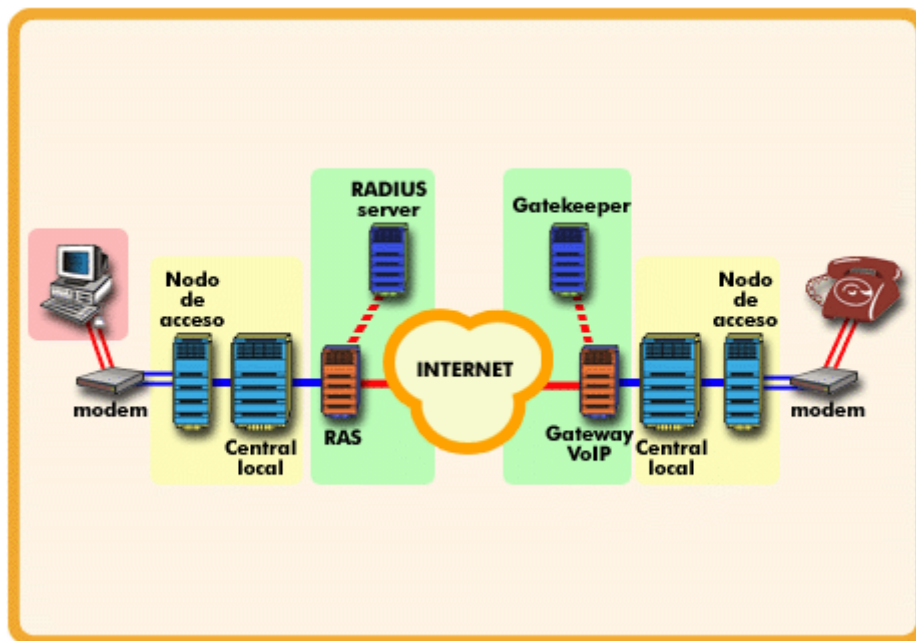
Una opción mensajería permite la toma de mensajes vocales por la máquina.

El principal **inconveniente** de este escenario es la incompatibilidad entre el software de las distintas aplicaciones, que hará imposible cualquier comunicación entre usuarios de distintas aplicaciones.

Además, al utilizar la red Internet como red de transporte de la voz, la calidad de servicio no está garantizada, con lo que las latencias pueden llegar a ser muy grandes.

Llamadas PC-a-teléfono

Si bien Internet permite telefonar al otro extremo del mundo, los únicos diálogos posibles utilizando el escenario anterior son entre usuarios equipados con ordenadores multimedia, una conexión a Internet, la misma aplicación, ... y conectados simultáneamente.



¿Y por qué no utilizar el teléfono como destino de una llamada?

La idea es muy simple, aunque otra cosa es el coste de su implementación. Basta con instalar en los grandes centros urbanos pasarelas o gateways, conectadas a la vez a Internet y a la red telefónica. Estos gateways serán los responsables de traducir las señales de voz a paquetes IP y viceversa.

Además, necesitaremos controladores de gateways, llamados a veces gatekeepers, que puedan ordenar a los gateways los eventos de señalización del mundo telefónico: toma de línea, envío de corriente de llamada, ...

Con este sistema, un abonado a Internet que desee llamar a un interlocutor lejano puede hacerlo marcando su número de teléfono en el teclado de su ordenador.

En función de este número, el proveedor del servicio del usuario, encamina la petición hacia el gateway más próximo al domicilio del interlocutor.

El gateway tomará una línea telefónica y llama al número solicitado; cuando el interlocutor descuelga, las dos partes se ponen en contacto.

Así, Internet y su tarifa ventajosa es quien encamina la comunicación tan cerca como sea posible del interlocutor, pero es la telefonía la que se encarga de la conexión final, cosa que no sabe hacer la red IP.

Desde el punto de vista del usuario del PC, él es quien debe contactar con el proveedor del servicio de telefonía sobre IP, y enviarle a él la información de señalización. Para ello, el usuario deberá disponer de un software de aplicación suministrado por proveedor del servicio, lo que nos lleva, de nuevo, al problema de

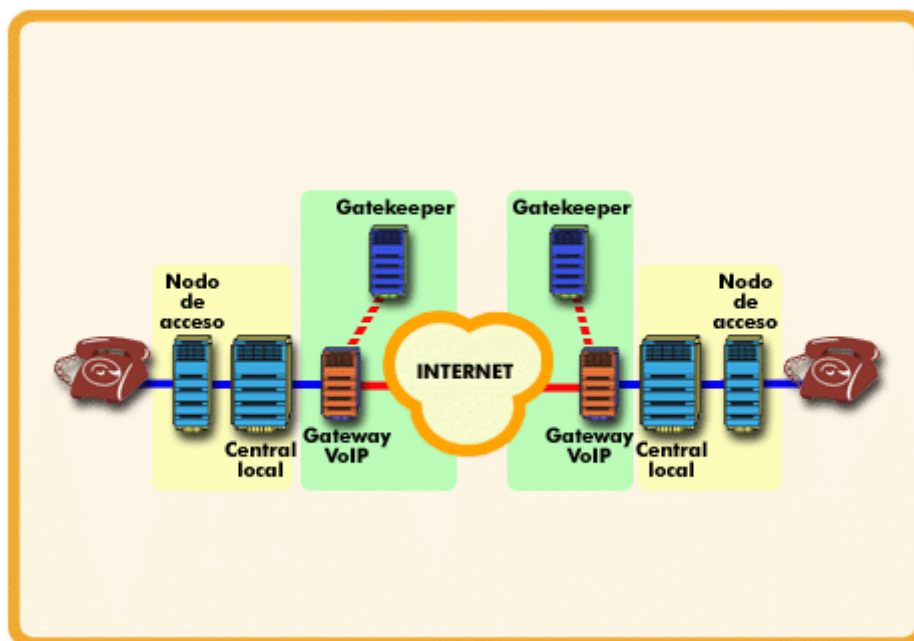


la compatibilidad entre aplicaciones de distintos proveedores. Hoy día existen proveedores que permiten la descarga gratuita de la aplicación que permite utilizar sus servicios, durante un período de prueba, y después ofrece unas tarifas moderadas.

Sobre la calidad de servicio, ya podemos imaginar lo que nos espera: la calidad de Internet, o lo que es lo mismo, ninguna. Puede que tengamos grandes latencias en nuestras comunicaciones.

Además, el servicio no tendría por qué ser gratuito. Téngase en cuenta que el proveedor del servicio debe mantener líneas de comunicación permanente con Internet y acceso a la red telefónica conmutada.

Llamadas teléfono-a-teléfono



¿Qué nos quedaría? Pues la interconectividad total. Si se utiliza hasta el extremo el principio del gateway, ya no es necesario que el emisor de la llamada se encuentre en Internet.

Le basta, utilizando la red telefónica local, llamar mediante su aparato telefónico al gateway de su elección e iniciar una llamada internacional.

La comunicación enlazará con las vías “subterráneas” de Internet, para emerger en otro gateway situado en la proximidad de la residencia del interlocutor.

Si pretendemos que la utilización por los usuarios sea lo más transparente posible, tendremos que evitar cualquier cambio en su comportamiento; es decir, él debe seguir utilizando el teléfono como lo venía haciendo hasta ahora, marcando directamente el número telefónico de su interlocutor.

Y es aquí donde interviene la figura del controlador de gateways, llamado gatekeeper a menudo. Internet no entiende de números telefónicos, tan sólo opera con direcciones IP.

El gatekeeper traducirá números telefónicos a direcciones IP, y viceversa. Además, será capaz de entender la señalización telefónica (SS7) y transportarla por la red IP hasta hacerla llegar a la central local del destinatario.

Este sería un escenario interesante para los operadores establecidos, si lo que pretenden es descargar sus saturadas redes de voz, a la vez que ofrecen a sus abonados tarifas más competitivas.

Sobre la calidad de servicio, como siempre, será la de Internet. Aunque, en este caso, el proveedor del servicio puede contratar una garantía de recursos con un operador privado de Internet. El tiempo de transmisión y la tasa de pérdida de paquetes están entonces perfectamente controlados gracias a protocolos como RSVP o RTP, y el proveedor puede comprometerse a un nivel de calidad de servicio comparable al de la telefonía.



El servicio prestado por los proveedores de pasarela de Internet no será gratuito. Competirán directamente con todos los operadores de telefonía surgidos de la liberalización general del sector.

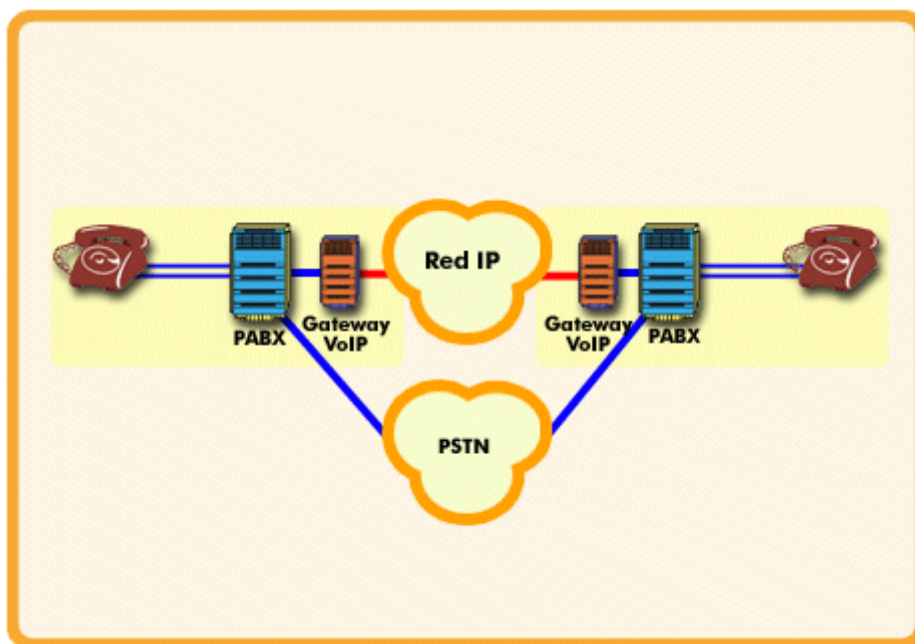
La alternativa de transporte ofrecida por IP sólo tiene aquí un interés económico. No aporta ninguna dimensión suplementaria a la comunicación telefónica clásica, ni en calidad de servicio ni en la utilización de nuevos servicios suplementarios.

Pasarela (gateway) corporativa

¿Se nos han acabado las alternativas en este tipo de estrategia?

Pues ciertamente no, ya que todavía no hemos tocado el mundo de las centralitas privadas.

Veamos qué posibilidades se abren para sus usuarios...



En una primera aproximación, la evolución natural de aquellas corporaciones que ya utilizaban sus redes de datos para el transporte de la voz, como ocurre con aquellos que utilizan redes Frame Relay, es la interconexión de sus redes locales IP a través de una red IP corporativa, en la que volveremos a integrar la voz, transportándose ahora en datagramas IP.

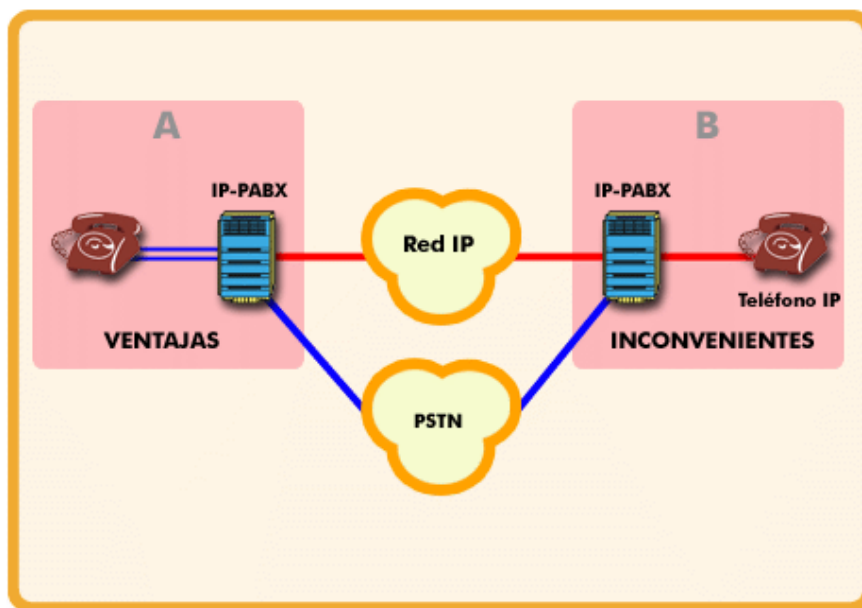
La solución consiste en la utilización de centralitas corporativas (PABX) conectadas directamente a los gateways de voz sobre IP.

El gateway sirve de intermediario entre la red de voz y la red IP, pudiendo incluso, estar integrado en un encaminador IP que fuese, a su vez, el "colector" de todas las redes locales de la oficina que encamina el tráfico de las redes locales hacia un enlace WAN.

El Gateway de VoIP entiende la señalización que se envía desde la PABX y localiza el Gateway de salida basándose en la numeración del destinatario. Entra en contacto con dicho Gateway remoto, el cuál iniciará la llamada a su PABX local. Una vez resuelta la señalización, comenzará el flujo de datos.

Nada nuevo que no hayamos visto hasta ahora, pero aún no hemos acabado con el tema...

PABX (Centralita) IP



Viendo el escenario anterior, se puede deducir visiblemente que el siguiente paso evolutivo es la integración de la PABX tradicional junto con el gateway de VoIP, formando lo que se denomina una PABX IP, cuya implantación puede desarrollarse en dos fases.

- **(A)** Supone la sustitución de la PABX y el gateway de VoIP por el equipo integrado PABX IP.

La interfaz hacia el usuario sigue siendo analógica o RDSI, pero ahora su salida hacia la red es en forma de paquetes IP que se integran en la red IP corporativa.

- **(B)** En una etapa posterior, puede sustituirse la PABX IP de la fase 1 por una nueva generación de PABX IP en la que todas sus interfaces sean IP, hacia la red y hacia el usuario.

Esto conllevará la sustitución de todos los teléfonos tradicionales por teléfonos IP, que se conectarán directamente al tráfico de las redes locales corporativas.

Las ventajas que ofrecería este escenario para las redes corporativas están bastante claras: aparte de la integración de los datos en un único protocolo y red, está la cuestión del coste, que resultaría muy inferior al generado por la solución tradicional, pero ¿qué nuevos problemas pueden surgir?

Si hablamos de **los inconvenientes** que plantea este tipo de implementación, tendremos que mencionar el mismo problema de planificación de numeración que en el caso anterior; habrá que prever distintos planes para llamadas a través de la red IP y llamadas a través de la red telefónica tradicional.

Además, en la fase segunda, en la que se despliegan los teléfonos IP sobre las LAN corporativas, ¿quién garantiza la calidad de servicio en dichas LAN? Los teléfonos IP van a ser unos grandes consumidores de recursos que ahora competirán con equipos de datos conectados a las LAN corporativas, y traerán más de un quebradero de cabeza nuevo a los administradores de las redes locales...



4.3 Sustituyendo la Red Telefónica Tradicional

Introducción a la Sección 4.3

Vas a comenzar el [apartado 4.3](#):

Introducción

¿Cuál es la segunda estrategia que podemos plantearnos a la hora de integrar las redes telefónica e IP? Pues ser ambiciosos y cumplir el objetivo final de dicha integración: sustituir la red telefónica por nuestra red IP, capaz de integrar tanto servicios de telefonía tradicional como de transmisión de datos.

Bueno, la sustitución de la red telefónica tradicional tendrá lugar cuando logremos utilizar las redes IP para las comunicaciones de voz de todo tipo de usuarios sin utilizar las redes telefónicas públicas. Sin duda, constituye el desafío más ambicioso.

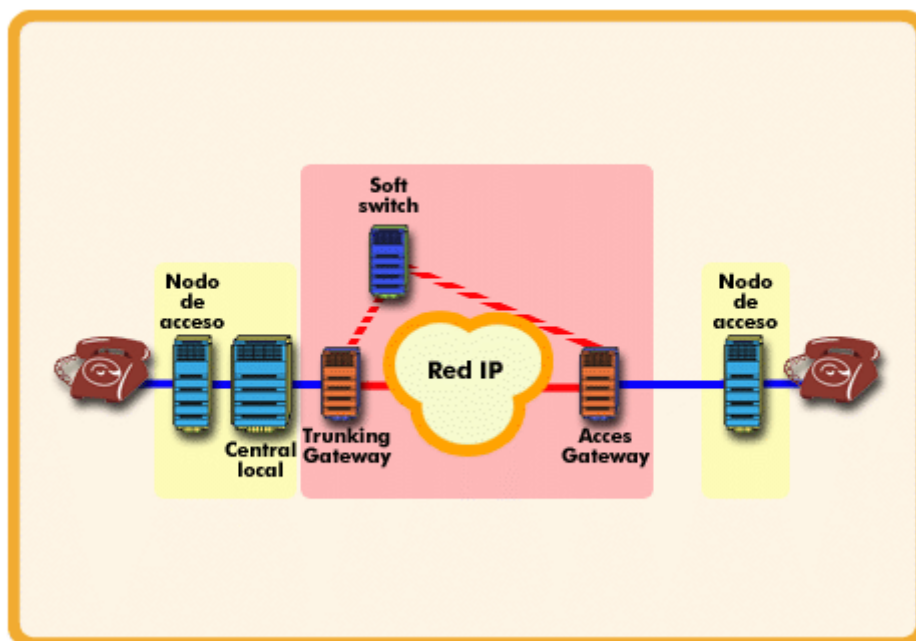
Además, la sustitución de dichas redes telefónicas seguramente no se hará de golpe, sino que habrá que pasar por varias etapas.

- Empezaremos con la sustitución de las centrales de tránsito, con lo que todas las llamadas podrán considerarse como llamadas locales.
- Sustituiremos después las centrales locales para lograr una estructura integrada tanto en el acceso como el núcleo de la red.

Las funciones que llevaban a cabo las centrales de conmutación de voz serán ahora realizadas por los encaminadores (routers), que serán los encargados de difundir la información desde el origen al destino. Sin embargo, no basta sólo con encaminadores; hace falta un nuevo tipo de equipos que sepa cómo encaminar la llamada hacia el destino partiendo de un número telefónico y que realice funciones de señalización y tarificación. Este equipo es el que se conoce como **SoftSwitch**.

El inconveniente más importante que presenta esta solución en el momento actual es la inmadurez de los estándares; por ejemplo, las polémicas entre los partidarios de los protocolos MEGACO contra los partidarios de MGCP, los diferentes modelos propuestos desde IETF y desde ITU, ...

El Softswitch o la Sustitución de las centrales de tránsito



Si vamos analizando fase por fase cómo será el proceso de sustitución de la red telefónica tradicional, en la imagen mostramos cómo será la primera de ellas, en la que comenzamos con la sustitución de las centrales de tránsito.

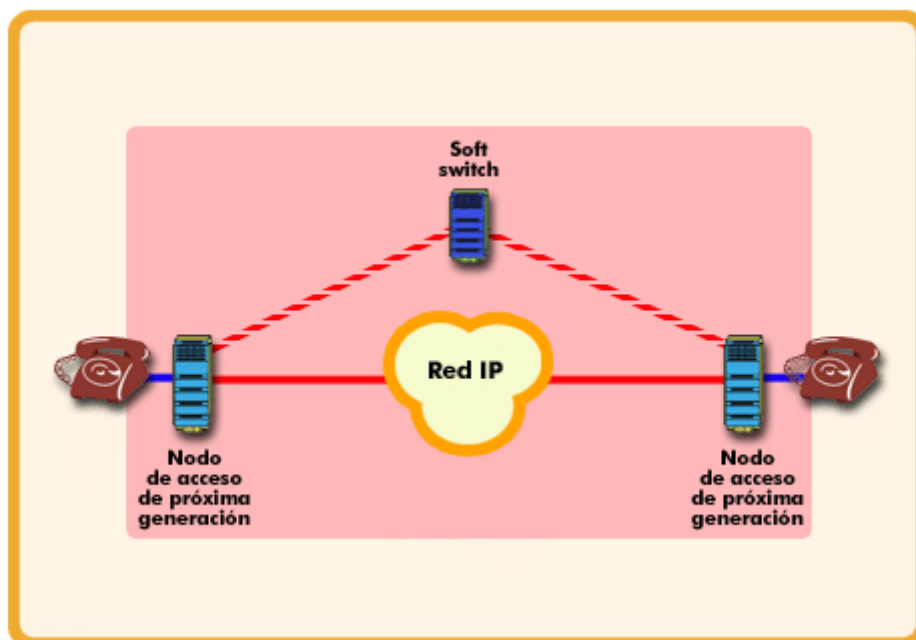
En esta fase, necesitaremos tres tipos de equipos.

- El propio SoftSwitch, que va a controlar a los gateways de VoIP.
- Gateways de acceso (Access Gateways) para la agregación de nodos de acceso.
- Trunking Gateways para el interfaz con las antiguas centrales de la red telefónica tradicional.

Cada vez que un gateway detecta la señalización de llamada entrante, contactará con el SoftSwitch para que éste le resuelva la dirección IP con la que hay que contactar para dar curso a la llamada.

Red de Acceso Integrada

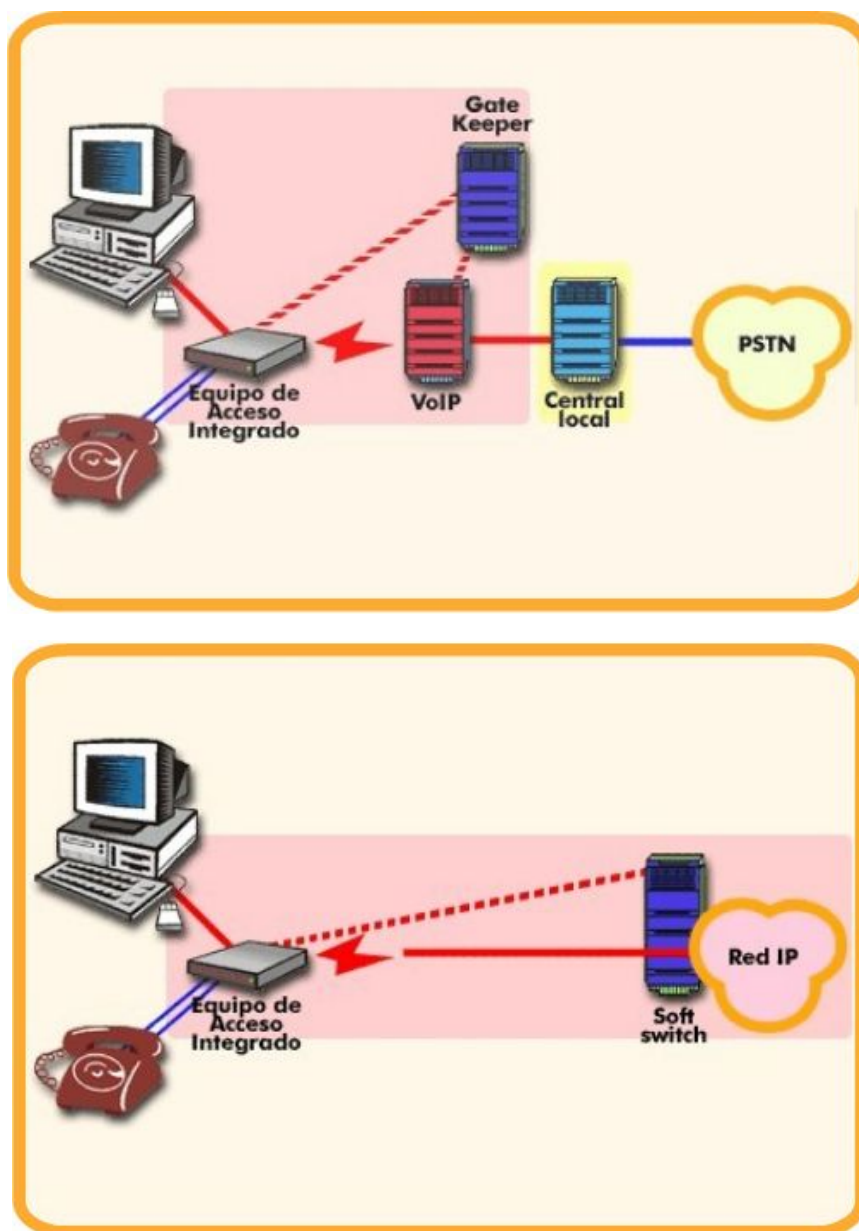
En la fase posterior, también procederemos a la sustitución de las centrales locales, constituyendo una red IP integrada en la que tan sólo los interfaces hacia el usuario siguen siendo tradicionales, y cuyo esquema sería el mostrado en la figura.



Esta nueva apuesta también necesitará del concurso de nuevos equipos; se trata de los nuevos nodos de acceso con el gateway VoIP integrado.

Una vez dentro de la red IP, bajo control del SoftSwitch, todo funcionará como en el caso anterior.

Equipos de Acceso Integrados



¿Qué función realizarán este tipo de dispositivos? El objetivo que se proponen es la creación de una única red de acceso para voz y datos.

Por ejemplo, como se muestra en la imagen, disponer de un único nodo de acceso integrado para todo tipo de redes de acceso inalámbrico, sean estas de banda ancha (LMDS) o de banda estrecha (WLL). En una primera fase, mientras tengamos todavía centrales locales, seguiremos necesitando los gateways de VoIP y los gatekeepers para el interfaz con dichas centrales.

En una segunda fase, según se muestra en la imagen, donde la utilización del SoftSwitch haga innecesario el uso de la telefonía tradicional, podremos prescindir de gateways y gatekeepers.

4.4 Servicios de Valor Añadido

Introducción a la Sección 4.4

Vas a comenzar el apartado 4.4:

Proporcionar Servicios de Valor Añadido VoIP



¿Cómo afecta a los servicios ofrecidos por las redes telefónica clásicas la utilización (ya sea sólo como transporte entre accesos locales a las redes telefónicas o la sustitución de dichas redes por redes IP) de la tecnología de VoIP?

La gestión personal de la telefonía

Al conocer la disponibilidad de todos los puntos de la red y controlar la conmutación, es posible implementar estrategias de telefonía evolucionadas. Se identifica al que llama, su ficha se extrae de la base de datos de la red, se muestra en la pantalla en el momento de pasar al interlocutor.

En una Intranet, el conjunto de los datos se visualiza en un navegador estándar. La gestión de la llamada se realiza a partir de cada puesto; puede rechazarse, transferirse o enviarse hacia la mensajería con un simple "clic" de ratón.

Ofrecimiento de nuevos servicios desconocidos en las redes telefónicas

Nuevos servicios para el comercio electrónico están ya disponibles. Servicios como "Click to dial" facilitará la compra por Internet permitiendo contactar al comprador con "call center" que le asesoren "de viva voz" sobre ciertos productos.

La comunicación de voz mientras navegamos también es actualmente posible, cuando utilizamos el servicio "Surf and talk" junto con la tecnología VoIP.

El buzón unificado de mensajería

Además de, como vimos anteriormente, permitir que la gestión de la llamada entrante puede rechazarse, transferirse o enviarse hacia la mensajería con un simple "clic" de ratón, el mismo buzón recibirá no sólo los mensajes internos y externos provenientes de Internet, sino también los faxes y los mensajes orales.

Estos últimos, almacenados en el mismo buzón, son fácilmente accesibles y difundidos hacia el ordenador del usuario. Son consultables desde el exterior mediante Internet, o por la red telefónica conmutada. El correo electrónico se lee por síntesis vocal.

Videotelefonía en Internet

Mediante webcams podemos ya transmitir imágenes a través de la red IP. Con la integración de la telefonía dentro de las redes IP, gracias a VoIP, el siguiente paso evolutivo será sincronizar la imagen enviada con la voz transmitida vía telefónica, es decir, el envío de videotelefonía a través de Internet.

El inconveniente que se plantea aquí es el del ancho de banda necesario para transmitir imagen en tiempo real, pero se están realizando avances firmes en dicha dirección. ¿La veremos implementada por fin?



Bienvenido al capítulo:

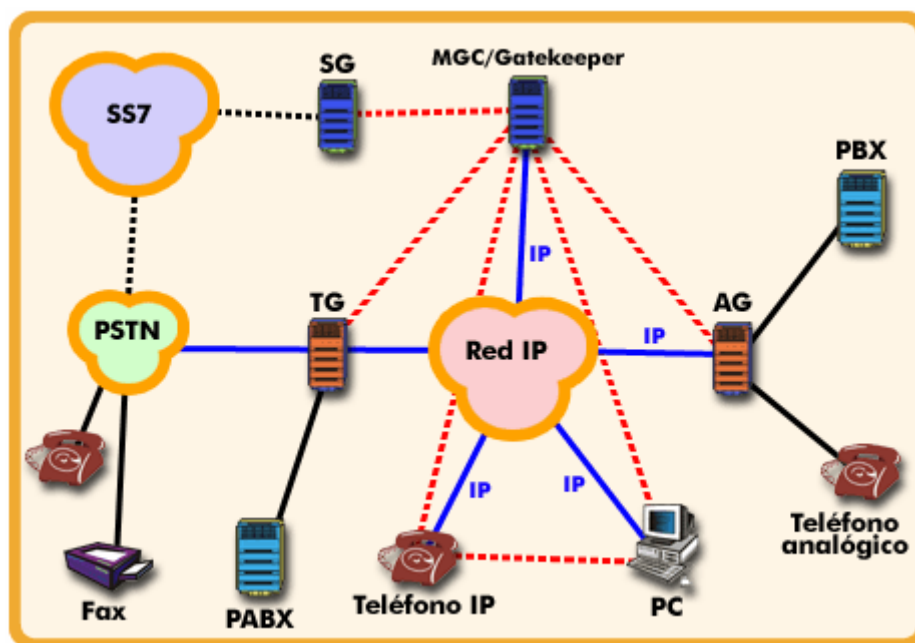
Modelo de red y Protocolos

5.1 Modelo de Red

Introducción a la Sección 5.1

Vas a comenzar el apartado 5.1:

La Falta de Estandarización en el Modelo de Red



Cuando hablábamos de la inmadurez de los estándares como un serio inconveniente para el desarrollo tecnológico de las soluciones de VoIP no lo decíamos en broma.

Dos organismos internacionales como son el [IETF](#) y el [ITU](#) proponen dos modelos de red diferentes, cada uno con sus funcionalidades y protocolos.

El IETF, la organización que regula y estandariza el mundo de Internet, define un modelo de topología de red conocido como **Softswitch Model** y que consta de los siguientes elementos:

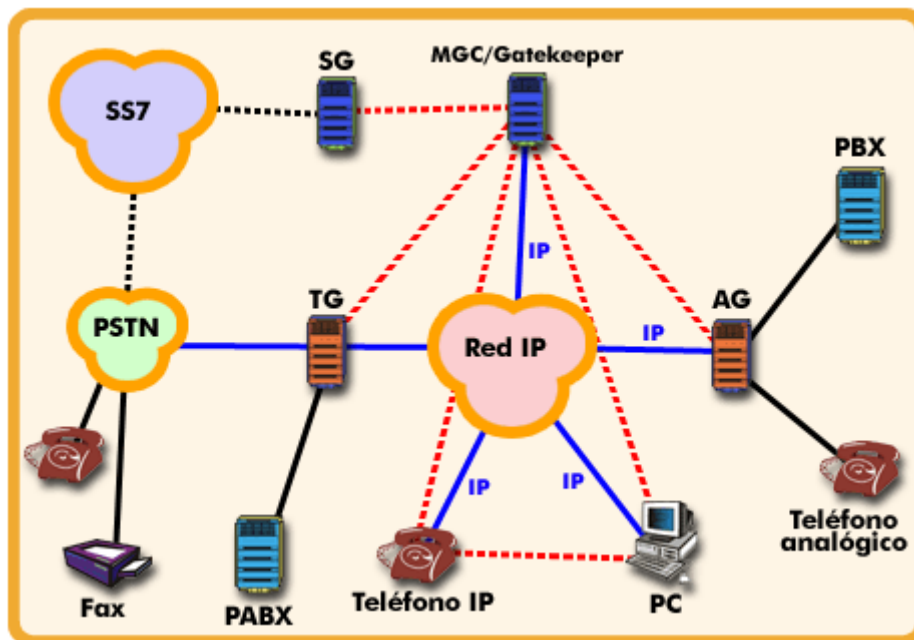
- **Media Gateways (MG):** son los equipos que manejan la conversión de la voz del formato de circuito (PCM) al formato de paquete (datagrama). Puede haber *Trunking Gateways* y *Access Gateways*, según tengan interfaces con líneas *trunking* o de PBX, respectivamente.
- **Media Gateway Controllers (MGC):** también llamados *Call Agents*, son los que gestionan las conexiones en la red de paquetes. Contienen la funcionalidad del control de llamada (*Call Control*)
- **Signalling Gateway (SG):** es el interfaz con la red de señalización número 7 (SS7) de la red de conmutación de circuitos.

En el lado opuesto está ITU, que en su estándar H.323 define un modelo de topología de red diferente, que consta de:

- **Terminal:** un Terminal H.323 es cualquier *end-point* de la red que es capaz de establecer comunicaciones dúplex, en tiempo real, con cualquier otro terminal H.323 o cualquier Gateway.
- **Gatekeeper (GK):** el *Gatekeeper* es una entidad H.323 de la red que proporciona la traducción de direcciones y los controles de acceso a la red para los Terminales H.323 y los *Gateways*.
- **Gateway (GW):** es el interfaz entre la red IP y la red de conmutación de circuitos que maneja la conversión de la voz al modo "datagrama".

Elementos del Modelo de Red

Fijándonos en el modelo de red propuesto por el IETF, vamos a estudiar las principales funcionalidades de cada uno de los elementos de dicho modelo de red:



Media Gateway

- Terminación de la llamada desde la PSTN.
- Codificación y paquetización de la voz.
- Terminación de la señalización PRI.
- *Call Control* (control de llamada) básico.

Podemos distinguir entre dos tipos diferentes de Media Gateways:

- *Public Access Gateway* (AG): proporciona un interfaz para accesos analógicos tradicionales o digitales hacia la red VoIP. Se trata de un gateway para VoIP de pequeña escala.
- *Trunking Gateway* (TG): es el interfaz entre la red telefónica y la red VoIP. Estos gateways suelen manejar un gran número de circuitos digitales.

Signalling Gateway

- Interfaz entre la Red de Datos y la de Señalización nº 7.
- Grabación de los aspectos de la llamada para tarificación.
- Funcionalidad de Call Control.
- Chequeo de la continuidad de la llamada.

Media Gateway Controller

- Implementa la principal funcionalidad de Call Control.
- Gestiona los Media Gateways.
- Realiza las funciones AAA (Authorisation, Authentication and Accounting).
- Puede funcionar como Gatekeeper H.323.
- Realiza la traducción de números.

5.2 Introducción a los Protocolos de VoIP

Introducción a la Sección 5.2

Vas a comenzar el apartado 5.2:

Visión General de los Protocolos de VoIP



En general, en toda arquitectura de protocolos distinguimos entre el plano de datos (o los protocolos que se encargan de transportar los datos de los usuarios) y el plano de control (o los protocolos que se encargan de realizar distintas funciones de control necesarias para dicho transporte de los datos, como por ejemplo: establecimiento de camino virtual o llamada, comprobación de errores, control de flujo, etc...)

El caso de VoIP no iba a ser menos, y así, podemos clasificar los diferentes protocolos en cada uno de los planos de usuario o datos y de control, definidos cada uno en el presente contexto de la siguiente forma.

El **plano de Datos** nos muestra cómo transportar información de tiempo real a través de una red no orientada a conexión, ofreciendo calidad de servicio (QoS) y evitando la pérdida de paquetes. Resumiendo, los protocolos encargados de transportar la voz dentro de los paquetes de datos.

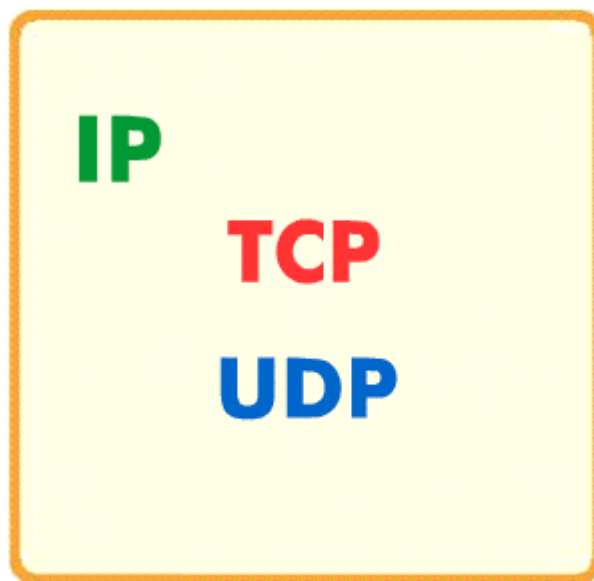
¿Qué protocolos de los que estudiaremos realizan esta función? Pues la lista sería la siguiente: RTP (RTCP), MPLS, DiffServ, RSVP, G7xx, H.26x, ...

El **plano de Control** en un principio se encargaría de funciones como el establecimiento de llamada y su liberación. Pero, al contrario que en las redes de conmutación de circuitos, las redes IP no necesitan establecer un camino en la red, ya que la conectividad es proporcionada por el propio protocolo IP.



El plano de control no se usa aquí para controlar el canal de transporte, sino que se usa para hacer asociaciones (lógicas) entre endpoints de VoIP. Una vez establecidas estas asociaciones, el plano de control será fundamentalmente el responsable del transporte de señalización y de información de control. ¿Qué protocolos veremos que asuman estas funciones? Pues, principalmente: MGCP, MEGACO, H248, H323 (H225, H245), SIP, (SS7, Q931), (SIGTRAN).

UDP vs TCP: El dilema continuidad-fiabilidad



Bueno, pues llegado a este punto sería recomendable que recordáramos algunas de las características de los protocolos principales utilizados en las redes IP:

IP, TCP y UDP, ya que con ellos son con los que van a tener que trabajar los protocolos de VoIP.

El protocolo utilizado en las redes IP para transportar los datagramas o paquetes de datos (precisamente es el protocolo IP, Internet Protocol) no es fiable.

Corresponde al protocolo de transporte de la capa superior asegurar el control de la transmisión.

En Internet, ésta función es asumida por TCP, Transport Control Protocol. TCP es, pues, un protocolo fiable, que corrige los errores del protocolo subyacente.

Para lograrlo, en TCP se envían confirmaciones a la fuente en la recepción de los paquetes, y cuando un paquete no es confirmado, se reenvía dicho paquete.

Desafortunadamente, este mecanismo es incompatible con las restricciones de tiempo real.

La recuperación de los paquetes perdidos multiplica, al menos por tres, el tiempo de tránsito, ya que se envía un primer paquete, la fuente espera una confirmación que no llega, y se acaba enviando un segundo paquete que reemplaza al primero.

Así, la pérdida repetida de un solo paquete puede producir demoras importantes. Pero el audio y el vídeo tienen velocidades constantes que no pueden variar y fluctuar, so pena de provocar rupturas de cadencia.

TCP no será pues muy útil más allá del 4 o 5% de pérdida de paquetes. A este nivel, la aplicación del destinatario rectificará ella misma la señal, reemplazando por ejemplo los agujeros por paquetes adyacentes.

No hay otra elección que abandonar los paquetes perdidos, para conservar la continuidad del flujo.



El tiempo real, como el espectáculo, debe proseguir.

El intérprete de una pieza musical no puede interrumpirse en medio de su interpretación para rectificar una falsa nota o volver a un pasaje.

Llevado por el metrónomo y el respeto hacia su auditorio, pasará por encima de sus errores para conservar el tempo y el aire de su obra.

Por lo tanto, en lugar de TCP, se utilizará UDP, que se trata del protocolo de Nivel 4 de la arquitectura de protocolos IP que, al igual que IP, no es fiable y no pide reenvío de los paquetes perdidos.

UDP, User Datagram Protocol, es extremadamente simple. Su función principal es servir de envoltorio de transporte a la capa de nivel 3.

Sólo sirve para “envolver” los paquetes IP, introduciendo un campo de número de “puerto”, vía lógica que servirá para orientar el paquete dentro de la aplicación. La noción de “puerto” sólo afecta a la capa de aplicación.

UDP se utilizará típicamente como protocolo subyacente a RTP.

El Real Time Transport Protocol, contrariamente a lo que su nombre indica, debe basarse en un protocolo de transporte como UDP, que en este caso no es fiable.



La necesidad de herramientas complementarias

Pero esto no acaba en la mera elección del protocolo de nivel de transporte más adecuado. Para hacer frente a sus nuevas obligaciones de tiempo real, la red IP tiene que dotarse, además, de herramientas más potentes.

¿Cuáles son estas herramientas? Pues las que te listamos a continuación.

El Multipunto

La red informática está naturalmente dotada para la difusión de una misma información hacia varios destinos simultáneamente. La participación de 100 personas en una audioconferencia por la red telefónica exigiría la apertura de 100 circuitos dedicados, conectados a un conmutador que centraliza y mezcla las señales.

En Internet resulta más simple. Una máquina centraliza los paquetes de todos los contribuyentes y los redistribuye hacia sus destinatarios.

Pero esta aptitud natural se utiliza muy mal. Un direccionamiento multipunto permitiría a una fuente emitir un solo paquete acompañado de una lista de difusión, y la red se encargaría de duplicarlo en los nodos situados en los cruces de los enlaces.

Desafortunadamente, sólo algunas máquinas aceptan este tipo de direcciones, y se comunican entre sí para formar la subred MBONE.

La Resincronización

El transporte de paquetes en una red no determinista no garantiza los retrasos. El receptor debe pues restaurar previamente la sincronización del flujo. Las cabeceras IP, UDP o incluso TCP no fechan los paquetes; no proporcionan el fechado que facilitaría la resincronización del flujo.

Gestionar las Conexiones

Las congestiones son debidas a la saturación de los nodos y los enlaces de la red y son la causa principal de las pérdidas de información y de los retrasos de encaminamiento. A nivel de recursos constante, sólo hay un medio de evitar las congestiones, y es reducir la velocidad de emisión. Esta disciplina supone que las fuentes conocen, en tiempo real, el estado de la red.

Un sistema de confirmación de recepción de paquetes como el de TCP ya hemos visto que no es adecuado, porque una transmisión en tiempo real no puede ser fiable. Su única estrategia es abandonar los paquetes perdidos para preservar la continuidad del servicio. Es necesario, pues, implementar un intercambio de informes de recepción, con los que los destinatarios informan a la fuente del nivel de calidad de servicio constatado.



Estos retornos de información existen para todos los medios, radios de onda corta o cadenas de televisión y permiten al emisor conocer la eficacia de la transmisión.

En el caso de Internet, este feedback servirá para que el difusor de medios por Internet disminuya su velocidad de emisión, de manera que descongestione la red. Este ajuste pasará por utilizar una tasa de compresión más elevada, o una frecuencia de refresco de vídeo más baja, a costa de un empobrecimiento de la calidad de la información.

Prioridad a los Flujos Multimedia

La consulta de las páginas Web o un diálogo vocal con un interlocutor no responden a los mismos criterios. Sin embargo, la red trata estos dos servicios con igualdad, de la misma manera, ya que en IP no existen prioridades de un tipo de tráfico sobre otro. Es indispensable, pues, jerarquizar los flujos según sus imperativos de tiempo, y hacer que la red gestione niveles de prioridad.

Esta gestión diferenciada puede ser:

- **Automática:** La red accede a todas las peticiones de prioridad, si se trata de un flujo en tiempo real. Este servicio sería pues gratuito e integrado básicamente en todos los protocolos (*DiffServ*).
- **A la carta:** En este caso, un receptor desea disponer de una calidad de servicio mejorada. Compra en la red los recursos que le garantizarán la prioridad y la calidad deseadas (*IntServ*).

5.3 RTP (Real-Time Transport Protocol)

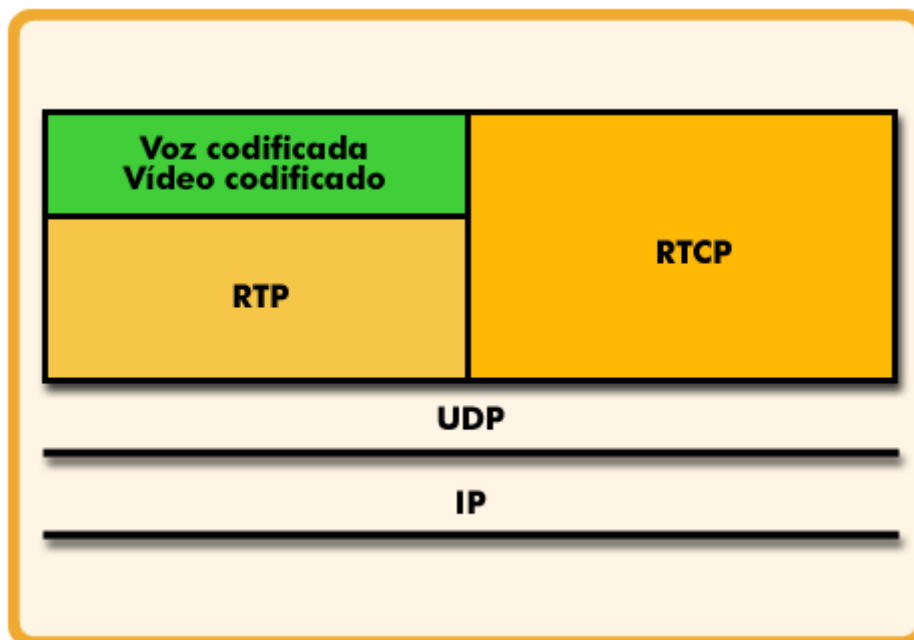
Introducción a la Sección 5.3

Vas a comenzar el apartado 5.3:

¿Qué hace RTP?

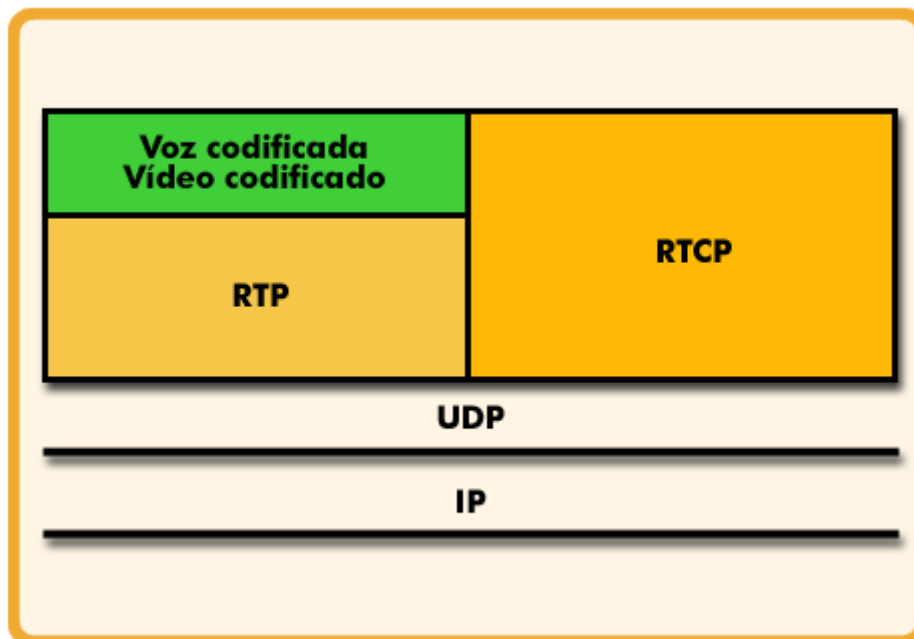
Básicamente, RTP es un protocolo de transporte y de control adoptado por las aplicaciones que presentan propiedades de tiempo real.

Ofrece los medios necesarios para:



- Reconstruir la base de tiempo de los flujos de datos de audio, vídeo y tiempo real en general.
- Detectar rápidamente las pérdidas de paquetes e informar a la fuente en los lapsos compatibles con el servicio.
- Identificar el contenido de los datos y permitir su transmisión segura.

El feedback RTCP



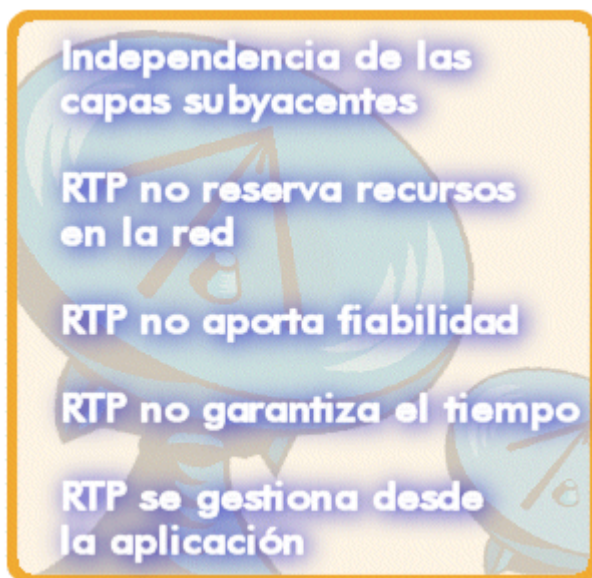
El protocolo de transporte de datos RTP va acompañado de un segundo protocolo que asegura el tráfico de control, RTCP (Real-Time Transport Control Protocol).

Éste envía al emisor un feedback sobre la calidad de la transmisión, así como otras informaciones útiles.

Por ejemplo, en el caso de conferencias de audio o vídeo que agrupan a un número importante de participantes, RTCP identifica las diferentes fuentes de emisión, integra soluciones para atravesar pasarelas de ciertas redes locales (firewalls), o asegura, llegado el caso, la conversión de direccionamiento multipunto a monopunto.

RTP puede utilizarse sin RTCP.

Características Principales



Las principales características que posee RTP son las que ves en la imagen.

Independencia de las capas subyacentes

RTP es independiente del protocolo de transporte subyacente y de las redes utilizadas.

Generalmente, se empleará sobre UDP, pero también existen implementaciones sobre CLNP, IPX u otros protocolos. Las capas inferiores que aseguran la fiabilidad o garantizan la calidad de servicio pueden encaminar aplicaciones RTP. Las experiencias de utilización de RTP se han llevado con éxito a las redes ATM (AAL5).

RTP no reserva recursos en la red

No se emprende ninguna acción sobre los encaminadores e intermediarios y no se controla la calidad de servicio.

Funciona de punto a punto y se completará con ventaja con cualquier protocolo de reserva de recursos, como RSVP, o con cualquier otro método de priorización del tráfico de tiempo real.

RTP no aporta fiabilidad

RTP sólo ofrece algunas características de un protocolo de transporte. En relación a TCP, no procura la fiabilidad de la transmisión y no garantiza la entrega de paquetes perdidos.

RTP no aporta control predefinido del flujo o de la congestión de la red. Por el contrario, proporciona a la aplicación los elementos de información que le permitirán contribuir a la fiabilidad y al control de flujos y red. No hay que añadir nada a la cabecera RTP; ya contiene toda la información útil, número de secuencia y fechado. La sincronización del sonido y el vídeo de un flujo en relación con otro, es posible por medio de los índices y guías transmitidos por RTP.



RTP no garantiza el tiempo de entrega: ningún protocolo de punto a punto puede garantizar el tiempo de entrega. Para garantizarlo, habría que basarse en capas más bajas del modelo OSI de referencia y controlar directamente los recursos a nivel de conmutadores y encaminadores.

La aportación de RTP a los intercambios en tiempo real es muy relevante. Proporciona información muy útil para el transporte de contenidos. Asegura el fechado de los paquetes, añadiendo un apunte de tiempo que indica la hora de su creación; su ordenación por parte del destinatario se ve así simplificada. Se proporcionan mecanismos de recuperación y de sincronización de flujos diferentes; cada paquete se reconoce como perteneciente a un flujo concreto.

RTP se gestiona desde la aplicación

Por el contrario, TCP es un protocolo de transporte completo.

En el caso de RTP, no se da la implementación de un kernel o de librerías.

5.4 Vista Previa del Plano de Control

Introducción a la Sección 5.4

Vas a comenzar el apartado 5.4:

El Plano de Control



Recordamos que, al contrario que en las redes de conmutación de circuitos, las redes IP no necesitan establecer un camino en la red, ya que la conectividad es proporcionada por el propio protocolo IP.

El plano de control no se usa aquí, por lo tanto, para controlar el canal de transporte, sino que se usa para hacer asociaciones (lógicas) entre endpoints de VoIP. Una vez establecidas estas asociaciones, el plano de Control será el responsable del **transporte de señalización y de información de control**.

Así pues, para proporcionar telefonía IP básica, podemos distinguir tres pasos.

Señalización de la llamada (Call signalling)

Equivale al establecimiento de conexión en las redes de conmutación de circuitos. Aunque no haya conexiones físicas establecidas entre llamante y llamado, se hace necesaria una asociación entre ellos.

El direccionamiento y la localización de los usuarios son aspectos que hay que resolver. Por ejemplo, ¿qué esquema de direccionamiento se usará? ¿Es necesaria una traducción entre números telefónicos y direcciones IP?

Control de la llamada (Call Control)

Equivale a la fase de negociación en las redes de conmutación de circuitos.



Una vez localizado el llamado, hay que negociar ciertos aspectos, como son las capacidades, el control del ancho de banda, el tipo de codec, etc.

Transferencia de los datos

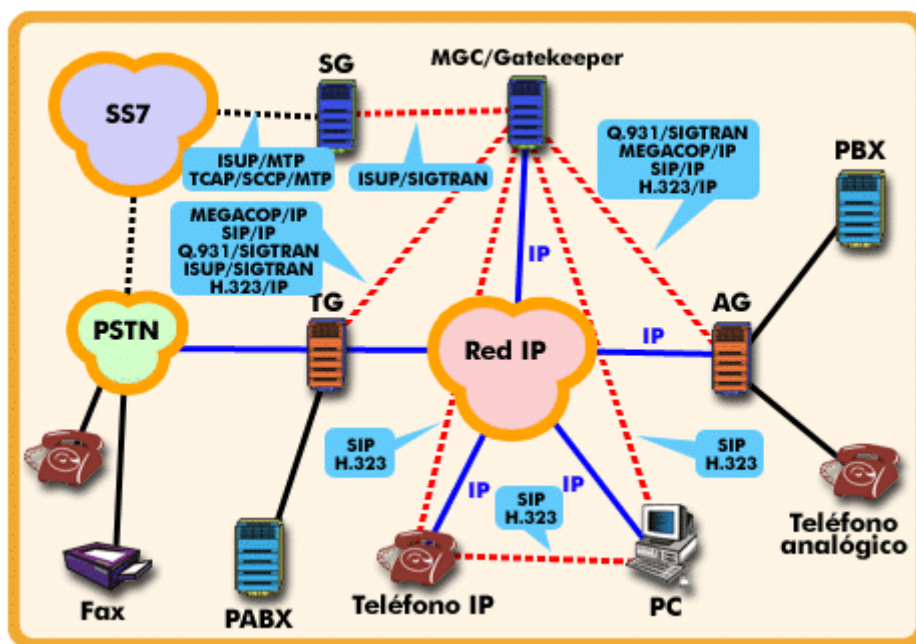
Después de la negociación, comienza la transferencia de los datos usando los parámetros negociados previamente: velocidad de muestreo, compresión, etc.

La ejecución de alguno de estos pasos requerirá el uso de "agentes intermediarios".

Protocolos de Señalización

Bueno, pues a la vista del esquema mostrado en la figura, en VoIP se han propuesto varios protocolos de señalización (H.323, SIP y SIGTRAN) y uno de control (MEGACOP).

Así por encima, sus características son las siguientes:



- Estándar de señalización H.323

H.323 fue el primer estándar adoptado por la comunidad de VoIP.

Este estándar de ITU-T define tres componentes básicos para un sistema de comunicación:

- Terminales H.323

Cualquier endpoint de red que pueda comunicarse con cualquier otro endpoint, sea éste otro terminal H.323 o un gateway (GW).

- Gateways (GW)

Equipos similares a los Media Gateways del modelo IETF.

- Gatekeeper (GK)

Equipos con la funcionalidad del Media Gateway Controller de IETF.

Más que un protocolo, se trata de un estándar "paraguas" bajo el que se han agrupado una serie de protocolos conocidos, adaptados para la señalización entre cualquier endpoint (terminal o gateway) y el GateKeeper.



- Protocolo de Señalización SIP

El protocolo SIP (Session Initiation Protocol) es un estándar más reciente desarrollado por el IETF (Internet Engineering Task Force).

Se trata de un protocolo que sigue el modelo cliente-servidor, similar a http, no tan complejo como H.323.

- Protocolo de Control **MEGACOP**

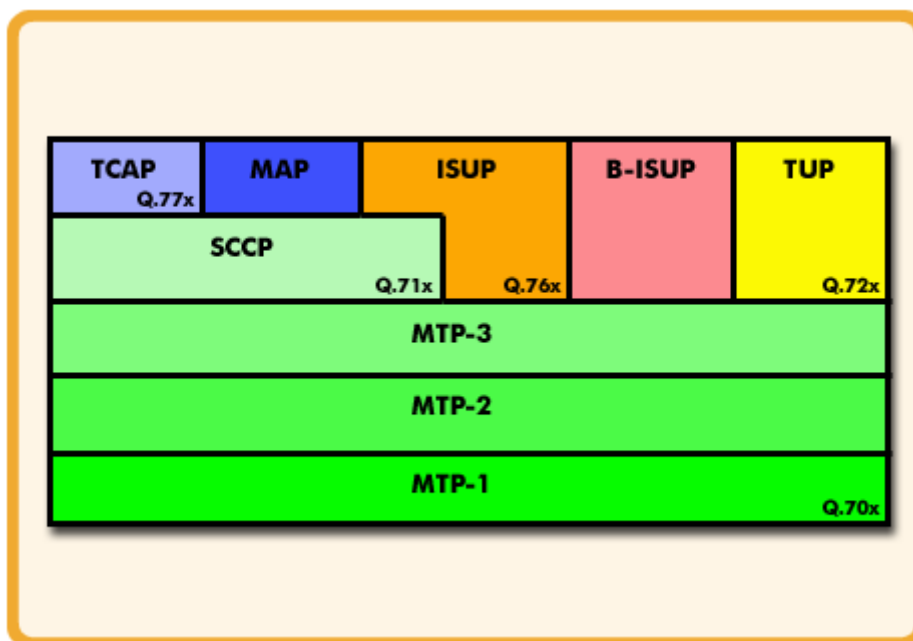
MEGACOP (Media Gateway Control Protocol) es un protocolo de control entre el MGC y los MGs, desarrollado por Bellcore y Level3 fruto de la combinación del protocolo SGCP, de Bellcore, y el protocolo IPDC, de una serie de compañías (Level3, Alcatel Nortel, Cisco, Lucent, Ericsson, ...).

MEGACOP es un protocolo patrocinado por IETF que tiene en **H.248** su equivalente en ITU.

- Protocolo de transporte de señalización SIGTRAN

SIGTRAN (SIGNalling TRANsport) es un estándar IETF de un protocolo para el transporte confiable y transparente de la señalización de las redes de conmutación de circuitos a través de redes IP.

Arquitectura de Protocolos SS7



Que no se nos olvide que una de las principales funciones de los protocolos del plano de control es transportar la señalización de la red telefónica a través de redes IP.

Pero, ¿recordamos cuál es dicha señalización? Pues entonces, un breve repaso no nos vendrá mal. La especificación SS7, responsabilidad del CCITT, propone una arquitectura en capas que se corresponde, con bastante aproximación, a la propuesta por el modelo OSI. Una breve descripción de los protocolos implicados es la de la imagen.

TCAP (*Transaction Capabilities Application Part*)

Permite el despliegue de servicios avanzados de redes inteligentes por medio del intercambio de información, no orientada a circuito, entre puntos de señalización (SP) utilizando el servicio SCCP no orientado a conexión.

MAP (*Mobile Application Part*)

Agrupar los mensajes que se envían entre nodos de conmutación de telefonía móvil y las bases de datos que soportan la autenticación de usuarios, identificación de equipos e información de "roaming".

ISUP (*ISDN UserPart*)

ISUP define el protocolo y los procedimientos usados para establecer, gestionar y liberar circuitos conmutados que llevan llamadas de voz y datos sobre la red pública telefónica conmutada.

ISUP se utiliza en ambos tipos de llamadas, RDSI y no RDSI. Aquellas llamadas que se originan y terminan en el mismo nodo de conmutación no utilizan ISUP.



SCCP (*Signalling Connection Control Part*)

Ofrece mejoras al nivel 3 de MTP para proporcionar servicios de red orientados y no orientados a conexión, así como capacidades de traducción de direcciones.

Las mejoras de SCCP con respecto a MTP proporcionan un servicio de red equivalente al nivel 3 de Red de OSI.

MTP3 (*Message Transfer Part – Level 3*)

Transfiere mensajes entre los nodos de la red de señalización.

MTP3 asegura un transporte fiable de los mensajes de señalización, incluso en el caso de fallos en los enlaces de señalización o en los STPs.

MTP2 (*Message Transfer Part – Level 2*)

Se trata de un enlace de señalización que, junto con MTP3, ofrece un transporte fiable de los mensajes de señalización entre dos puntos de señalización conectados directamente.

5.5 Protocolo MEGACOP (Media Gateway Control Protocol)

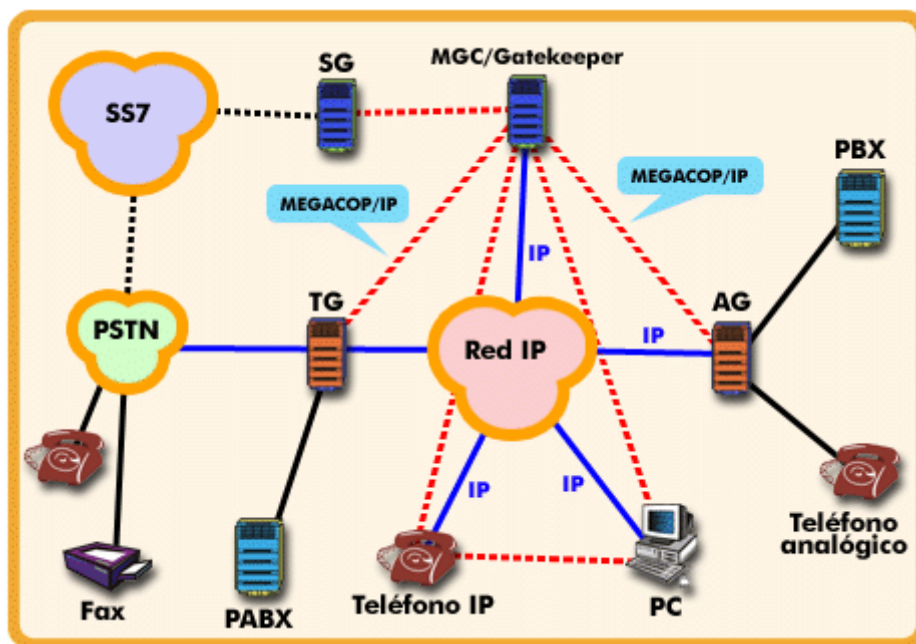
Introducción a la Sección 5.5

Vas a comenzar el apartado 5.5:

Descripción

¿Comenzamos viendo los distintos protocolos enunciados en mayor profundidad?
No sería mala idea, ¿verdad?

Podríamos empezar por MEGACOP...



MEGACOP es un protocolo, patrocinado por IETF, utilizado por el Media Gateway Controller (MGC) para el control de los Media Gateways (MGs).

El protocolo indica a los GWs, desde el MGC, que envíen y reciban flujo de información hacia/desde direcciones específicas, que generen tonos y que modifiquen su configuración.

También permite el envío de informes desde los GWs hacia el MGC, sobre eventos detectados como, por ejemplo, detección de dígitos DTMF y tonos.

En definitiva, MEGACOP permite que la función de call control sea implementada por dispositivos externos a los propios gateways, los Media Gateway Controller.

MEGACOP es un protocolo que funciona sobre la capa de transporte UDP, no fiable, y que tiene su equivalente ITU en el protocolo H.248.

Funciones de MEGACOP



Gestión limitada del MG desde el MGC

El MG puede notificar sus re-arranques al MGC. Con ello:

- MGC puede auditar el estado de los endpoints y de las conexiones.
- Se están investigando, además, capacidades adicionales de gestión.

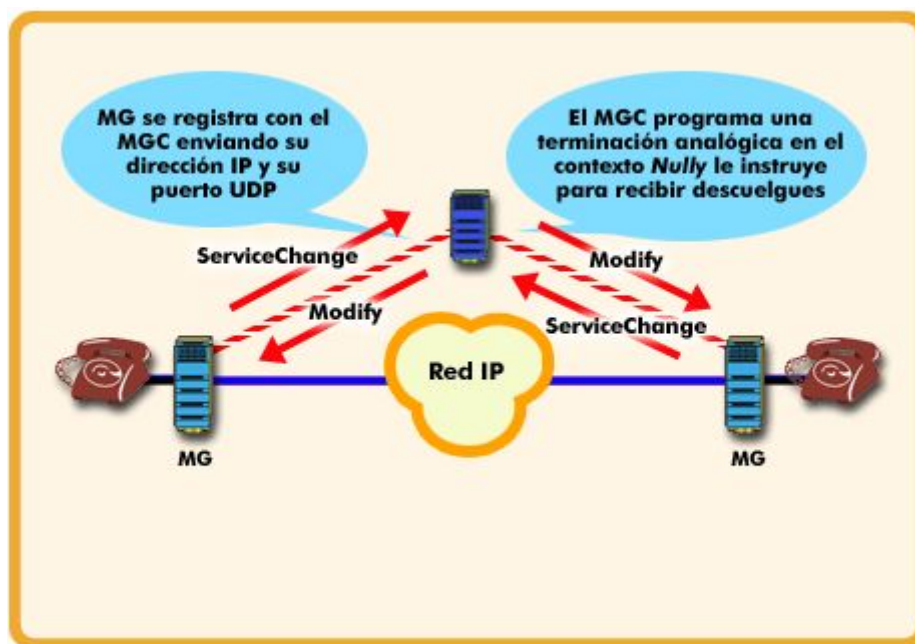
Control de la Conexión:

- Establecimiento, modificación y liberación de las conexiones entre la red de conmutación de circuitos y la red IP.
- Especificación de los endpoints de una conexión: una línea en la red de conmutación de circuitos, un circuito en un trunk, dirección IP y puerto RTP en una red IP.
- Especificación de los atributos de una conexión: codificador, supresión de silencios, encriptación, cancelación de eco, etc.

Interworking con la señalización en banda de la red de conmutación de circuitos: esto es necesario para poder responder a eventos como cuelgues/descuelgues, corriente de llamada, tono de invitación a marcar, tono de ocupado, etc.

- Eventos desde la red de conmutación de circuitos: el MGC pide al MG que explore en endpoints específicos a la búsqueda de algunos eventos (por ejemplo, el descuelgue) y que le informe de ellos.
- Eventos salientes hacia la red de conmutación de circuitos: el MGC pide al MG que genere eventos hacia un determinado endpoint (por ejemplo, corriente de llamada).

Escenario de llamada con MEGACOP



Vamos a estudiar el proceso de la llamada desde un usuario analógico a otro, atravesando una red IP y utilizando MEGACOP como protocolo de señalización.

La primera fase será registrar el Media Gateway en su Media Gateway Controller específico:

1. Cuando cualquier Media Gateway (MG) ha terminado su inicialización, se registra en el MGC mediante el comando ServiceChange, que incluirá como parámetros la dirección IP del MG y el puerto UDP sobre el que funciona MEGACOP en el MG.

Con estos dos parámetros, el MGC está en condiciones de comunicar con el MG cuando lo desee.

2. El MGC programa, mediante el comando Modify, una terminación analógica (lado de la red de conmutación de circuitos del MG) en el contexto NULL (éste es un tipo especial de contexto que contiene una terminación que no está asociada con ninguna otra) y le pide que se prepare para detectar posibles descuelgues.

Una vez registrados nuestros Gateways, veamos cómo transcurre el establecimiento de llamada:

1. El MG1, previamente registrado, recibe el evento de descuelgue desde el lado de la red de conmutación de circuitos.
2. El MG1 detecta el descuelgue en la terminación y se lo comunica al MGC mediante el comando Notify.
3. El MGC modifica los eventos que tienen que esperar la terminación en el MG: búsqueda de dígitos y de un posible cuelgue.
4. El usuario envía los dígitos de marcación.



5. Los dígitos son almacenados en el MG y cuando el DialPlan está satisfecho, se le comunican al MGC mediante el comando Notify.
6. El MGC analiza los dígitos y determina que hay que establecer una conexión con el MG2. Mediante el comando Add, el MGC informa al MG de que añada, a la Terminación TDM, una nueva Terminación RTP dentro del mismo nuevo contexto. El comando incluye parámetros que especifican los valores preferidos para el codec.
7. Con el reconocimiento, desde el MG1, se envían: la dirección IP de MG1 y el puerto UDP seleccionado, así como el codec elegido.
8. Mediante el comando Add, se le ordena al MG2 que añada una terminación idle en un nuevo contexto. Además, se le comunican los valores preferidos para el flujo RTP.
9. Con el reconocimiento, desde el MG2, se envían: la dirección IP de MG2 y el puerto UDP seleccionado.
10. Mediante el comando Modify se le envía al MG1: la dirección IP del MG2, el puerto UDP en MG2, la orden de generación de tono de llamada hacia el abonado.
11. Con el comando Modify se le ordena al MG2 que envíe al abonado 2 la corriente de llamada. Desde este momento los dos MGs están conectados y los usuarios están recibiendo los tonos correctos. Además MG2 está esperando detectar un descuelgue.
12. MG2 detecta el descuelgue.
13. El descuelgue es reportado al MGC mediante el comando Notify.
14. Se quitan los tonos en ambos usuarios y se le ordena al MG2 que busque eventos de "cuelgue".
15. La conversación tiene lugar.

5.6 El estándar H.323

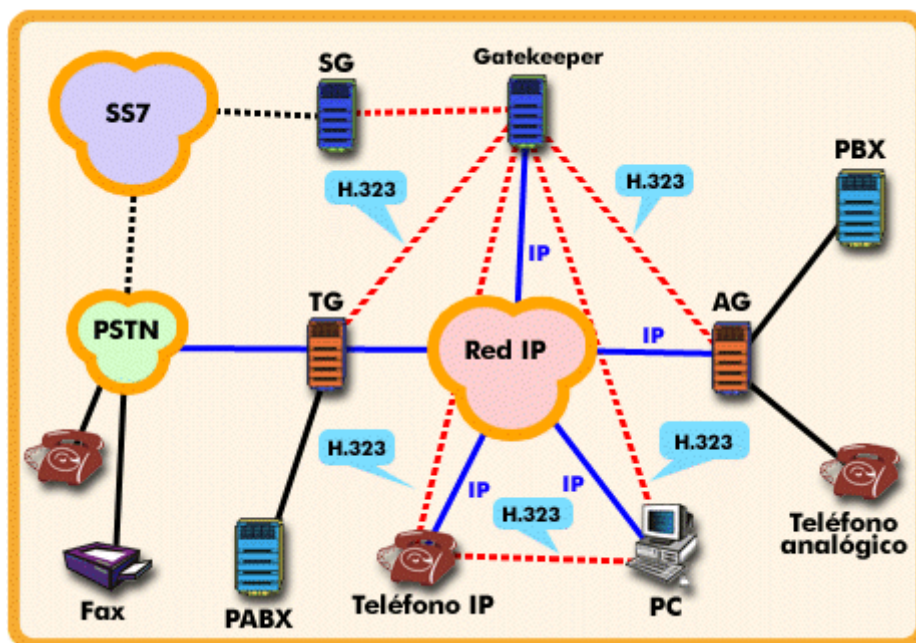
Introducción a la Sección 5.6

Vas a comenzar el apartado 5.6:

Descripción de H.323

¿Qué se esconde tras dicha especificación?

El estándar H.323 de ITU-T, Equipos y Sistemas de Telefonía Videotelefonía para redes de Área Local sin garantía de Calidad de Servicio (QoS), es una recomendación que define los componentes, procedimientos y protocolos para proporcionar comunicaciones audiovisuales entre LANs.



H.323 puede usarse en cualquier red de conmutación de paquetes, cualquiera que sea el nivel físico implementado. En los niveles altos, puede utilizarse IP junto con los protocolos de transporte TCP (fiable) o UDP (no fiable).

H.323 también incluye los protocolos RTP y RTCP, de IETF, extensiones para señalización de llamada y algoritmos adicionales para la codificación de audio y vídeo.

H.323 es independiente de la topología de red, por lo que los terminales H.323 pueden comunicarse entre sí a través de LANs (vía hubs, LAN switches, etc) de Internets locales o remotas (vía routers, bridges, etc) o a través de accesos por marcación (dial-up).

Por ello, los proponentes ven, como "aplicación más atractiva" de esta recomendación, la videotelefonía sobre Internet.

Elementos de la Arquitectura H.323



En la Arquitectura de H.323 encontramos tres componentes fundamentales.

Terminales

Los terminales H.323 son los endpoints clientes en la LAN que proporcionan comunicaciones full-duplex en tiempo real. Todos los terminales deben soportar comunicaciones de voz, mientras que las de vídeo y de datos son opcionales.

Así mismo, los terminales H.323 deben soportar el protocolo de control para comunicaciones multimedia H.245. Los terminales H.323 deben implementar la recomendación H.225.0.

Gateways

El Gateway es un elemento opcional en un modelo de red H.323. Desde el punto de vista de H.323 es un terminal más, ya que dentro de la LAN, se comunica con otros terminales. Un Gateway H.323 proporciona una amplia variedad de servicios. El más común es una traducción entre terminales H.323 y otros tipos de terminales. Dicha traducción incluye:

- Cambios en formatos de transmisión, de H.225.0 (RTP) a H.221 (RDSI) y viceversa.
- Cambios en procedimientos de comunicación (señalización de control), de H.245 (H.323) a H.242 (RDSI).

El Gateway también realiza el establecimiento y la liberación de la llamada en ambos lados, en el de la LAN y en el de la Red de Conmutación de Circuitos.

En general, podemos decir que el propósito de un Gateway H.323 es reflejar las características de un endpoint de la LAN a un endpoint de la Red de Conmutación de Circuitos, y viceversa.

Los Gateways no son necesarios si no se necesitan conexiones a otras redes, ya que los terminales H.323 pueden, en este caso, comunicarse con otros terminales en la misma LAN.

Gatekeepers: un Gatekeeper (GK) es el componente fundamental de una red H.323. Funciona como el punto central de todas las llamadas dentro de su zona y proporciona servicios de "call control" a endpoints previamente registrados en el propio Gatekeeper. En muchos sentidos, un Gatekeeper H.323 funciona como un conmutador virtual.

El conjunto de terminales, Gateways y Multipoint Control Units gestionados por un solo Gatekeeper se conoce como zona H.323. No es obligatorio instalar un Gatekeeper en cada sistema H.323. Sin embargo, si está presente, los terminales deben usar los servicios ofrecidos por él. RAS (un protocolo de señalización que veremos dentro de un rato) define estos servicios como: Traducción de Direcciones, Control de Admisiones, Control del Ancho de Banda y Gestión de Zona.



Funciones Obligatorias y Opcionales en un Gatekeeper H.323

Atendiéndonos a su obligatoriedad u opcionalidad, podemos clasificar las funciones de un Gatekeeper definido según la norma H.323 en:

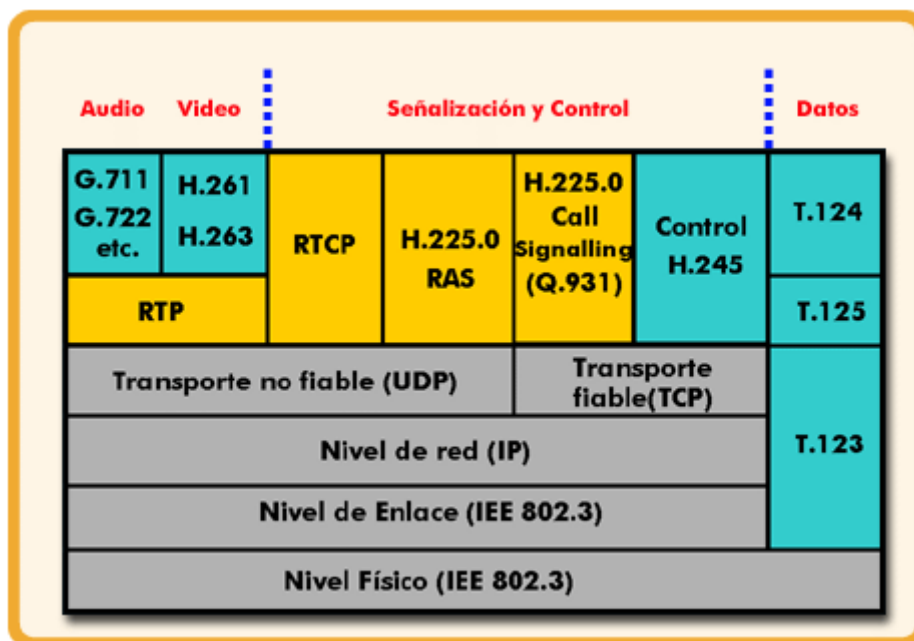
Funciones obligatorias

- **Traducción de direcciones** de los alias de LAN con que se conocen los Terminales y Gateways H.323 desde fuera de la LAN a direcciones IP, como se define en la especificación RAS
- **Gestión del ancho de banda**, también especificada por RAS. Por ejemplo, si un gestor de red ha especificado un umbral para el número máximo de conferencias simultáneas en la LAN, el Gatekeeper puede rechazar nuevos intentos de conexión una vez que se ha sobrepasado el umbral.
- **Control de Admisión**: consiste en la autorización del acceso a la LAN usando los mensajes AdmissionRequest, Confirm y Reject (ARQ/ARC/ARJ). Los accesos a la LAN pueden estar basados en autorización, ancho de banda o cualquier otro criterio.
- **Gestión de Zona**: un Gatekeeper proporciona las funciones anteriormente mencionadas para terminales, MCUs y Gateways que se han registrado en su zona de control.

Funciones opcionales

Enrutamiento de llamadas H.323. Se trata de una opción interesante para los proveedores de servicios, para que puedan facturar por las llamadas que se atraviesan en su red. Además, una llamada podría ser enrutada hacia otro endpoint si el endpoint llado no está disponible.

Arquitectura de Protocolos H.323



Ahora te voy a dar una sorpresa, en realidad, la arquitectura de protocolos H.323 no es un único protocolo, sino que está formado por un variado número de conocidos estándares.

Codificadores de audio y vídeo

- Codificadores de audio: sólo es obligatorio soportar G.711 (PCM); G.722, G.728, G.723.1 y G.729 son opcionales.
- Codificadores de vídeo: sólo H.261 QCIF es obligatorio; H.261 CIF y H.263 son opcionales.

Aplicaciones de datos

- Recomendaciones de la serie T.120.

RTP/RTCP

La recomendación H.323 hace uso del protocolo RTP/RTCP (que ya hemos visto anteriormente, ¿recuerdas?) para la paquetización de datos.

H.225.0 RAS (*Registration/Admission/Status*): protocolo de señalización entre el Terminal y el Gatekeeper. Se utiliza para registros y solicitudes de ancho de banda y de recursos. Funciona sobre una capa de transporte no fiable (UDP, por ejemplo).

- Registration: proceso por el que un endpoint entra a formar parte de una Zona.
- Admission: proceso por el que un endpoint verifica si el Gatekeeper le autoriza a acceder a la red de paquetes. Su solicitud puede ser rechazada si, por ejemplo, solicita un ancho de banda mayor del disponible en esos instantes, o si no está al día en los pagos, ...
- Status: proceso por el que un Gatekeeper determina si un endpoint está apagado o ha entrado en fallo.



H.225.0 Call Signalling

Protocolo de señalización para el establecimiento/liberación de los canales, petición de cambios en el ancho de banda de los canales, obtención del status de los endpoints en la llamada.

Los mensajes son los mismos que los del protocolo de señalización Q.931 (ISDN). Funciona sobre una capa de transporte fiable (TCP, por ejemplo).

Control H.245.

Protocolo de Control para comunicaciones multimedia **H.245**: se trata de un protocolo para la negociación y la determinación de las capacidades de los canales lógicos:

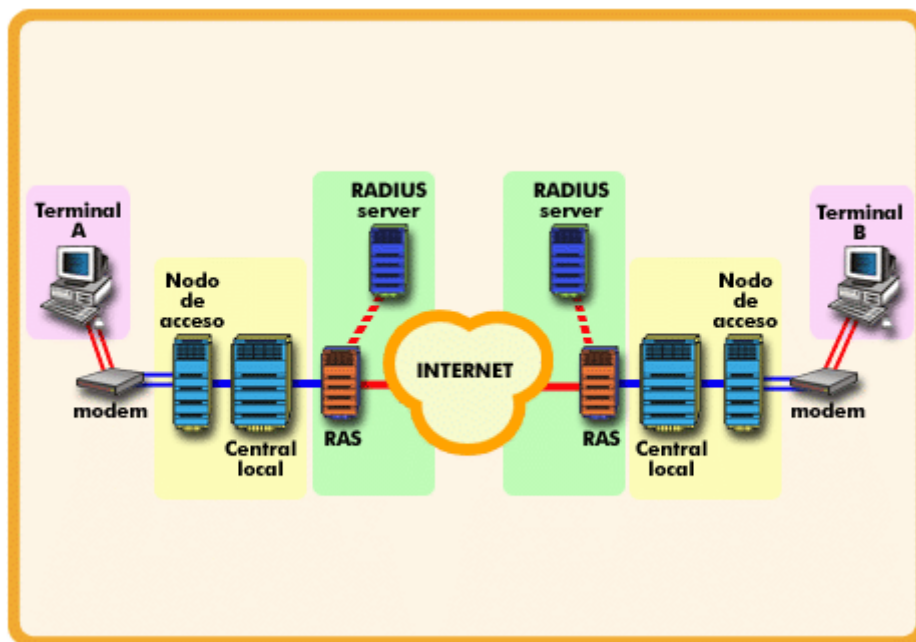
- quién es el maestro y quién el esclavo en la comunicación entre dos terminales,
- establecimiento del tipo de señales multimedia que entienden ambos terminales, para asegurar que, en adelante, todos los tipos de señales multimedia que van a transmitirse son entendidos por ambos terminales (intercambio de capacidades),
- señalización para la apertura y cierre de los canales lógicos que transportan la información audiovisual o de datos.

H.245 es un protocolo independiente del mecanismo de transporte elegido, aunque éste debe ser fiable, es decir, que proporcione garantía de la entrega de los datos.

Escenario de Llamada Básica sin Gatekeepers en H.323

Veamos dos ejemplos de escenarios de llamada posibles con este estándar. Por ejemplo, en el escenario contemplado, ningún endpoint está registrado a un Gatekeeper.

Por lo tanto, éste es el escenario en el que el terminal llamante conoce la dirección IP del llamado, y no necesita que nadie le traduzca ningún número de teléfono a dirección IP, con lo que los dos se comunican directamente entre ellos.



El establecimiento de la llamada, para este caso, tiene lugar en tres fases:

- Señalización H.225.0 (Q931) para el establecimiento del canal de control.
- Negociación de las capacidades por el canal de control (H.245).
- Flujo de información RTP/UDP.

Para comprenderlo mejor, podemos ver el proceso paso a paso:

1. El Terminal A envía un mensaje de Setup al Terminal B.
2. El Terminal B responde con un Call Proceeding para informar al Terminal A de que su llamada ha comenzado a procesarse.
3. El Terminal B responde con un mensaje Alerting para indicarle al Terminal A que el usuario llamado ha sido avisado.

En caso de cursar la llamada a través de un Gateway hacia una Red de Conmutación de Circuitos, el mensaje Alerting debe ser enviado por el Gateway cuando éste reciba la indicación de corriente de llamada desde la Red de Conmutación de Circuitos.

4. El Terminal B envía al Terminal A el mensaje Connect para indicarle que la conexión ha sido establecida.

Acompañando al mensaje, se le comunica también la Dirección de Transporte (el puerto TCP) del Canal de Control H.245, con lo que queda establecido el canal de control para su posterior uso en la fase de señalización H.245.

5. Sobre el canal de control establecido, tiene lugar la fase B de intercambio de capacidades y establecimiento del canal sobre el que tendrá lugar el flujo de datos RTP (señalización H.245).

6. Los canales de transporte de datos RTP han sido establecidos y la llamada ha sido completada con éxito.



Llamadas PC-a-teléfono

Este escenario, por el contrario, contempla la utilización de un Gatekeeper para el control del Gateway de la red IP con la red telefónica. Se supone que ambos endpoints se encuentran registrados en el mismo *Gatekeeper*. Evidentemente, el proceso paso a paso es bastante diferente del caso anterior.

- **El Terminal A desea llamar al teléfono de la figura.**

1. Antes de iniciar el procedimiento de establecimiento del canal por el que fluirá la señalización H.245, mediante mensajes H.225.0 (Q.931), el Terminal A debe ejecutar un **proceso de Admisión** con su *Gatekeeper*, mediante mensajes H.225.0 RAS.

2. Cuando finalice el proceso de Admisión (con el mensaje *ACF*), el Gatekeeper indica al Terminal A que envíe la llamada de señalización **directamente al Gateway de VoIP**, para ello, debe enviarle la dirección IP de dicho *Gateway*.

- **Comienza el proceso de establecimiento del canal de señalización, mediante mensajes H.225.0 (Q.931)**

1. El Terminal A envía un mensaje de *Setup* (H.225.0 *Call Signalling*) al *Gateway*

2. El *Gateway* envía *Call Proceeding* (H.225.0 *Call Signalling*) al Terminal, mientras traslada la señalización hacia la central local.

3. El *Gateway* arranca un proceso de Admisión (H.225.0 RAS) con su *Gatekeeper*, para que le autorice a entrar en la llamada. Con *ACF*, el Gatekeeper le autoriza a entrar.

4. El *Gateway* envía *IAM/ISUP* (SS7) hacia la central local.

5. La central local envía *SETUP* (Q.931) al abonado y *CPG/SS7* al *Gateway*.

6. El *Gateway* envía *ALERTING* (H.225.0 *Call Signalling*) al Terminal.

7. El abonado descuelga, y envía *CONNECT* (Q.931) a la central local.

8. La central local envía *ANM/ISUP* (SS7) al *Gateway*.

9. El *Gateway* envía *CONNECT* (H.225.0 *Call Signalling*) al Terminal, acompañado de la Dirección de Transporte (puerto TCP) para el canal de Control H.245, con lo que queda establecido el canal de control para su posterior uso en la fase de señalización H.245.

- Sobre el canal de control establecido, tiene lugar la segunda fase, entre el terminal y el Gateway, de intercambio de capacidades y establecimiento del canal sobre el que tendrá lugar el flujo de datos RTP (señalización H.245)
- Los canales de transporte de datos RTP han sido establecidos y la llamada ha sido completada con éxito.

- Si el *Gatekeeper* decidiera que la llamada de señalización fuera enrutada, es decir a través de él mismo, todos los pasos descritos en el **proceso de establecimiento del canal de señalización** se harían a través de dicho *Gatekeeper*. Este escenario podría ser de interés si se pretende tarificar desde el operador del *Gatekeeper*.

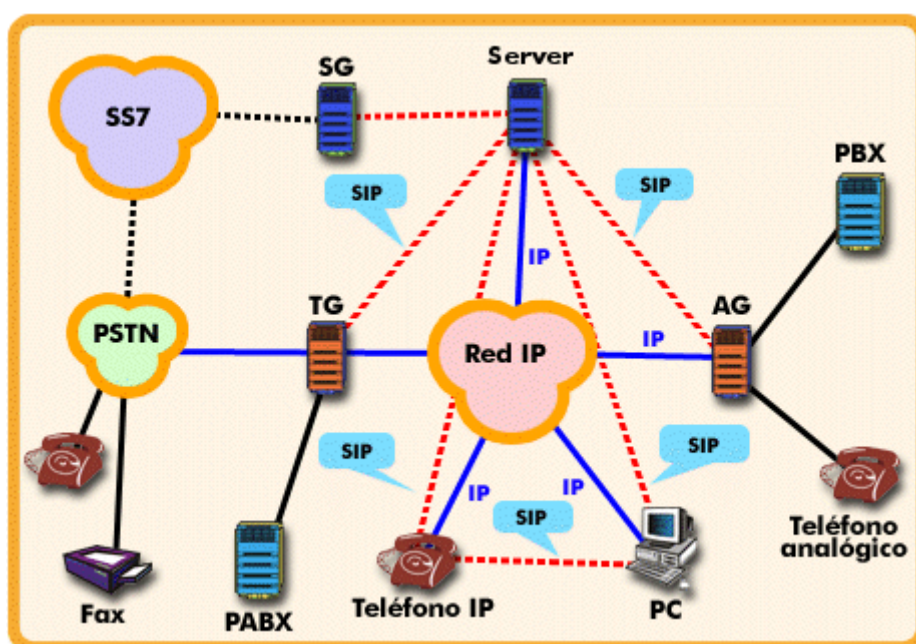
5.7 Protocollo SIP

Introducción a la Sección 5.7

Vas a comenzar el apartado 5.7:

Definición e Historia

Bueno, ya vistes que en el plano de control existían demasiados protocolos por ver, pero no desesperes, que ya nos van quedando menos...



Los orígenes de SIP se remontan a 1996, como un componente del conjunto de utilidades y protocolos “Mbone”.

El “Mbone” (que es un concepto que ha ido surgiendo bastante a lo largo del curso, y ya era hora de explicar), o Multicast backbone, fue una red multicast experimental, superpuesta a Internet, y que se usaba para la distribución de contenidos multimedia, incluyendo charlas y seminarios, difusiones de los lanzamientos espaciales y reuniones del IETF.

Uno de sus componentes esenciales era un mecanismo para invitar a los usuarios a futuras sesiones multimedia que iban a tener lugar en Internet. Es decir, básicamente, se trataba de un protocolo de inicio de sesión.

Así, como herramienta de Mbone, y producto de IETF, SIP fue diseñado con ciertas asunciones:

- Adaptabilidad al crecimiento de la red (scalability): puesto que los usuarios pueden residir en cualquier parte de Internet, el protocolo necesitaba funcionar en área amplia desde el comienzo.

- Reutilización de protocolos existentes: en lugar de dedicar esfuerzos a inventar nuevos protocolos, se usarían algunos de los que ya habían sido desarrollados dentro de IETF y que ya incluían cosas como MIME, URLs y SDP (por ejemplo, el protocolo SAP).

Así, surgió un protocolo que se integraba bien con otras aplicaciones IP (tales como web y e-mail).

- Interoperabilidad: la interoperabilidad está en el corazón de todos los procesos y operaciones de IETF.

En la mentalidad de sus diseñadores de estándares, rige la filosofía KISS (Keep It Simple Stupid) como mejor manera de garantizar la interoperabilidad.

Cuando el interés en la telefonía sobre Internet creció, la gente empezó a pensar en SIP como una tecnología que podría funcionar en VoIP, no sólo para sesiones de Mbone.

El resultado fue un esfuerzo intenso para la finalización de los estándares a finales de 1998. Recibió la aprobación oficial para convertirse en la RFC número 2543 en marzo de 1999.



Funcionalidad de SIP

Como su propio nombre indica, el protocolo de inicio de sesión (SIP) trata sobre el inicio de sesiones de comunicación interactivas entre usuarios. SIP también describe cómo modificar y terminar tales sesiones. Lo que no hace SIP es describir en qué consiste una sesión; eso está descrito por el contenido de los mensajes que lleva SIP.

La mayor parte de SIP está dedicada al proceso de inicio de la sesión, ya que suele ser el aspecto más problemático:

Localización del usuario

El inicio de una sesión requiere la **localización del usuario**, es decir, determinar en qué lugar se encuentra en ese instante el usuario con el que se quiere contactar. Pensemos que dicho usuario puede tener un PC en el trabajo, otro en casa y un teléfono IP en el laboratorio. Una llamada a ese usuario puede necesitar hacer sonar todos los teléfonos a la vez. Además, el usuario puede ser móvil; un día en el trabajo, otro de visita en la Universidad, etc. La información de localización dinámica debe ser tenida en cuenta al localizar al usuario.

Descripción de la sesión

Una vez que el usuario ha sido localizado, SIP puede realizar su segunda misión importante: la emisión de **la descripción de la sesión a la que el usuario está siendo invitado**. Como ya hemos mencionado, SIP, por sí mismo, no conoce los detalles sobre el tipo de sesión. Lo que hace SIP es transportar información sobre el protocolo utilizado para describir la sesión, y lo hace utilizando *Multipurpose Internet Mail Extensions* (MIME), ampliamente usadas en servicios **web** y de *e-mail* para describir contenidos codificados que no sean sólo texto (HTML, audio, video, etc). El protocolo más usado para describir sesiones es SDP (*Session Description Protocol*), descrito en la RFC 2327.

Respuesta a la petición

Con el usuario localizado y la descripción de la sesión emitida, se usa SIP para **llevar la respuesta a la petición de inicio de la sesión** (*accept*, *reject*, etc). Si se acepta, la sesión está activa desde ese momento.



Modificación de una sesión

La **modificación de una sesión** es muy sencilla con SIP; basta con enviar el mismo mensaje original de inicio de la sesión, pero con una descripción de sesión nueva. Modificar una sesión significa, por ejemplo, añadir o quitar señales de audio, añadir vídeo, cambiar codificadores, hacer *mute*, etc. Como puede verse, esto es muy fácil con SIP, siempre que el protocolo de descripción de sesión elegido lo soporte (SDP soporta todas las descripciones mencionadas anteriormente)

Finalmente, SIP también permite la **finalización de una sesión** (por ejemplo, por un cuelgue)

Características de SIP



¿Cómo serían los elementos que manejaría SIP para establecer y modificar sesiones?

SIP se basa en la arquitectura cliente-servidor.

Para iniciar una sesión, el llamante, también conocido como el User Agent Client (UAC), envía un request (llamado un INVITE), dirigido a la persona con la que el llamante quiere hablar.

En SIP, además, las direcciones son URLs.

SIP define un formato URL que es muy parecido al popular URL de "mailto".

Por ejemplo, si la dirección de correo electrónico es "lalonsobo@nexo.es", su URL SIP será: "sip:lalonsobo@nexo.es".

El mensaje INVITE no es enviado directamente al llamado, sino a una entidad conocida como proxy server.

El proxy server es el responsable del enrutamiento y envío de los mensajes al llamado.

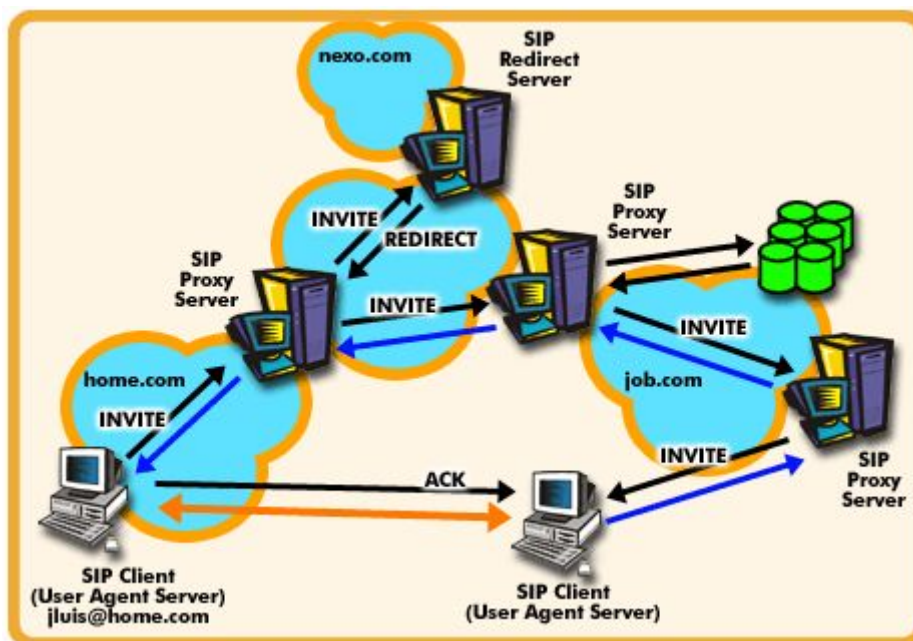
Cuando el llamado reciba el mensaje INVITE, responderá aceptando o rechazando la invitación, mensaje que es enviado en dirección contraria a través del mismo conjunto de proxies.

Un proxy puede recibir un único mensaje INVITE, y enviarlo a varias direcciones.

Esta funcionalidad, conocida por "forking" (bifurcación), permite que un intento de inicio de sesión alcance múltiples localizaciones, en la esperanza de encontrar al usuario en alguna de ellas.

Una analogía cercana es el servicio de línea telefónica doméstica, donde todos los teléfonos suenan a la vez.

Escenario SIP



Para hacerlo un poco más visual, utilizaremos un ejemplo concreto, mostrado en la figura, en el que el llamante jluis@home.com desea hablar con lalonso@nexo.com.

1. jluis envía el mensaje SIP INVITE al proxy server de home.com
2. Este proxy dirige el mensaje hacia la red Nexo, donde encuentra al server nexo.com. Este server no es un proxy. Se trata de un tipo especial de server similar a un proxy, llamado Redirect Server.
3. En lugar de reenviar los mensajes, como hace un proxy, indica al server que envió el mensaje INVITE, que contacte directamente con otro server (se le dice con cuál). Lo que ha sucedido es que, el server de nexo.com ha mirado en sus bases de datos y ha determinado que, hoy, lalonso no se encuentra en nexo.com, sino que está en job.com, así que envía una respuesta especial, llamada REDIRECT, al proxy home.com diciéndole que lo intente con lalonso@job.com
4. El proxy server home.com envía ahora el mensaje INVITE al server job.com, tratando de contactar con lalonso.
5. El proxy server job.com mira en su base de datos y descubre que lalonso está en ventas, en este momento.
6. El proxy server job.com construye la nueva URL lalonso@ventas.job.com y envía el mensaje INVITE al proxy server ventas.job.com
7. El proxy del departamento de ventas necesita ahora enviar el mensaje INVITE al PC donde lalonso está trabajando en este momento, pero no sabe a cuál.

Para ello, SIP proporciona un mecanismo de registro de clientes por el que lalonso deberá enviar un mensaje REGISTER al proxy ventas.job.com informándole de una ligazón entre las direcciones lalonso@ventas.job.com y lalonso@mipc.ventas.job.com.

Esto permitirá al proxy saber que lalonso se encuentra en mipc en estos momentos (la ligazón es temporal y se puede refrescar). Entoces, el proxy ventas.job.com consulta su base de datos y manda el mensaje INVITE a lalonso@mipc.ventas.job.com

8. El mensaje INVITE llega a lalonso que responderá con alguno de los mensajes de respuesta de que SIP dispone (ACCEPT, REJECT, REDIRECT, BUSY, etc).

9. Entonces jluis envía un reconocimiento (otro tipo de petición SIP, llamada ACK).

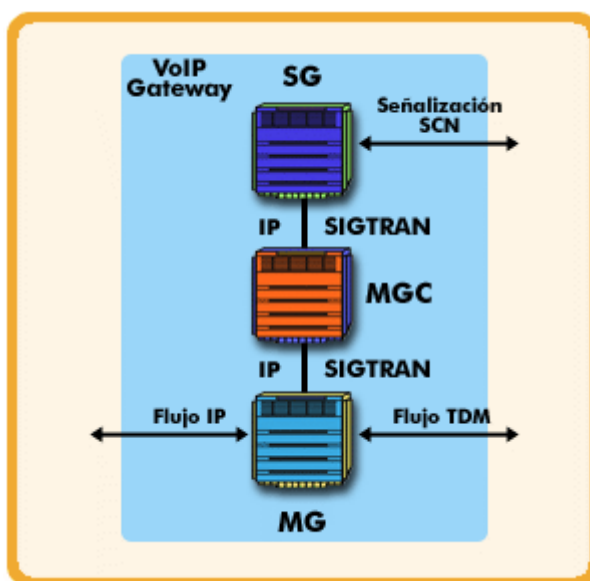
10. Y ... comienza el flujo de datos.

5.8 Protocolo SIGTRAN (Signalling Transport)

Introducción a la Sección 5.8

Vas a comenzar el apartado 5.8:

Definición y Modelo Funcional



¡Y ya hemos llegado al último protocolo que nos quedaba por ver! Ha sido un camino largo, pero muy interesante, ¿no?

Pero centrémonos en este nuevo protocolo. ¿Qué es SIGTRAN?

SIGTRAN es un protocolo que proporciona el transporte transparente de la señalización de las redes de conmutación de circuitos sobre redes IP.

SIGTRAN sólo se ocupa del transporte de señalización entre Signaling Gateway (SG) y Media Gateway Controller (MGC), así como entre Media Gateway y MGC.

SIGTRAN permite transportar una gran variedad de sistemas de señalización de las redes de conmutación de circuitos y, como todo protocolo de transporte, no interpreta dicha señalización, ya que su función se limita tan sólo a transportarla de forma transparente.

Resumiendo, si recordamos el modelo completo de dispositivos de VoIP necesarios, podríamos definir para el caso de SIGTRAN un modelo funcional que separa las funciones de un Gateway de VoIP en tres categorías:

- Signalling Gateway (SG),
- Media Gateway Controller (MGC) y



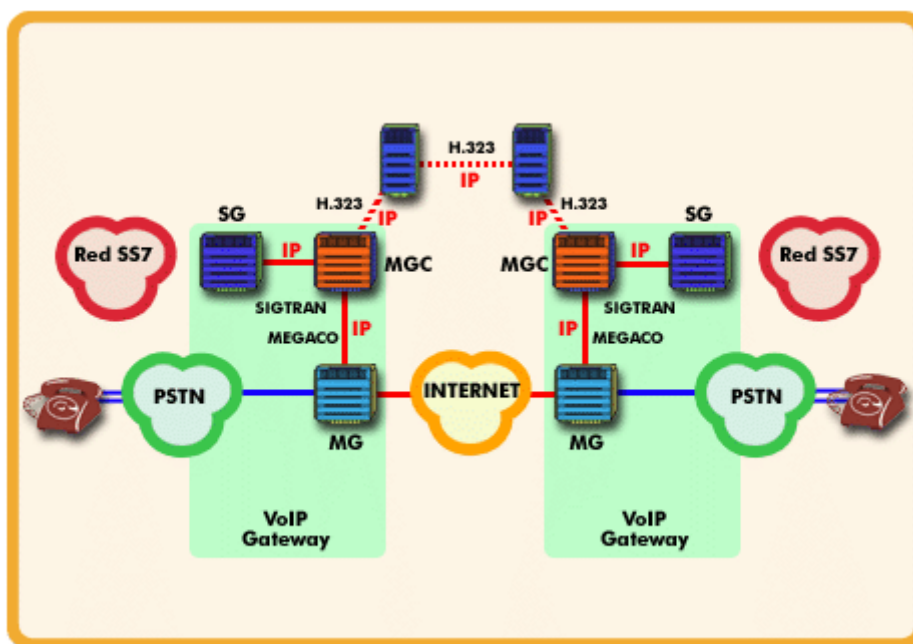
- Media Gateway (MG).

Las tres entidades que muestra el modelo pueden implementarse en equipos diferentes o agrupadas en un único equipo y funcionando como tres módulos software independientes que utilizan SIGTRAN para comunicarse.

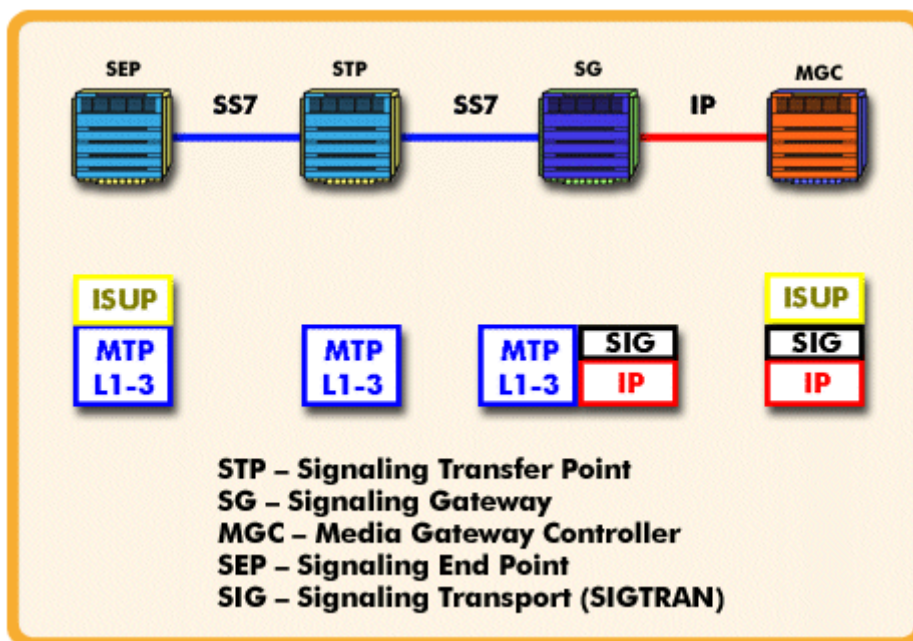
Ejemplo de Implementación de Llamada con SIGTRAN

Por último, podríamos ilustrar SIGTRAN mediante un ejemplo de implementación de llamada de teléfono-a-teléfono a través de Internet.

Un par de observaciones que realizar:



- La señalización transportada por los SG hasta el MGC es SS7.
- El control del MG desde el MGC se ha hecho con MEGACOP, aunque podía haberse implementado con H.248 (versión ITU de MEGACOP).





¿Y cuál sería la arquitectura de protocolos utilizada en el transporte de la señalización hasta el MGC? Pues la mostrada en la figura adyacente...