

INTRODUCCIÓN	4
PARTE I INVESTIGACION DE LA TECNOLOGIA VOZ SOBRE IP	6
CAPITULO 1 BASES DE LA PSTN	7
1.1 ANTECEDENTES	7
1.2 BASES DE LA PSTN	7
1.2.1 SEÑALIZACIÓN ANALÓGICA Y DIGITAL	8
1.2.2 SEÑALES DE VOZ DIGITALES	9
1.2.3 ESTRUCTURA DE LA PSTN	9
1.2.4 MEDIOS DE TRANSMISIÓN EN LA PSTN Y MÉTODOS DE SEÑALIZACIÓN	10
CAPÍTULO 2 SEÑALIZACION BASICA DE LA TELEFONIA	13
2.1 SEÑALIZACIÓN DE BIT ROBADO (RBS)	13
2.2 SEÑALIZACIÓN DE CORRIENTE CONTINUA	13
2.3 SEÑALIZACIÓN DENTRO Y FUERA DE BANDA	13
2.3.1 FRECUENCIA ÚNICA (FS).	14
2.3.2 MULTIFRECUENCIA (MF).	14
2.3.3 DTMF (DUAL-TONE MULTI FREQUENCY).	14
2.4 SEÑALIZACIÓN INICIO DE BUCLE E INICIO EN TIERRA	14
2.4.1 SEÑALIZACIÓN DE INICIO DE BUCLE.	14
2.4.2 SEÑALIZACIÓN INICIO EN TIERRA.	15
2.5 SEÑALIZACIÓN CAS Y CCS	15
2.5.1 SEÑALIZACIÓN CAS	15
2.5.2 SEÑALIZACIÓN CCS	15
2.6 SEÑALIZACIÓN E&M	17
CAPÍTULO 3 SERVICIOS Y APLICACIONES DE LA PSTN	18
3.1 PRINCIPALES SERVICIOS DE LA PSTN	18
3.1.1 SERVICIO TELEFÓNICO ANALÓGICO CONVENCIONAL (POST)	18
3.1.2 RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI)	19
3.1.3 SERVICIOS DE EMPRESA	19
3.1.4 SERVICIO DE PROVEEDOR DE SERVICIOS	20
3.2 INCONVENIENTES DE LA PSTN	21
3.3 NUEVO MODELO DE INFRAESTRUCTURA DE RED PSTN	21
CAPÍTULO 4 INVESTIGACIÓN SOBRE IP	23
4.1 MODELO OSI (OPEN SYSTEM INTERCONNECTION)	23
4.1.1 CAPA DE APLICACIÓN	24
4.1.2 CAPA DE PRESENTACIÓN	24
4.1.3 CAPA DE SESIÓN	24
4.1.4 CAPA DE TRANSPORTE (CAPA HOST – HOST)	24

4.1.5 CAPA DE RED	25
4.1.6 CAPA DE ENLACE DE DATOS	25
4.1.7 CAPA FÍSICA	26
4.2 PROTOCOLO DE INTERNET (IP)	26
4.3 DIRECCIONES DE LA CAPA DE ENLACE (MAC)	27
4.4 DIRECCIONES IP	28
4.5 TCP (TRANSFER CONTROL PROTOCOL)	29
4.6 UDP (USER DATAGRAM PROTOCOL)	29
4.7 COMPARACIÓN ENTRE EL MODELO OSI Y TCP/IP	29

CAPÍTULO 5 FUNCIONAMIENTO DE VOZ SOBRE IP **31**

5.1 FUNCIONAMIENTO GENERAL	31
5.2 DE CONMUTACIÓN DE CIRCUITOS A CONMUTACIÓN DE PAQUETES.	32
5.3 REDES ORIENTADAS Y NO ORIENTADAS A CONEXIÓN.	34
5.4 ASPECTOS A CONSIDERAR EN VOIP	35
5.4.1 RETRASO / LATENCIA	35
5.4.2 FLUCTUACIÓN DE FASE	37
5.4.3 MODULACIÓN POR IMPULSOS CODIFICADOS	37
5.4.4 COMPRESIÓN DE VOZ	38
5.4.5 ECO	38
5.4.6 PÉRDIDA DE PAQUETES	39
5.4.7 DETECCIÓN DE ACTIVIDAD DE VOZ	39
5.4.8 CONVERSIÓN DIGITAL A ANALÓGICO	40
5.4.9 CODIFICACIÓN TÁNDEM	40
5.4.10 PROTOCOLOS DE TRANSPORTE	41
5.4.11 DISEÑO DE PLAN DE MARCACIÓN	43
5.5 CALIDAD DE SERVICIO EN VOIP	44
5.5.1 ANCHO DE BANDA	44
5.5.2 GESTIÓN DE COLAS	45
5.5.3 CLASIFICACIÓN DE PAQUETES	45
5.5.4 FRAGMENTACIÓN	46

CAPÍTULO 6 EL ESTÁNDAR VOIP H.323 **47**

6.1 ESTÁNDAR VOIP	47
6.2 ESTÁNDAR H.323	48
6.3 HISTORIA DEL H.323	49
6.4 ARQUITECTURA H.323	51
6.4.1 DEFINICIONES	52
6.4.2 COMPONENTES DEFINIDOS EN H.323	52
6.5 ESTÁNDARES Y PROTOCOLOS DEL H.323	56
6.5.1 PROTOCOLOS DE DIRECCIONAMIENTO	56
6.5.2 PROTOCOLOS DE SEÑALIZACIÓN	71
6.5.3 PROTOCOLOS DE COMPRESIÓN DE VOZ	80
6.5.4 PROTOCOLOS DE TRANSMISIÓN DE VOZ	83
6.5.5 PROTOCOLOS DE CONTROL DE LA TRANSMISIÓN:	92
6.5.6 PROTOCOLOS DE DATOS	100
6.5.7 PROTOCOLOS PARA TRANSMISIÓN EN TIEMPO REAL	100

6.6 MECANISMOS PARA MANTENER LA CALIDAD DE SERVICIO (QOS)	102
6.7 RENDIMIENTOS VoIP CON H.323	104
6.7.1 INTEROPERATIVIDAD E IMPLEMENTACIÓN	105
6.7.2 CARENCIA DE SERVICIOS DE VALOR AÑADIDO	106
6.7.3 CALIDAD Y SEGURIDAD	106
6.7.4 NUEVOS ESTÁNDARES PARA VOZ SOBRE IP	107
6.7.5 FUTUROS DESARROLLOS EN H.323	110
<u>CAPÍTULO 7 GATEWAYS Y GATEKEEPER</u>	<u>111</u>
7.1 GATEWAY (GW)	111
7.2 GATEKEEPER (GK)	113
<u>CAPÍTULO 8 VENTAJAS Y APLICACIONES DE VOZ SOBRE IP</u>	<u>114</u>
8.1 PRINCIPALES VENTAJAS	114
8.2 OTRAS VENTAJAS	114
8.3 APLICACIONES DE VoIP	115
<u>CAPÍTULO 9 SOLUCIONES DE PROVEEDORES</u>	<u>116</u>
9.1 MOTOROLA	116
9.2 CISCO	118
9.2.1 SOLUCIONES PEQUEÑAS	119
9.2.2 SOLUCIONES MEDIANAS	120
9.2.3 SOLUCIONES GRANDES	121
9.2.4 OTRAS SOLUCIONES	122
<u>CONCLUSIONES</u>	<u>124</u>
<u>PARTE II PRACTICA: IMPLEMENTACION VOIP</u>	<u>126</u>
IMPLEMENTACIÓN DE VoIP	127
COMANDOS UTILIZADOS PARA LA CONFIGURACIÓN DE VoIP	129
PRUEBAS Y EJECUCIÓN	131
CONCLUSIONES Y RECOMENDACIONES TÉCNICAS	132
LISTADO DE ACRÓNIMOS	134
<u>BIBLIOGRAFÍA</u>	<u>135</u>
<u>ANEXO 1 – CONFIGURACION DE LOS EQUIPOS</u>	<u>137</u>
<u>ANEXO 2 - DISEÑO DE TESIS</u>	<u>142</u>

INTRODUCCIÓN

Durante mucho tiempo las redes de datos se han utilizado únicamente para la transmisión de datos, pero hoy en día, gracias a los avances tecnológicos y mediante la adopción de ciertos estándares, es posible enviar voz y vídeo sobre LANs corporativas, WANs y sobre Internet, con la gran ventaja de utilizar la infraestructura existente.

Este progreso fue posible debido al rápido crecimiento y fuerte implantación de las redes IP, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que han permitido mejorar la calidad de servicio en redes IP.

En la actualidad es muy común escuchar el término VoIP, sin embargo no todos conocen o entienden su funcionamiento, ventajas, utilidad.

En esta tesis se han desarrollado los conceptos básicos y fundamentos necesarios para entender el funcionamiento de esta nueva tecnología, conocer los equipos necesarios y conocer los protocolos que la rigen.

Hemos dividido la tesis en dos partes, la primera que es un entorno teórico y la segunda parte en la que describimos una implementación práctica de VoIP en la empresa ECUAELECTRICIDAD.

En los capítulos 1, 2 y 3, describimos las primeras tecnologías utilizadas para la transmisión de voz (PSTN), así como los métodos de señalización para la transmisión, todo esto como un antecedente que dio origen al desarrollo de la tecnología de Voz sobre IP.

El capítulo 4, explica los conceptos básicos sobre redes y sobre el protocolo IP que es el protocolo base de esta tecnología. No se profundiza en ningún punto, el objetivo de este capítulo es recordar conceptos como el modelo OSI pues es un protocolo estándar, y algunos otros términos importantes.

En los capítulos 5, 6 y 7, se analiza a profundidad el protocolo VoIP, los estándares que rigen el funcionamiento de este protocolo, aspectos importantes que se deben considerar como es el eco, retraso, fluctuación de fase, etc., mecanismos para mantener la calidad de servicio. Estos tres capítulos son considerados el centro de nuestra tesis, pues describen en sí al protocolo VoIP. Como el protocolo H.323 es el protocolo más conocido e implementado para soluciones de VoIP, hemos profundizado en éste y en cada uno de los protocolos relacionados. También se hace una breve comparación entre el H.323 y un nuevo estándar muy prometedor como es el SIP.

En el capítulo 8, se describen las ventajas de utilizar la tecnología VoIP sobre todo en el ámbito empresarial, donde el aspecto principal es la reducción de costos en las planillas telefónicas. En este capítulo se describen brevemente algunas aplicaciones desarrolladas para VoIP.

En el capítulo 9, se han expuesto soluciones VoIP de dos proveedores que tienen renombre en nuestro medio como son Cisco y Motorola.

PARTE I

INVESTIGACION DE LA TECNOLOGIA VOZ SOBRE IP

La primera parte de esta tesis engloba todo el marco teórico relacionado con la tecnología de Voz sobre IP. Comenzamos con una explicación de la infraestructura telefónica actual, se presentan conceptos relacionados con la señalización de la voz en las redes telefónicas actuales, todo esto como una introducción a VoIP para llegar a comprender de mejor manera lo que es VoIP, sus ventajas y utilidades, como funciona tanto en redes privadas como al hacer uso de la red pública de telefonía. Se explican también todos los protocolos que rigen el funcionamiento de VoIP, profundizando en el protocolo H.323 que es el más difundido y utilizado hoy en día.

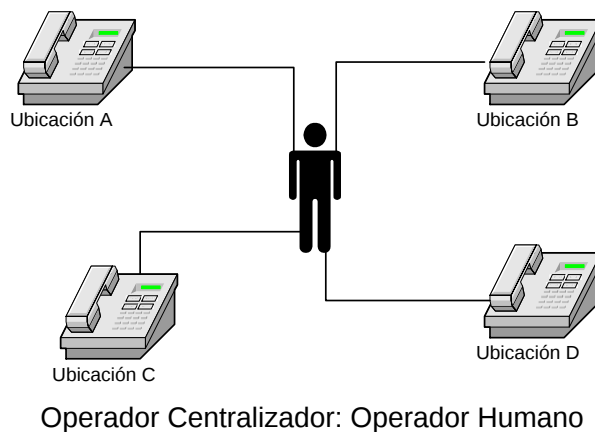
Capítulo 1 Bases de la PSTN

1.1 ANTECEDENTES

La Red Pública de Telefonía Conmutada (PSTN) nace en 1876, cuando Alexander Graham Bell realiza la primera transmisión de voz por un circuito que llamó ring-down en el que no existía marcación de números, sino que un cable conectaba físicamente los dos dispositivos y básicamente una persona descolgaba el teléfono y la otra se encontraba al otro extremo.

Este diseño con el tiempo evolucionó desde una transmisión de voz de un único sentido, hasta una transmisión de voz bidireccional. Entre cada ubicación a la que el usuario quería llamar se necesitaba un cable físico y aún no existía el concepto de marcación, lo que no resultaba de ninguna manera rentable.

Se desarrolló entonces el dispositivo switch ó conmutador, con el cual, los usuarios de teléfonos necesitaban un solo cable que vaya a la oficina de switch central donde un operador preguntaba a la persona que llamaba a donde quería llamar y conectaba manualmente las dos rutas de voz. Cien años más tarde este operador fue reemplazado por la conmutación electrónica.

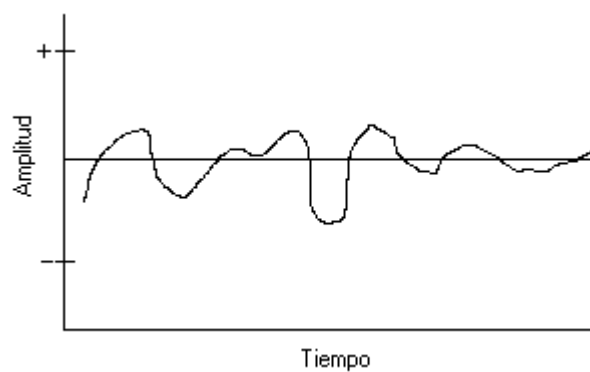


1.2 BASES DE LA PSTN

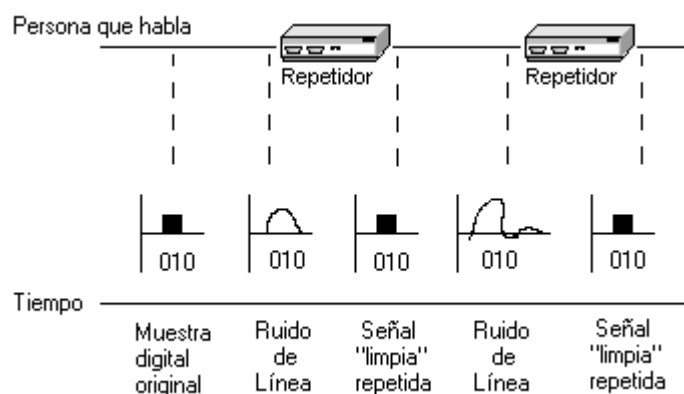
En este capítulo se explicará cómo se transmite la voz a través de una red digital, como está estructurada la PSTN y conceptos básicos del switching de circuitos.

1.2.1 Señalización analógica y digital

Todo lo que nosotros escuchamos, incluso la voz humana, tiene una forma analógica y hasta varias décadas atrás la red de telefonía también tenía una infraestructura analógica. Si bien la comunicación analógica es muy buena para la interacción humana, ésta no es robusta ni eficiente para evitar el ruido en la línea. En los inicios de las redes telefónicas la voz se pasaba a través de amplificadores para aumentar la señal, pero esto no resultó ya que no solo se amplificaba la voz sino también el ruido en la línea lo que hacía que a veces la conexión fuera inutilizable.



En las redes digitales el ruido en la línea no es problema ya que dicha comunicación se basa en “unos” y “ceros”, por lo tanto los repetidores amplifican la señal y a la vez la limpian hasta devolverle su condición original, es decir solo regenerar un 1 o un 0. Cuando los beneficios de este tipo de comunicación fueron evidentes, la red de telefonía migró a la modulación por impulsos codificados (PCM).



Distorsión de línea digital.

1.2.2 Señales de voz digitales

El método más común de codificar una voz analógica en un flujo digital es la modulación por impulsos codificados (PCM). La técnica de PCM más habitual utiliza el teorema de Nyquist, que dice básicamente que si se hace un muestreo al doble de la frecuencia más alta en una línea de voz, se consigue una transmisión de voz de buena calidad.

En el proceso PCM : - las formas de onda analógicas se pasan por un filtro de frecuencia de voz para filtrar señales mayores a 4000 Hz; - la señal analógica filtrada es muestreada a una velocidad de 8000 veces por segundo cumpliéndose el teorema de Nyquist pues la frecuencia más alta es de 4000 Hz; - la forma de onda muestreada se convierte en una forma digital discreta. La muestra está representada por un código de 8 bits que indica la amplitud de la forma de onda en el instante en que se tomó la muestra. Se utiliza un método de compresión logarítmico que asigna más bits para señales de amplitud más baja.

La base para la infraestructura del teléfono es de 64000 bps (bits por segundo) ó 64 kbps que resulta de multiplicar las palabras de ocho bits 8000 veces por segundo.

Para la compresión de voz se utilizan dos variaciones básicas de PCM de 64 kbps: La ley μ y la ley a . Ambos utilizan compresión logarítmica para alcanzar de 12 a 13 bits de calidad PCM lineal en palabras que tienen sólo 8 bits, pero se diferencian en detalles de compresión relativamente pequeños (la ley μ tiene una ligera ventaja en la capa baja, rendimiento en relación de señal al ruido). La ley μ se utiliza en América del Norte y la ley a en Europa.

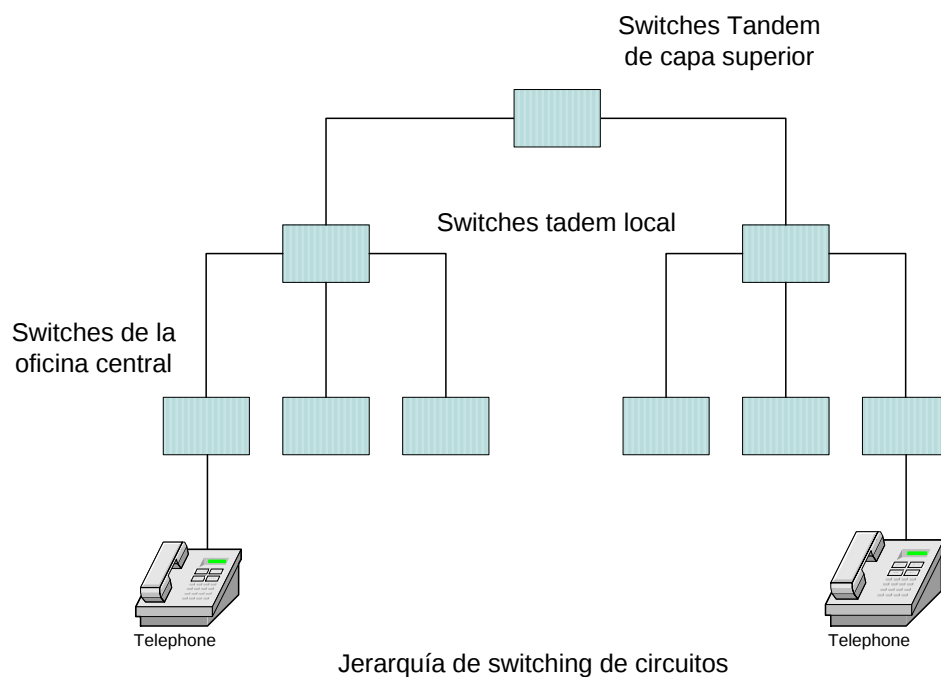
1.2.3 Estructura de la PSTN

El sistema telefónico se basa en el uso de centrales para conmutar las llamadas entre diversos abonados, y de pares de hilos de cobre para unir a cada abonado con la oficina central.

Se conoce como bucle local, al cableado físico, es decir el cable que une el teléfono del abonado con el switch de su central telefónica. La ruta de comunicación entre el switch de la central telefónica y la casa se conoce como línea telefónica. Los bucles locales conocidos también como bucle de abonado, suelen ser pares de cobre trenzado.

A los switches de la central telefónica se los conoce también como switch de clase 5 o switch de oficina final. La ruta de comunicación entre los switches de varias centrales telefónicas, se conoce como enlace troncal (trunk). Las líneas troncales típicamente utilizan cable coaxial, microondas, fibra óptica o enlaces vía satélite.

Como no sería rentable colocar un cable físico entre los switches de cada central telefónica, se ha establecido la jerarquía de switching que consiste en interconectar los switches de clase 5, a través de enlaces troncales, con switches tándem (clase 4), a su vez los switches tándem estarán conectados a otros de mayor rango, y así sucesivamente; pueden llegar a existir hasta cinco niveles de jerarquización.



1.2.4 Medios de transmisión en la PSTN y Métodos de Señalización

Los métodos de señalización están divididos en dos grupos, sin importar el medio de transmisión:

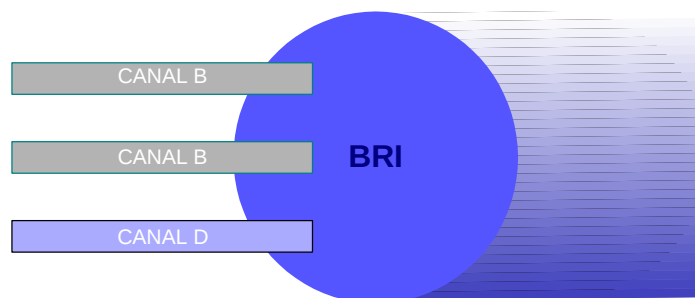
- Señalización usuario red. Comunicación entre usuario final con la PSTN.
- Señalización red a red. Intercomunicación entre la PSTN.

1.2.4.1 Señalización usuario a red

Un usuario que utiliza un par de cobre trenzado para el transporte, generalmente se conecta con la PSTN a través de una Red Digital de Servicios Integrados (RDSI o ISDN) analógica, o a través de un carrier (portadora) T1 (de capa digital 1).

Marcación Multifrecuencia (DTMF), es la más habitual para la comunicación analógica usuario a red. Es un método de señalización dentro de banda pues transporta los tonos de marcación a través de la ruta de voz. Los tonos de marcación pasan desde el teléfono hasta el switch de la oficina central e indican a que número se quiere llamar. Cuando la señalización se transporta a través de la ruta de voz, es decir cuando se utiliza un método de señalización dentro de banda, se puede presentar el inconveniente de que haya tonos perdidos.

Señalización fuera de banda, es el método utilizado por la RDSI, la señalización es transportada en un canal separado de la voz. El canal que transporta la voz se llama canal portador (bearer ó canal B) y es de 64 Kbps, el canal que transporta la señal se llama canal de datos (canal D) y es de 16 Kbps. Existen muchos beneficios al utilizar la señalización fuera de banda, entre los cuales tenemos: - La señalización viaja en un canal común, - Reducción de la colisión, - Retraso posmarcación más bajo, - Ancho de banda mayor.



Interfaz de acceso básico

1.2.4.2 Señalización red a red

La comunicación red a red puede llevarse a cabo a través de los siguientes medios de transmisión:

- Carrier T1/E1 sobre par trenzado T1 es un enlace de transmisión digital de 1,544 Mbps utilizado normalmente en América del Norte y Japón. E1 es un enlace de transmisión digital de 2,048 Mbps que se utiliza normalmente en Europa.
- Carrier T3/E3, T4 sobre cable coaxial T3 transporta 28 T1 o 672 conexiones de 64 kbps y tiene 44,736 Mbps. E3 transporta 16 E1 ó 512 conexiones de 64 kbps y tiene 34,368 Mbps. T4 maneja 168 circuitos T1 o 4.032 conexiones de 4 kbps y tiene 274,176 Mbps.
- Carrier T3, T4 sobre enlace de microondas
- La red óptica sincrónica (SONET) a través de los medios de fibra óptica. SONET se despliega normalmente a una velocidad de OC-3 (155,52 Mbps), OC-12 (622,08 Mbps) y OC-48 (2,488 Gbps).

La señalización red a red incluye métodos de señalización dentro de banda, como la multifrecuencia (MF) y la señalización de bit rodado (RBS), y, métodos fuera de banda como el Sistema de Señalización 7.

Los sistemas de carrier digitales (T1, T3) utilizan los bits A y B para indicar el estado colgado – descolgado. Estos bits emulan tonos de Frecuencia única (SF). (La SF suele utilizar la presencia o ausencia de una señal para señalar las transiciones del bit A/B). Estos Bits pueden ser “robados” del canal o multiplexados en un canal común.

Señalización multifrecuencia (MF), es un método de señalización dentro de banda, es similar a la DTMF pero ésta utiliza un conjunto diferente de frecuencias. A diferencia de la DTMF que señala desde el teléfono al switch de oficina central, la MF señala de switch a switch.

Sistema de señalización 7 (SS7)(C7 en Europa), es un método de señalización fuera de banda que se utiliza para conectar switches. En el capítulo 2 se explica más a fondo el SS7.

Capítulo 2 Señalización Básica de la telefonía

Es importante conocer los tipos de señalización básica de la telefonía para poder luego entender métodos y estándares de señalización.

En este capítulo se amplían los métodos de señalización vistos en el capítulo anterior.

2.1 SEÑALIZACIÓN DE BIT ROBADO (RBS)

La señalización digitalizada es la más común utilizada actualmente en redes corporativas y de proveedores de servicios.

La técnica de señalización que utiliza ésta, es la señalización de bit robado (robbed-bit) que consiste en robar un bit de las tramas designadas para utilizarlo con fines de señalización, este bit viaja en el flujo de voz digital sin afectar la calidad de voz.

2.2 SEÑALIZACIÓN DE CORRIENTE CONTINUA

Depende de la corriente continua (CC) para señalar el switch extremo u oficina. Esta señalización indica los cambios del estado de la transición activando o desactivando el flujo de corriente continua. Los Switch de oficina final utilizan detectores de corriente para identificar los cambios en el estado.

El bucle de abonado utiliza este tipo de señalización entre el abonado y la oficina final local. Las tarjetas de la línea en la oficina local están equipadas con detectores de corriente para determinar cuándo se requiere de una conexión.

2.3 SEÑALIZACIÓN DENTRO Y FUERA DE BANDA

La señalización dentro de banda utiliza tonos en lugar de CC, los mismos que se transmiten por la misma instalación que la voz y, por tanto, están dentro de la banda de voz de 0-4 Hz.

2.3.1 Frecuencia única (FS).

Se utiliza para enlaces troncales ínter oficina y tiene dos estados posibles: on-hook (desocupado), y off-hook (ocupado). El tono de frecuencia única está basado en una única frecuencia de 2600 Hz., y se utiliza para identificar el cambio de estado. Cuando una conexión ha terminado no hay tono presente. Cuando una de las dos partes cuelga, se envía un tono de 2600 Hz. por el circuito notificando la desconexión.

2.3.2 Multifrecuencia (MF).

Se utiliza por los enlaces troncales ínter oficina para indicar eventos, como toma, liberación, respuesta o reconocimiento, y para transmitir información como el número de quien llama. La MF utiliza una combinación de impulsos especificada por frecuencias para señalar a través de una red.

2.3.3 DTMF (Dual-Tone Multi Frequency).

Se utiliza para transmitir dígitos de números de teléfono desde el abonado hasta la oficina local. Los tonos de la DTMF identifican números del 0 al 9 y los símbolos * y #. Los dígitos están representados por una combinación particular de frecuencias: una del grupo inferior (697, 770, 852 y 941 Hz) y otra del superior (1290, 1336, 1447 y 1633 Hz).

2.4 SEÑALIZACIÓN INICIO DE BUCLE E INICIO EN TIERRA

Son las más comunes en la señalización de bucle final.

2.4.1 Señalización de inicio de bucle.

Es utilizada por el bucle del abonado. Funciona de la misma manera que el teléfono y la oficina final local, donde la creación de un bucle inicia una llamada y el cierre de un bucle termina una llamada. El inconveniente de esta señalización es que pueden ocurrir colisiones.

2.4.2 Señalización inicio en tierra.

Se diferencia del anterior en que proporciona un reconocimiento positivo de las conexiones o desconexiones a través de mecanismos de detección en cada extremo del enlace troncal. Este es el método preferido de señalización para los PBX pues minimiza el efecto de colisión.

2.5 SEÑALIZACIÓN CAS Y CCS

2.5.1 Señalización CAS

La señalización asociada al canal (CAS) consiste en transportar información sobre la señalización desde el enlace troncal hasta el propio enlace troncal. Existen muchas versiones del CAS pues en su origen fueron desarrollados por diferentes fabricantes.

2.5.2 Señalización CCS

La señalización Sistemas comunes de tipo de canal (CCS) utiliza un enlace común para transportar la información de la señalización un una cantidad de enlaces troncales. Es más flexible que el CAS. La primera generación de CCS se conoce como SS6; la segunda como SS7.

2.5.2.1 Señalización SS7.

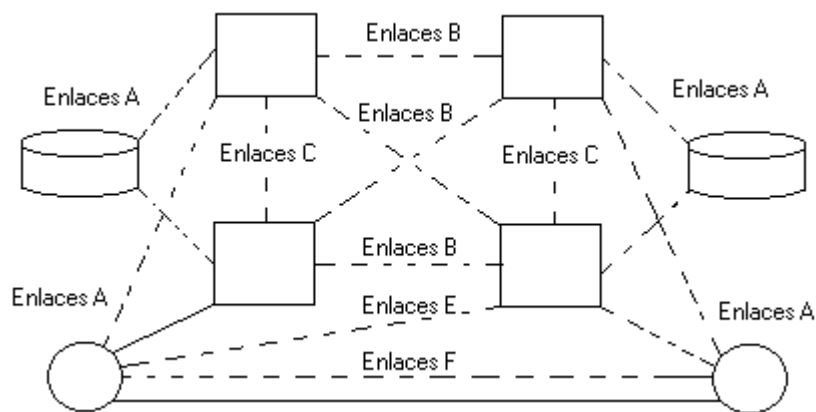
SS7 es un estándar de señalización de canal común (CCS) desarrollado a finales de los setenta por la ITU-T. La funcionalidad del SS7 se ha extendido desde sus orígenes y actualmente incluye la consulta a bases de datos, las transacciones, las operaciones en red y la RDSI.

La SS7 soporta la PSTN manejando el establecimiento de la llamada, el intercambio de información, el enrutamiento, las operaciones, la facturación y el soporte para servicios de red inteligente (IN).

SS7 proporciona un protocolo común para la señalización, el envío de mensajes o el interfacing para los que se pueden desarrollar dispositivos VoIP, de ahí su importancia en

Voz sobre IP. Los planos de señalización y los planos de circuito de voz están separados lógicamente.

Las redes SS7 constan de tres elementos de señalización: Punto de Switching de servicios (SSP), punto de transferencia de señal (STP) y punto de control de servicio (SCP), así como varios tipos de enlaces.



Enlaces de Señalización.

Los SSP (Service Switching Point) son oficinas finales o switches tándem (conmutadores de tránsito), que concentran circuitos de voz y realizan las funciones de señalización necesarias para originar y terminar las llamadas.

El STP (Signal Transfer Point) enruta todos los mensajes de señalización en la red SS7.

El SCP (Service Control Point) proporciona acceso a las bases de datos para información de enrutamiento adicional que se utiliza en el proceso de llamada para los procesos no basados en circuitos. El SCP es un elemento clave para entregar aplicaciones IN.

Los enlaces de señalización proporcionan la transmisión de señalización y acceden a la red SS7 y, por tanto, deben estar siempre disponibles.

El método de señalización SS7 ofrece los siguientes beneficios:

- Retraso posmarcado reducido: Transmite todos los dígitos en un mensaje de configuración inicial incluyendo los números completos del que llama y al que llama.
- Finalización incrementada de la llamada. Genera paquetes sencillos con toda la información necesaria que son transmitidos más rápido que los tonos generados en una red dentro de banda.
- Conexión a la red inteligente (NI)

2.6 SEÑALIZACIÓN E&M

Es una técnica de señalización de enlace troncal común utilizada en los switches telefónicos y PBX. Los enlaces troncales de señalización y voz en E&M están separados. La voz se transmite a través de circuitos de dos o cuatro cables, con seis métodos de señalización: Tipo I, II, III, IV, V que son conocidos como el estándar SSDC5 de la British Telecom (BT).

En la siguiente tabla se resumen las condiciones del cable de E&M para los estados on-hook (desocupado) y off-hook (ocupado).

Tipo	Cable M		Cable E	
	<i>Off-hook</i>	<i>On-hook</i>	<i>Off-hook</i>	<i>On-hook</i>
I	Batería	Tierra	Tierra	Abierto
II	Batería	Abierto	Tierra	Abierto
III	Bucle actual	Tierra	Tierra	Abierto
IV	Tierra	Abierto	Tierra	Abierto
V	Tierra	Abierto	Tierra	Abierto

Capítulo 3 Servicios y aplicaciones de la PSTN

La PSTN ofrece numerosos servicios diferentes, cada uno con un gran conjunto de prestaciones y funcionalidad. En este capítulo se trata los principales servicios ofrecidos tanto a clientes particulares, como empresariales.

3.1 PRINCIPALES SERVICIOS DE LA PSTN

Entre los principales servicios se tienen los siguientes:

- Servicio telefónico analógico convencional (POTS)
- Red digital de Servicios Integrados (ISDN ó RDSI)
- Servicios Empresariales, incluidas las redes privadas virtuales, Centres, y los servicios de centros de llamadas.
- Servicios SP, incluidos servicios de Base de Datos y de operadoras.

3.1.1 Servicio Telefónico Analógico Convencional (POST)

La Red de Telefonía Básica (RTB) también llamada POST (Plain Old Telephone Service), está formada por las líneas analógicas tradicionales.

El POST proporciona un tono de marcado a los teléfonos de disco (Rotary), teléfonos de teclas (Touch-Tone), así como el acceso a las portadoras (Carriers) nacionales e internacionales.

La mayoría de abonados post tiene disponible los siguientes servicios:

- Función de personalización de llamada que incluye llamada en espera, desvío de llamadas a un destino diferente, multiconferencia, marcado rápido almacenando los números más utilizados;
- Funciones CLASS (Función de servicios de señalización de área local personalizados);
- Correo de voz con dos principales servicios: mensajes de voz (saludos pregrabados, recibir y distribuir mensajes de otros usuarios) y, mensajes de fax (graba los faxes para consultarlos posteriormente).

CLASS es un conjunto de funciones muy populares que proporcionan a los abonados una potente y cómoda herramienta para controlar las llamadas entrantes y salientes. El acceso a estos servicios se ha hecho posible gracias al desarrollo de la red SS7:

- Presenta o muestra el número del que está llamando;
- Bloqueo de llamada de números específicos;
- Bloqueo del ID para que el número no pueda ser visto en la pantalla de la persona que recibe la llamada;
- Retrollamada automática cuando el número marcado está ocupado;
- Devolución de llamadas para responder rápidamente llamadas perdidas.

3.1.2 Red Digital de Servicios Integrados (RDSI)

La RDSI (Red Digital de Servicios Integrados) o ISDN (Integrated Services Digital Network) suministra un conjunto de servicios datos y voz digitales que está disponible actualmente en la PSTN; está constituida por enlaces digitales hasta el bucle de abonado, por lo que el circuito se constituye de forma digital extremo a extremo. En RDSI la velocidad por circuito es 64 Kbps, pudiendo con relativa facilidad agregarse varios circuitos (llamados canales) en una misma comunicación para aumentar el ancho de banda. La RDSI es una red de conmutación de circuitos, en la que la conexión extremo a extremo sólo se establece durante el tiempo necesario, la transmisión de datos utiliza la misma red que para la transmisión de voz.

3.1.3 Servicios de Empresa

Los entornos corporativos requieren amplios servicios de comunicación para soportar sus negocios y entre otros servicios tenemos:

3.1.3.1 Redes de voz privadas virtuales

Estas interconectan el tráfico de voz corporativo entre múltiples ubicaciones en la PSTN, la alternativa a este servicio sería una línea Tie dedicada entre ubicaciones.

3.1.3.2 Servicios Centrex

Los servicios centrex pueden crear una red empresarial privada virtual, proporcionando los siguientes servicios:

- Tratamiento de llamada. Llamada en espera, transferencia de llamada, estacionamiento de llamada, etc.;
- Funciones de conveniencia, como marcado automático, remarcado, identificación de llamada;
- Planes de marcación personalizadas, permitiendo, marcación abreviada para llamadas internas;
- Seguridad que incluye restricción de líneas, códigos de autorización para empleados, registro detallado de llamadas.

3.1.3.3 Servicios de centros de llamadas

Como los centros de llamadas tienen un gran volumen de llamadas entrantes, este servicio ofrece una distribución automática de llamada (ACD) que enruta de manera eficaz las llamadas entrantes hacia múltiples estaciones de respuesta.

3.1.4 Servicio de Proveedor de servicios

Los servicios de proveedor de servicios (SP) son funciones internas para soportar usuarios de la PSTN. Entre los servicios que ofrece se encuentran los siguientes:

3.1.4.1 Servicios de Bases de Datos

Que permiten mantener, acceder y traducir información utilizada para soportar servicios especiales y números de acceso. Las bases de datos pueden proporcionar los siguientes servicios: Servicio de tarjetas de llamada, servicios de autorización, Servicios del número 800/900.

3.1.4.2 Servicios de Operadora

Entre los servicios de operadora tenemos: las llamadas de larga distancia, asistencia general, asistencia de directorio marcando un código, servicios de facturación para llamadas a cobro revertido, facturación de terceras partes, tarjetas de llamada y servicios de tarjeta de crédito.

3.2 INCONVENIENTES DE LA PSTN

Los inconvenientes que presenta la PSTN cuando se intenta transportar Voz son muchos y las siguientes son las razones que están llevando a pensar en una nueva red donde la voz sea una aplicación en lo alto de una red de datos:

- Los datos son el tráfico principal incluso en muchas redes que fueron construidas para la voz. Para diferenciar la voz se deberá utilizar la base de la aplicación en lugar de los circuitos físicos;
- La PSTN no puede crear y desarrollar prestaciones con la rapidez suficiente. La arquitectura actual de la PSTN no permite a los fabricantes escribir nuevas aplicaciones, lo que es un limitante pues no todas las necesidades se encuentran totalmente satisfechas;
- Los datos, la voz y el vídeo no pueden converger en la PSTN con la arquitectura actual, sería necesario que todos los abonados tengan acceso a una banda ancha de alta velocidad, como una línea digital, el cable o inalámbrico, para permitir esta convergencia;
- La arquitectura construida para la voz no es suficientemente flexible para transportar datos, pues las características de transmisión no permiten hacer cambios que mejoren la calidad de audio.

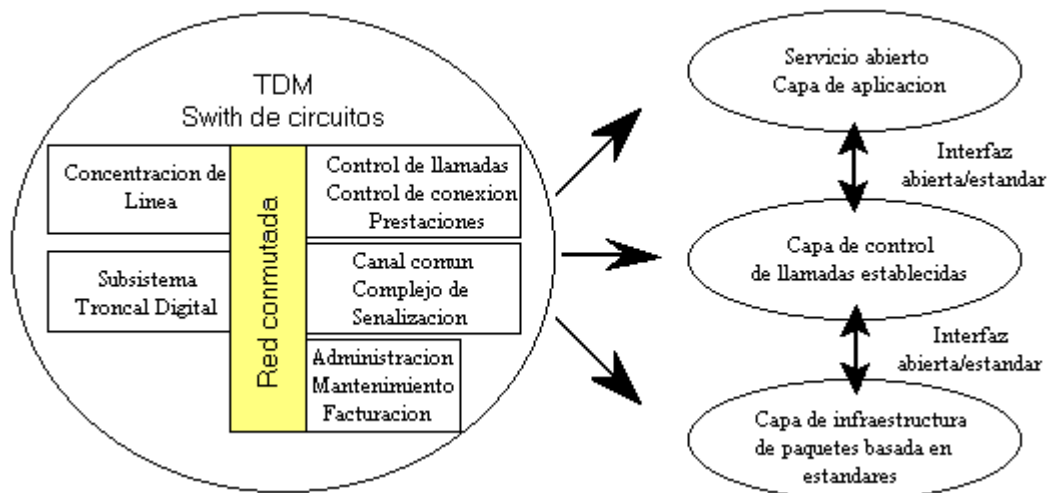
3.3 NUEVO MODELO DE INFRAESTRUCTURA DE RED PSTN

El nuevo modelo de infraestructura de una red PSTN incluye el desarrollo de una red de telefonía basada en paquetes en lugar de una basada de circuitos conmutados.

La integración de Datos, Voz, Vídeo (D/V/V) es más que un simple cambio en la infraestructura. La integración abre el desarrollo de aplicaciones a miles de fabricantes de software independientes. Esta integración se puede comparar con el cambio desde los computadores mainframe donde unos pocos fabricantes desarrollaban aplicaciones, hasta la computación cliente / servidor donde múltiples fabricantes desarrollan aplicaciones para sistemas distribuidos.

El modelo de circuito conmutado se está rompiendo en un nuevo modelo mediante el cual existen estándares abiertos en tres capas:

- Capa de infraestructura de paquetes que transportará la voz actual (medios);
- La capa de control de llamada será separada de la capa de medios ; y,
- Capa de aplicación (API, interfaz de programación de aplicaciones) que permitirá crear nuevos servicios de múltiples fabricantes de software independientes.



Con este nuevo modelo, la infraestructura de paquetes sustituye a la infraestructura de circuitos. Esta infraestructura será IP, aunque este modelo también funciona si ATM es el transporte subyacente e IP discurre en la parte superior.

Capítulo 4 Investigación sobre IP

Muchos de los beneficios que brinda la VoIP vienen de la utilización del protocolo IP como su mecanismo de transporte. Para tener una idea más clara del funcionamiento y características del protocolo IP es necesario primeramente familiarizarse con el modelo OSI.

4.1 MODELO OSI (OPEN SYSTEM INTERCONNECTION)

Este modelo OSI fue desarrollado por la ISO (International Organization for Standardization) a principios de los ochenta, y se ha convertido en un estándar para el desarrollo de protocolos que permiten a las computadoras comunicarse entre sí.

“Nota: ISO es una organización internacional fundada para fomentar la cooperación en los desarrollos tecnológicos, especialmente en el campo de las comunicaciones. Por su parte la ITU-T es una organización global que crea estándares para todas las áreas de las comunicaciones analógicas o digitales internacionales. ITU-T trabaja con los estándares de las telecomunicaciones.”
(Configuración de Routers Cisco, Pag. 4)

El modelo OSI divide en siete capas la comunicación entre dos computadores, cada capa solo se ocupa de hablar con su correspondiente en la máquina receptora, a su vez proporciona servicios a su capa superior y exige determinados servicios de su capa inferior. De esta forma cada una de las capas maneja una parte específica de información, realiza los cambios que sean necesarios a los datos y agrega las funciones necesarias antes de pasar los datos a la siguiente capa, estos datos mientras pasan por cada una de las capas se van transformando hasta llegar a ser 0 y 1 en la capa física.



Modelo OSI

4.1.1 Capa de Aplicación

Esta es la capa con la que se relacionan la mayoría de los usuarios de computadores, ya que en éstas se encuentran aplicaciones conocidas para los usuarios como:

- Procesadores de Textos;
- Correo Electrónico;
- Browser (Navegadores Web);
- Juegos.

4.1.2 Capa de Presentación

La capa de presentación tiene como función principal la de asegurar que la información enviada por la capa de aplicación sea legible por la misma capa en el computador receptor, en el caso de ser necesario esta capa también se encarga de traducir entre múltiples formatos de datos para que tengan un formato común de representación, también se encarga de las estructuras de datos utilizadas por los programas para la transferencia de datos para la capa de aplicación.

4.1.3 Capa de Sesión

Esta capa se encuentra encargada de establecer, administrar y terminar sesiones entre aplicaciones, estas sesiones consisten en el diálogo entre dos o más entidades de presentación.

La capa de sesión sincroniza el diálogo entre las entidades de la capa de presentación, administra el intercambio de datos, regula las conversaciones, ofrece provisiones para la expedición de datos, clase de servicio y el registro de problemas de la capa de sesión, presentación y aplicación.

4.1.4 Capa de Transporte (Capa Host – Host)

La capa de transporte se encarga de asegurar una transmisión fiable de los datos a través de una red, para lo cual utiliza un control de flujo, confirmación extremo a extremo, verificación de errores (suma de comprobación), secuencia de datos y la retransmisión. El protocolo TCP (Transmisión Control Protocol) posee mecanismos para administrar

congestión, éste ajusta su temporizador de transmisión cuando detecta congestión o se pierden paquetes en la red, con este temporizador TCP reduce la cantidad de tráfico que envía, la congestión viene determinada porque no se reciben acuses de recibo desde el nodo de destino.

4.1.5 Capa de Red

La capa de red nos proporciona la dirección lógica que permite que dos sistemas que se encuentran en redes lógicas diferentes encuentren un posible camino para comunicarse, en esta capa se encuentran los protocolos de enrutamiento. En Internet la dirección IP es el esquema más utilizado.

Los protocolos de enrutamiento como:

- EIGRP (Enhanced Interior Gateway Routing Protocol, o IGRP mejorado);
- OSPF (Open Shortest Path First) Primero la ruta libre más corta;
- BGP (Border Gateway Protocol) Protocolo de gateway fronterizo;
- IS-IS (Intermediary System to Intermediary System) Sistema intermedio – sistema intermedio;

Y otros se utilizan para determinar el mejor camino entre dos subredes lógicas. Los routers tradicionales enrutan paquetes IP sobre la base de su dirección de la capa de red.

Las principales funciones de la capa de red son:

- Formateo de paquetes;
- Direccionamiento de redes y hosts;
- Resolución de direcciones y enrutamiento;
- Creación y mantenimiento de tablas de enrutamiento.

4.1.6 Capa de Enlace de Datos

La capa de enlace de datos esta encargado de proporcionar un paso fiable a través del enlace físico, posee su propio esquema de direcciones y se ocupa de la conectividad física y transporta tramas sobre la base de la dirección de la capa de enlace. Los switches normales ethernet conmutan su tráfico de red sobre la capa de enlace, el realizar esta labor

sobre la capa 2 se conoce como bridging (puentear) y de hecho un switch es un puenteador de alta velocidad con varias interfaces.

4.1.7 Capa Física

La capa física se encarga de crear en unos y ceros en el medio físico para la transmisión de la información con cambios de impulso eléctricos, para esto se utilizan especificaciones de comunicación comunes como las siguientes:

- EIA/TIA-232 (Electrical Industries Association / Telecommunications Industry Association) Asociación de Industrias Electrónicas/Asociación de la Industria de las telecomunicaciones, por lo general se utiliza para la comunicación de dispositivos de computadora como módems, se puede utilizar con diferentes tipos de conectores;
- V.35 (ITU-T, International Telecommunications Union Telecommunication Standardization Sector) es un mecanismo de sector de la normalización de las telecomunicaciones de la Unión Internacional de las telecomunicaciones, que define la velocidad desde 19.2 Kbps a 1,544 Mbps, es una interfaz física con un conector de 34 pines también conocido como Winchester Block;
- RS-449. Es un conector de 37 pines y es mucho mejor que el RS-232.

4.2 PROTOCOLO DE INTERNET (IP)

Es un protocolo que reside en la capa tres (capa de red), es decir no tiene mecanismos de fiabilidad, control de flujo, secuenciación o reconocimiento. El protocolo TCP se puede alojar en la capa superior del IP, capa cuatro (capa de sesión) y pueden agregar los diferentes mecanismos anteriormente mencionados.

El protocolo IP en el modelo OSI no tiene que tratar con problemas de enlace de datos comunes como Ethernet, ATM (Modo de Transferencia Asíncrono), Frame Relay y Token Ring o con cuestiones físicas como SONET (Red Óptica Sincrónica), cobre y Fibra Óptica. Las capas inferiores son independientes a las aplicaciones que se pongan en IP, las aplicaciones que residen sobre IP experimentan largos períodos de silencio seguidos de una necesidad de una gran porción de ancho de banda.

Existen tres maneras generales para dirigir un paquete IP que proporcionan a cada paquete una etiqueta con la dirección destino:

- Unidifusión.- Identifica una sola dirección específica y únicamente ese modo envía el paquete a las capas superiores del modelo de referencia OSI. Permite que dos estaciones se comuniquen con independencia de su ubicación física;
- Difusión.- En este mecanismo los paquetes son enviados a todos los usuarios de la subred local, las difusiones pueden atravesar puentes y swiches pero no routers a menos que se encuentren configurados para esto. Se utiliza para comunicarse con todo aquel que se encuentra en una subred simultánea;
- Multidifusión.- Los paquetes utilizan una gama de direcciones la cual puede llegar a un grupo de usuarios que se encuentran en diferentes subredes. Permite aplicaciones como videoconferencia que tiene un transmisor y múltiples receptores.

4.3 DIRECCIONES DE LA CAPA DE ENLACE (MAC)

Las direcciones de la capa de enlace son conocidas también como MAC (Media Access Control). Las direcciones MAC y las direcciones de la capa física son únicas para cada dispositivo. Esta dirección va grabada en memoria ROM en el hardware de la tarjeta de red y es única e inalterable. El IEEE (Institute of Electrical and Electronics Engineers, desarrolla estándares en el área de ingeniería eléctrica e informática) se encarga de administrar las direcciones; cada fabricante de tarjetas o equipos puede comprar un rango de direcciones IEEE.

La dirección MAC se compone de 48 bits. El primer bit de la dirección indica el ámbito del envío: 0 – Envío unicast (dirigida a un ordenador), 1 – Envío multicast (a un grupo de ordenadores), cuando toda la dirección está a unos se trata de una trama broadcast.

Si en la transmisión de datos utilizamos un switch Ethernet LAN el tráfico es enrutado en base a la dirección MAC, si utilizamos un HUB el paquete se transmite a todos los puertos, con independencia de la dirección MAC pues el envío se hace sobre la base de una capa física.

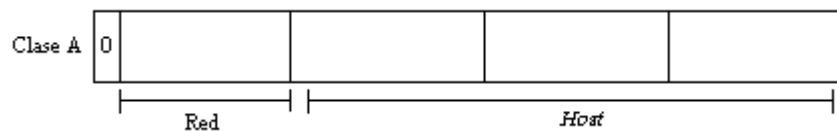
4.4 DIRECCIONES IP

La Dirección IP identifica a la interfaz de red de cada nodo. La dirección IP es única y utiliza 32 bits para su representación. Tienen estructura jerárquica, una parte de la dirección corresponde a la red y otra al host dentro de la red.

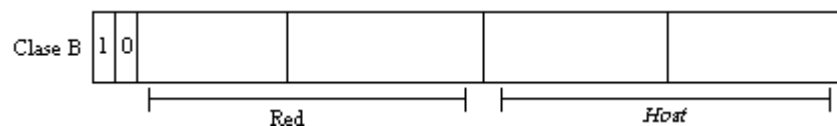
Las direcciones IP suelen representarse por cuatro números decimales separados por puntos que equivalen al valor de cada uno de los cuatro bytes que componen la dirección.

La dirección IP soporta cinco clases de red, los bits que se encuentran más a la izquierda indican la clase de red:

- Las redes de clase A proporcionan solo 7 bits para el campo de dirección de red;



- Las redes de clase B proporcionan 14 bits para el campo de dirección de red y 16 bits para el campo de dirección de hosts;



- Las redes de clase C reserva 21 bits para el campo de dirección de red y solo 8 bits para el campo de hosts;



- Las direcciones de clase D, los cuatro primeros bits más altos están definidos por 1,1,1 y 0;
- Las direcciones de clase E están reservadas para su utilización en el futuro, los cuatro bits superiores están definidos por 1 y el quinto bit es siempre 0.

La asignación de direcciones válidas de Internet la realizan los NICs (Network Information Center).

4.5 TCP (TRANSFER CONTROL PROTOCOL)

TCP (Protocolo de Control de Transferencia) proporciona un servicio dúplex completo, mueve los datos en una corriente de bytes continua no estructurada donde los bytes se identifican mediante número de secuencia. Para el control de flujo, TCP utiliza el mecanismo que se conoce como sliding window (ventana deslizante), es decir, TCP permite que cada estación envíe múltiples paquetes antes de que llegue un acuse de recibo, cuando el acuse de recibo llega para un paquete saliente, el remitente desliza la ventana de paquetes por la corriente de bytes y envía otro paquete.

4.6 UDP (USER DATAGRAM PROTOCOL)

UDP (Protocolo de datagrama de usuario) es un protocolo sin conexión. UDP se utiliza en VoIP para transportar el tráfico de voz real, TCP no se utiliza porque no se necesitan ni el control de flujo ni la retransmisión de paquetes de audio de voz.

Si se utilizara TCP para VoIP, la latencia en la que se caería a la espera de los acuses de recibo y retransmisiones haría que la calidad de voz fuera inaceptable. (Más detalles de este protocolo se encuentra en el capítulo 6).

4.7 COMPARACIÓN ENTRE EL MODELO OSI Y TCP/IP

La concepción del modelo OSI fue diferente a la de TCP/IP, en el modelo OSI primero fue el modelo y luego los protocolos, mientras que en TCP/IP el orden fue inverso. Por esto el modelo OSI se utiliza como referencia para explicar cualquier tipo de redes ya que realiza una distinción clara entre servicios, interfaces y protocolos. Pero al momento de diseñar el modelo OSI no se tenía experiencia práctica aplicando el modelo al desarrollo de protocolos, por lo que no se tomaron en cuenta algunas funcionalidades importantes, pues,

las redes broadcast no fueron previstas inicialmente en la capa de enlace y posteriormente tuvieron que ser insertadas en la subcapa MAC; otro problema fue la interconexión de redes diferentes, que es el alma del modelo TCP/IP.

El modelo TCP/IP tiene solamente cuatro capas a diferencia del modelo OSI que como ya hemos visto tiene siete capas. En el modelo TCP/IP hay la unión de la capa física y de enlace en una oscura capa host-red, mientras que la fusión de las capas de sesión, presentación y aplicación en una sola del modelo TCP/IP es más lógica que en el modelo OSI. Los servicios orientados a conexión son otra diferencia fundamental entre estos dos modelos. El modelo OSI soporta ambos modos CONS (Servicios orientados a conexión) y CLNS (Servicios no orientados a conexión) en la capa de red, pero en la capa de transporte solo CONS que es la que percibe el usuario. En el modelo TCP/IP soporta solo CLNS en la capa de red, pero ambos en la capa de transporte. Esto se debe básicamente a que en la capa de red con el modo CONS se hace mucho más sencillo facturar por tiempo de conexión, operación que es muy común para las compañías telefónicas, que son las que participaron en los comités técnicos de ISO en el diseño del modelo OSI.

Modelo OSI	Modelo TCP/IP
Capa Física	Capa host-red
Capa de Enlace	
Capa de Red	Capa Internet
Capa de Transporte	Capa de Transporte
Capa de Sesión	Capa de Aplicación
Capa de Presentación	
Capa de Aplicación	

Pero en el protocolo TCP/IP también existen aspectos negativos, por ejemplo, no se distinguen conceptos claros de servicio, interfaz y protocolo. El modelo TCP/IP fue diseñado después del protocolo. La capa host-red es más bien una interfaz, no distingue entre la capa física y de enlace pues ésta únicamente transmite paquetes IP.

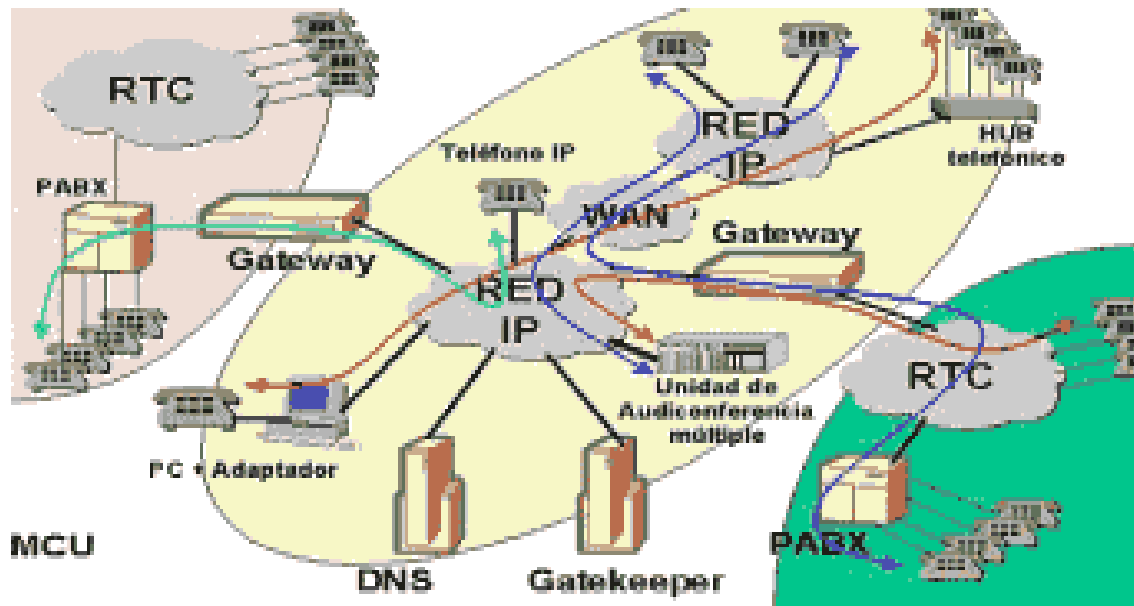
Capítulo 5 Funcionamiento de Voz sobre IP

5.1 FUNCIONAMIENTO GENERAL

La voz que ingresa por el micrófono del teléfono es convertida en paquetes de datos y se comprimen, estos paquetes se encapsulan dentro de otros con el protocolo IP para poder viajar por una red de datos (intranet o Internet), usando el protocolo UDP (UDP se explica en el Capítulo 4). Los paquetes poseen un encabezado en donde se encuentra la dirección a la que van dirigidos, esta deberá ser traducida a una dirección IP o al número de teléfono al que se quiere alcanzar. Si la comunicación se realiza hacia un teléfono de red, existen Gateways en donde los paquetes se convierten para viajar por la red de telefonía estándar y se redirigen a la central en donde se encuentra el número de destino. Al alcanzar el destino, una compuerta idéntica invierte el proceso, luego rutea la llamada desde la red IP a la PBX de la oficina filial o central a la red telefónica pública.

La calidad del sonido podrá ser superior a la que estamos acostumbrados, ya que están en continuo desarrollo los métodos que comprimen y protegen los paquetes sin la necesidad de solicitar que se reenvíen aquellos que se pierden o se dañan en el largo camino que deben transitar.

En el caso de querer comunicarse por VoIP desde un teléfono normal, se deberá marcar un código de acceso al Gateway más cercano y una vez autorizado se obtiene un tono similar al normal. Este Gateway se encarga de la digitalización, compresión y envío de los paquetes hacia otro gateway destino, el cual enviará los datos al teléfono indicado. Es importante destacar que también es posible el uso de fax y de vídeo. El resultado es que para una llamada de larga distancia solo se paga por una local.



Red VoIP

5.2 DE CONMUTACIÓN DE CIRCUITOS A CONMUTACIÓN DE PAQUETES.

La PSTN ó Red Telefónica Conmutada (RTC), se basa en la conmutación de circuitos. La conmutación de circuitos establece la conexión extremo a extremo sólo durante el tiempo necesario. Para transmitir datos se utiliza la misma red que para la transmisión de voz, mediante el uso de módems u otros adaptadores. La PSTN comprende tres redes diferentes:

- La Red de Telefonía Básica (RTB) o POTS (Plain Old Telephone Service). Está formada por las líneas analógicas tradicionales. Requiere el uso de módems para la transmisión de datos;
- La Red Digital de Servicios Integrados (RDSI). Es una tecnología orientada a conexión que usa la telefonía digital para digitalizar voz, datos, vídeo y otro tipo de información a través de la línea telefónica existente;
- La Red GSM (Global System for Mobile Communications). Se forma de conexiones digitales de radioenlaces.

Existen ciertos inconvenientes con la conmutación de circuitos, como:

- Pueden no haber circuitos libres para establecer la conexión;

- No se garantiza que se aproveche todo el ancho de banda asignado;
- El servidor debe tener una conexión física para cada circuito.

Estos inconvenientes fueron superados al crear redes con circuitos virtuales (VC, Virtual Circuit), es decir se mantiene una sola conexión física a la red y sobre ella varios circuitos virtuales con equipos remotos. Todos los paquetes de datos relacionados con la llamada siguen la misma ruta a través de la red, con lo que nos aseguramos que los datos llegan al destino en el mismo orden que se enviaron. Al terminar la transferencia de datos, se finaliza la llamada. Es necesario disponer de equipos que puedan hacer la distribución de los paquetes en función de su destino, y por esto a estas redes se las denominan redes de conmutación de Paquetes.

La subred de una red de conmutación de paquetes se constituye mediante conmutadores unidos entre sí por líneas dedicadas. La distribución de los conmutadores y la topología de la red lo decide el proveedor del servicio.

El ***switching de Paquetes*** es un método de transmisión de datos que envía los datos en unidades de longitud variable, también llamadas paquetes. Frame Relay y X.25 utilizan switching de Paquetes. La tecnología de switching de paquetes está orientada a conexión.

ATM y el Servicio de datos multimegabit conmutado (Switched Multimegabit Data Service, SMDS), convierten los datos de los paquetes en celdas de longitud fija y realizan relay de celda. El ***relay de celda*** es un método de transmisión de datos que envía datos en pequeñas unidades de tamaño fijo, también llamadas celdas que pueden procesar el hardware de una manera rápida y eficaz.

X.25 y Frame Relay no son apropiadas para tráfico de multimedia porque el retardo y el jitter son impredecibles cuando la red esta cargada. Estas redes por lo general son demasiado lentas, sobretodo X.25.

La tecnología ATM (Asynchronous Transfer Mode) está diseñada para manejar varios tipos de servicios de red entre los que se incluyen voz, vídeo y datos en una única red digital. ITU-T se basó en el estándar Red digital de servicios integrados de banda ancha que se diseñó inicialmente para enviar voz, vídeo y datos a través de una red pública. ATM proporciona servicios tanto orientados a conexión como sin conexión.

5.3 REDES ORIENTADAS Y NO ORIENTADAS A CONEXIÓN.

Para transmitir Voz sobre IP de buena calidad se necesita transmitir en tiempo real, pues cualquier alteración en la llegada de los paquetes puede variar sus características, por lo que se requiere de redes que ofrezcan un alto grado de servicio y garanticen el ancho de banda necesario.

Existen dos tipos de redes en cuanto a la conexión:

- Las redes orientadas a la conexión; y,
- Las redes no orientadas a la conexión.

En las redes que son ***orientadas a la conexión***, se negocia y establece al inicio de la comunicación, la ruta que han de seguir todos y cada uno de los paquetes y se reserva un determinado ancho de banda. Estas redes ofrecen las características necesarias para la transmisión de voz e imagen, es decir ofrecen un alto grado de servicio y se garantiza el ancho de banda.

En las ***redes no orientadas a conexión*** se realiza el llamado "mejor esfuerzo" para entregar los paquetes, pero cada uno y en función del estado de los enlaces puede seguir una ruta distinta, por lo que el orden secuencial se puede ver alterado, lo que se traduce en una pérdida de calidad. A los paquetes enviados en un servicio no orientado a conexión se les denomina datagramas.

El tipo de servicio que ofrece una red (*orientado a conexión o no orientado a conexión*) está dado en función a su arquitectura, es decir en como cada capa se comunica con su correspondiente del otro extremo.

En las redes IP (IP "Internet Protocol" reside en la capa de red del modelo OSI o en la capa host-red del modelo TCP/IP), con TCP se garantiza la integridad de los datos.

En las redes IP, con UDP (datagrama) se proporciona un servicio de entrega no garantizado.

Sin embargo, como se vio en el Capítulo 4, TCP no se utiliza porque no se necesitan ni el control de flujo ni la retransmisión de paquetes de audio de voz. Si se utilizara TCP para VoIP, la latencia en la que se caería a la espera de los acuses de recibo y retransmisiones haría que la calidad de voz fuera inaceptable.

Ninguno de estos protocolos (TCP, UDP) puede proporcionar el soporte de aplicaciones en tiempo real como la voz.

Existe una serie de protocolos que intentan proporcionar servicios en tiempo real sobre IP como son RTP (Real time Transport Protocol), RTCP (Real time Control Protocol), RSVP (Resource Reservation Protocol) y RTSP (Real time Streaming Protocol), sin embargo es H.323 el protocolo internacional que da la base para la transmisión de voz, datos y vídeo sobre redes no orientadas a conexión y que no ofrecen un grado de calidad del servicio, como son las basadas en IP, incluida Internet.

5.4 ASPECTOS A CONSIDERAR EN VOIP

La tecnología VoIP tiene muchos aspectos a considerar, los mismos que pueden afectar a las redes de conmutación de paquetes:

5.4.1 Retraso / Latencia

El retraso o latencia se define como el tiempo que tarda la voz desde que es emitida hasta llegar al oído del que está escuchando.

En las redes de telefonía actuales existen tres tipos de retraso: retraso de propagación, retraso de manejo y el retraso de serialización.

5.4.1.1 Retraso de propagación:

Es causado por la velocidad de la luz en la fibra óptica o las redes de cobre, aunque este retraso es casi imperceptible junto con los retrasos de manejo puede provocar una degradación apreciable de la voz.

5.4.1.2 Retraso de manejo:

Es causado por los dispositivos que transmiten la trama a través de la red, también se lo conoce como retraso de procesamiento y tiene diferentes causas: empaquetado, compresión y switching de paquetes.

5.4.1.3 Retraso de serialización:

Es la cantidad de tiempo que se tarda en colocar un bit o byte en una interfaz. La influencia de este retraso es relativamente pequeña.

Además de los mencionados existen retrasos que afectan a una red basada en paquetes y éstos son: switching de paquetes y retraso de la gestión de colas.

5.4.1.4 Switching de paquetes:

Este tipo de retraso hace referencia al tiempo que se necesita para mover un paquete hasta la cola de salida.

5.4.1.5 Retraso de gestión de colas:

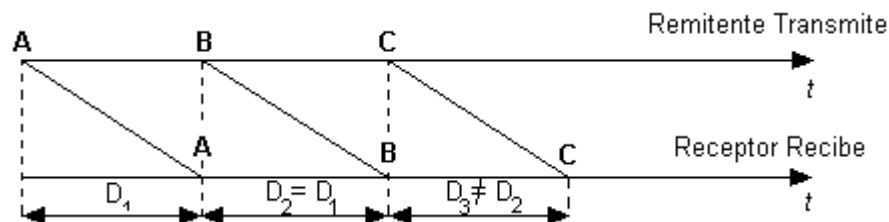
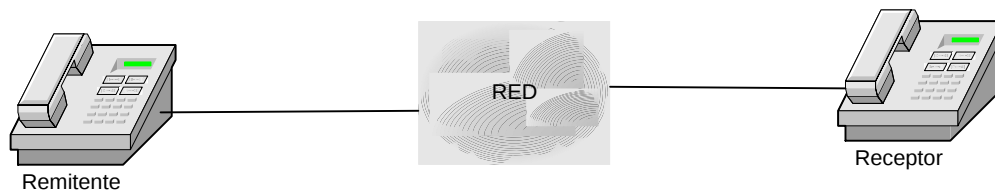
Este retraso se da cuando los paquetes son guardados en una cola debido a la congestión en una interfaz outbound (de salida). Este tipo de retraso ocurre cuando se han enviado más paquetes de los que la interfaz puede manejar en un intervalo de tiempo determinado.

Según la especificación G.114 de la ITU-T recomienda un retraso no mayor a los 150 ms (milisegundos) extremo a extremo para mantener una buena calidad de voz. En redes no administradas y congestionadas el retraso en la gestión de colas puede llegar a agregar más de 2 segundos en la transmisión extremo a extremo o provocar que el paquete se caiga, este período es inaceptable en las redes de voz.

Las redes de satélite tienen un retraso inherente de unos 500 ms. Esto incluye 250 ms para llegar al satélite y otros 250 ms para volver a la Tierra. La pérdida de paquetes en estas redes es muy controlada pues tienen un amplio ancho de banda.

5.4.2 Fluctuación de Fase

La fluctuación de fase (jitter) es la variación del tiempo de llegada de un paquete, existe solo en redes basadas en paquetes. Cuando un paquete de voz es enviado en un intervalo de tiempo regular y no llegan en el mismo intervalo a la estación receptora por retrasos dados en la red es lo que se llama fluctuación de fase.



Fluctuación de Fase

En el ejemplo anterior se puede ver que el tiempo que se tarda en enviar y recibir los paquetes A y B es el mismo ($D_1 = D_2$). El paquete C tiene un retraso en la red y se recibe después de la hora a la que se le esperaba. Por esta razón es necesario un búfer de fluctuación de fase que oculta el retraso.

5.4.3 Modulación por impulsos codificados

La comunicación analógica es la ideal para la comunicación humana, sin embargo la transmisión analógica se ve perjudicada por el ruido de la línea. El ruido puede afectar la forma de la onda y producir una recepción desvirtuada. Al generar las señales analógicas como muestras digitales, es decir utilizar bits “unos” y “ceros” para representar la señal, se hizo mucho más fácil separar las muestras digitales del ruido de la línea. Las ventajas de la representación digital originaron que la red telefónica migre a la modulación por impulsos codificados (PCM). (PCM se explicó en el punto 1.2.2 Señales de voz digitales).

5.4.4 Compresión de Voz

PCM y ADPCM son técnicas de compresión de voz que se basan en la forma de onda. Existen nuevas técnicas que emplean procedimientos de procesamiento de señales que comprimen la voz enviando sólo información paramétrica simplificada sobre vibración y modulación de la voz original, necesitando menos ancho de banda para transmitir esa información. Estas técnicas se conocen como códecs de origen y son las siguientes: codificación con predicción lineal (LPC, Linear Predictive Coding), la compresión de predicción lineal con excitación por código (CELP, Code Excited Linear Prediction Compresión) y la MP-MLQ (Multipulse, Multilevel Quantization).

ADPCM (Adaptive Differential Pulse Code Modulation) ó modulación por impulsos codificados diferencial y adaptable, es un método de compresión que a diferencia de la PCM que codifica directamente la amplitud de la voz, ADPCM codifica las diferencias de la amplitud de la voz y la velocidad de cambio de esa amplitud. (PCM se explicó en el punto 1.2.2 Señales de voz digitales).

5.4.5 ECO

El eco se produce cuando la voz del emisor impacta con un desajuste de impedancia u otro entorno causante del eco, y se refleja de nuevo hacia el mismo, el eco llegará al emisor varios milisegundos después de haber hablado.

El eco tiene dos inconvenientes: puede ser alto y puede ser largo. Cuando más alto y largo es el eco, más incómodo resultara.

La mayoría de redes telefónicas analógicas utilizan supresores de eco, pero esto resulta ser un inconveniente, pues la Red Digital de Servicios Integrados (RDSI) no se puede utilizar sobre una línea que tiene supresor de eco, porque éste corta el radio de acción de la frecuencia que utiliza la RDSI.

Actualmente para las redes basadas en paquetes, existen los canceladores de eco que funcionan de la siguiente manera:

El dispositivo a través del cual está hablando el usuario A (router A) guarda una imagen inversa de las palabras del usuario A durante un cierto tiempo. Es lo que se llama voz

inversa (inverse speech)(-G). El cancelador de eco oye el sonido que viene del usuario B y sustrae el $-G$ para eliminar todo el eco.

Cisco realiza toda la cancelación de eco en su DSP, otros fabricantes incluyen en el software la cancelación de eco.

Es importante configurar la cantidad apropiada de cancelación de eco cuando se instala inicialmente el equipamiento de VoIP. Si no se configura la suficiente cancelación de eco, los que llaman escucharán el eco durante la llamada. Si se configura demasiada cancelación de eco, el cancelador de eco tardará más tiempo en converger y eliminar el eco.

5.4.6 Pérdida de Paquetes

La pérdida de paquetes es muy común en las redes de datos, y muchos protocolos utilizan esta información para reducir el número de paquetes de datos que están enviados.

Cuando se transmite voz en redes de datos, es importante que el transporte se realice con éxito y oportunamente, lo que hace pensar en algún mecanismo para hacer que la voz sea resistente a la pérdida periódica de paquetes.

La implementación de VoIP de Cisco Systems permite al router de voz responder a la pérdida periódica de paquetes. Si el paquete de voz no es recibido en el tiempo que se esperaba, se considera como perdido y se vuelve a repetir el último paquete recibido. Como el paquete perdido sólo tiene 20 ms de voz, el oyente medio no aprecia la diferencia en la calidad de voz.

5.4.7 Detección de Actividad de Voz

Cuando se establece una conversación normal, donde una persona habla y la otra escucha, se pierde por lo menos el 50% del total del ancho de banda, pues las redes actuales contienen canales bidireccionales de 64 Kbps (con independencia de si alguien está hablando o no). La cantidad de ancho de banda que se pierde puede ser mayor si se toman en cuenta las interrupciones y pausas normales de voz de una persona.

En VoIP, este ancho de banda “perdido” puede ser utilizado para otros propósitos cuando está habilitada la detección de la actividad de Voz. El VAD (Voice Activity Detection) Detección de la actividad de voz, funciona detectando la magnitud de la voz en decibelios

(dB) y decidiendo cuándo debe dejar la voz de poner tramas de voz en los paquetes. Cuando la VAD detecta una disminución en la amplitud de la voz espera un determinado tiempo que se conoce como hangover y que suele ser de 200 ms antes de dejar de poner las tramas.

La VAD tiene dos problemas considerables:

1. No distingue la voz del ruido de fondo, esto se conoce también como **el umbral de señal a ruido**; y,
2. Otro problema es determinar cuando finaliza y empieza la voz, lo que hace que el principio de una frase sea cortada o recortada. Este fenómeno se conoce como **recorte de voz frontal** (front-end speech clipping) que es imperceptible para la persona que escucha.

5.4.8 Conversión Digital a Analógico

Muchas de las conversaciones son digital/analógicas (D/A) es decir intervienen en esa llamada redes digitales y analógicas. Cuando se convierte la señal de digital a analógica y viceversa, la voz o forma de onda es menos verdadera. Una conversación D/A debe estar estrictamente administrada en un entorno de voz comprimido.

Las redes toll actuales (redes de larga distancia) puede manejar por lo menos siete conversiones D/A antes de que la calidad de voz se vea afectada.

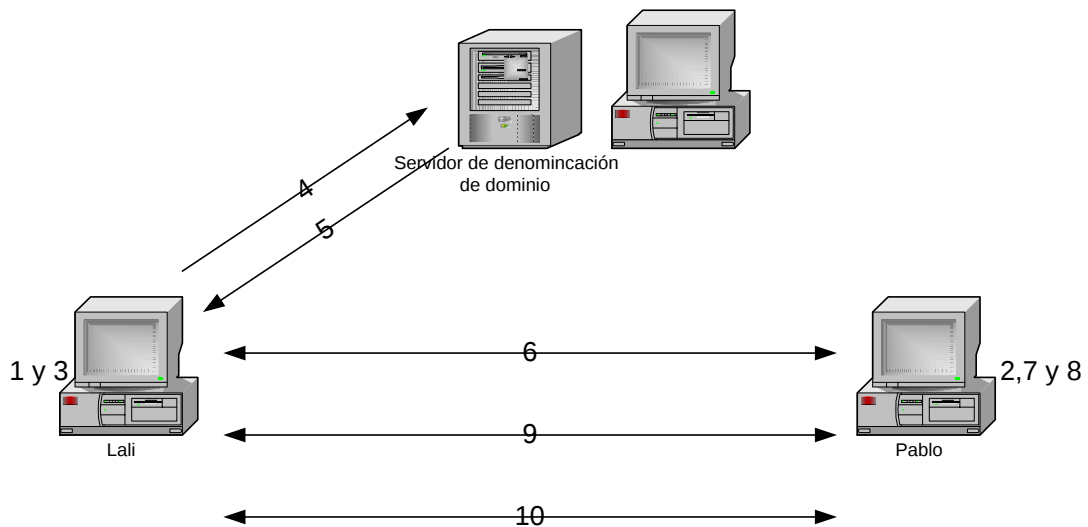
A pesar de que las conversiones D/A afectan a todas las redes de voz, las redes VoIP que utilizan un códec PCM (G.711) son resistentes a estos problemas.

5.4.9 Codificación Tándem

En el modelo jerárquico de la PSTN los switches más altos de la jerarquía se llaman switches tándem, tal como se vio en el Capítulo 1. Estos switches conectan switches de capa inferior.

Los switches tándem deben descomprimir la voz que llega y volver a comprimir para enviarla, por lo que la calidad de ésta se verá drásticamente afectada. Esta compresión y descompresión no es común en la PSTN pero deberá ser planificada y diseñada en redes de paquetes.

La degradación de la voz se da cuando se tiene más de un ciclo compresión/descompresión en cada llamada telefónica.



Jerarquía de switching tándem.

Esta figura muestra tres switching de circuitos separados para transportar una llamada de voz. En este caso no hay degradación de voz ya que se utilizan dos switches TDM y un switch tándem con canales de 64 Kbps.

5.4.10 Protocolos de Transporte

Por el Protocolo de Internet (IP) se desplazan dos tipos de tráfico: UDP (Protocolo de Datagrama de Usuario) y TCP (Protocolo para el control de la transmisión). Para el transporte de voz se utiliza UDP/IP, pero como la transmisión en tiempo real es una característica necesaria en la transmisión de voz, la Internet Engineering Task Force (IETF) adoptó el RTP. VoIP circula en la parte superior del RTP, que circula a su vez en la parte superior del UDP. Por tanto, VoIP es transportado con una cabecera de paquete RTP/UDP/IP.

5.4.10.1 RTP (Real-time Transport Protocol)

RTP es el protocolo estándar para transmitir tráfico sensible al retraso por las redes basadas en paquetes. RTP recorre la parte superior del UDP e IP. El RTP utiliza dos bits de

información para indicar la secuencia y la marca de temporización. La secuencia sirve para determinar si los paquetes están llegando en orden y la marca de temporización se utiliza para determinar el tiempo de llegada entre los paquetes (fluctuación de fase).

RTP consta de una parte de datos y una parte de control llamada Protocolo de Control RTP (RTCP).

La parte de datos es un protocolo limitado que proporciona soporte para aplicaciones con propiedades de tiempo real, como medios continuos (audio y vídeo), incluida la reconstrucción de la temporización, la detección de pérdidas y la identificación de contenidos.

RTCP proporciona soporte para conferencias en tiempo real de grupos de cualquier tamaño dentro de Internet.

Versión	IHL	Tipo de Servicio	Longitud total			
Identificación			Indica- ciones	Compensación de fragmentos		
Tiempo de existencia		Protocolo	Suma de verificación de la cabecera			
Dirección de origen						
Dirección de destino						
Opciones				Relleno		
Puerto de origen			Puerto de destino			
Longitud			Suma de verificación			
V=2	P	X	CC	M	PT	Número de secuencia
Marca para la temporización						
Identificador de origen de sincronización (SSRO)						

Cabecera de RTP.

Existen algunos inconvenientes en el uso del RTP para el tráfico en tiempo real. Las cabeceras IP/RTP/UDP tienen 20, 8, 12 bytes respectivamente esto se agrega a una cabecera de 40 bytes que es dos veces más grande que la carga útil cuando se utiliza G.729 con dos muestras de voz (20ms).

Se puede comprimir esta gran cabecera 2 o 4 bytes utilizando la Compresión de cabecera RTP (CRTP, Header Compression).

5.4.10.2 RUDP (Reliable User Data Protocol)

El RUDP, Protocolo de datos de usuario Fiable, incorpora fiabilidad el protocolo UDP, sin necesidad de tener un protocolo basado en la conexión. El método de RUDP consiste en enviar múltiples copias del mismo paquete y permitir que la estación receptora descarte los paquetes innecesarios o redundantes, con esto al menos un paquete debería llegar al receptor. Esto se conoce como corrección de errores hacia delante (FEC). Al momento de implementar el FEC se debe considerar el ancho de banda, pues se utiliza el doble o triple cantidad mayor de ancho de banda. FEC es un mecanismo que mejora la fiabilidad y la calidad de voz.

5.4.11 Diseño de plan de marcación

Para evitar problemas en el momento de integrar redes (redes dispares), considere las siguientes recomendaciones dentro de su empresa cuando diseñe el plan de marcación:

- Planes para crecer, Integración con otras redes;
- Coste de los circuitos dedicados o VPN;
- Coste del equipamiento adicional para paquetes de voz;
- Superposición de número (cuando más de un sitio tienen el mismo número de teléfono);
- Flujo de llamadas (los patrones de llamada desde cada sitio);
- Hora punta (la hora en la que se ofrece el mayor número de llamadas en un circuito).

El plan de marcación puede ir de 2 a 8 dígitos dependiendo del tamaño de la compañía.

5.5 CALIDAD DE SERVICIO EN VOIP

Calidad de Servicio (QoS) hace referencia tanto a la clase de servicio (CoS) como al tipo de servicio (ToS). El objetivo básico es conseguir el ancho de banda y la latencia necesarios para una aplicación determinada.

Una CoS (Clase de servicio) permite al administrador de la red agrupar diferentes flujos de paquetes, tendiendo cada uno requisitos de latencia y ancho de banda diferentes.

Un ToS es un campo en la cabecera del IP que permite que tenga lugar una clase de servicio. Un campo ToS utiliza tres bits, lo que permite agrupar ocho flujos de paquetes o CoS (0-7).

Tal como se explicó VoIP tiene algunos problemas a los que QoS puede ayudar a solucionar, como son: la pérdida de paquetes, la fluctuación de fase, el retraso de manejo, el retraso de propagación, el retraso de códec, el retraso de muestreo y el retraso de digitalización.

La ITU-T en su recomendación G-114 sugiere que no haya más de 150 milisegundos (ms) de retraso de extremo a extremo para mantener una “buena” calidad de voz.

A continuación se describen algunas herramientas utilizadas para conseguir la necesaria QoS para un usuario o aplicación:

5.5.1 Ancho de Banda

Dependiendo de qué códec se esté utilizando y de cuántas muestras de voz se quiera por paquete, la cantidad de ancho de banda por llamada puede incrementarse drásticamente.

Códec	Ancho de banda consumido	Ancho de banda consumido con cRTP(Cabecera de 2 Bytes)	Latencia de muestra
G.729 w / una 10ms muestra/Trama	40kbps	9,6kbps	10ms
G.729 w / cuatro 10ms muestras/trama	16kbps	8,4kbps	40ms
G.729 w / dos 10ms muestras/trama	24kbps	11,2kbps	20ms
G.711 w / una 10ms muestra/trama	112kbps	81,6kbps	10ms
G.711 w / dos 10ms muestras/trama	96kbps	80,8kbps	20ms

Se debe tener en cuenta que una llamada puede consumir diferentes cantidades de ancho de banda dependiendo de qué capa de enlace de datos se utiliza (Ethernet, Frame Relay, PPP, etc.).

C RTP es un esquema de comprensión que permite comprimir la cabecera de 40 bytes (IP/RTP/UDP) a 2 ó 4 bytes. Reduce a 2 bytes cuando las sumas de verificación de UDP no se utilizan ó 4 bytes cuando se utilizan las sumas de verificación UDP.

5.5.2 Gestión de Colas

La gestión de colas del tipo FIFO (Primero en entrar, primero en salir) fue la primera que se utilizó en los routers y sigue utilizándose actualmente, dependiendo de la topología de la red.

Sería muy útil tener herramientas de gestión de colas que permitan al administrador de la red especificar qué tipo de tráfico es “especial” o importante y organizar la cola de tráfico en base a esta información en lugar del orden de llegada de los paquetes. Cisco provee una técnica conocida como WFQ (Weighted Fair Queuing, Gestión de colas apropiada ponderada) que consiste en utilizar múltiples colas para separar los flujos y concede a cada flujo la misma cantidad de ancho de banda, evitando que una aplicación en particular (ejemplo FTP) consuma todo el ancho de banda disponible. Otra técnica es la CQ (Custom Queuing, Gestión de colas personalizada), permite que los usuarios especifiquen un porcentaje de ancho de banda disponible para un protocolo determinado. PQ es otra técnica (Gestión de colas por prioridad) y permite que el administrador de la red configure cuatro prioridades de tráfico: alta, normal, media y baja. El tráfico de la cola de prioridad alta es atendido hasta que la cola esté vacía, luego se transmiten los paquetes que están en la cola de prioridad siguiente.

5.5.3 Clasificación de paquetes

Precedencia IP: El campo ToS de la cabecera IP permite ocho tipos de CoS diferentes que se enumeran a continuación:

Tipo de Servicio	CoS
Rutina	0
Prioridad	1
Inmediato	2
Flash	3
Flash-Override (Ignorar Flash)	4
Crítica	5
Internet	6
Red	7

La precedencia IP (ToS) permite al router agrupar flujos de tráfico y administrarlos sobre la base de estas 8 configuraciones, es el mecanismo QoS más utilizado en las redes de gran escala.

- **Políticas de Enrutamiento:** Las políticas de enrutamiento permiten configurar una norma definida para los flujos de tráfico y no tener que depender completamente de los protocolos de enrutamiento para determinar el envío del tráfico y el enrutamiento. Las normas pueden estar basadas en las direcciones IP, en los números de puerto, en los protocolos o en el tamaño de los paquetes.
- **RSVP (Protocolo de configuración de reserva de recursos)** permite que los puntos finales señalen la red con el tipo de QoS necesario para una aplicación determinada.

5.5.4 Fragmentación

La fragmentación divide los paquetes grandes (1.500 bytes de MTU (unidad máxima de transmisión)) en paquetes más pequeños para que puedan desplazarse en menor tiempo en enlaces de ancho de banda bajos (768 kbps y menos). Esta fragmentación se lleva a cabo en la capa 2 o 3 del modelo de referencia OSI.

La fragmentación no es suficiente para eliminar el problema de la latencia en circuitos de ancho de banda bajo. El router debe también ser capaz de gestionar la cola sobre la base de fragmentos o paquetes más pequeños en lugar de por el paquete original (antes de ser fragmentado). Cisco Systems permite que los usuarios modifiquen el número de muestras por paquete, lo que es muy importante porque permite determinar el tamaño de la fragmentación necesaria.

Capítulo 6 El Estándar VOIP H.323

6.1 ESTÁNDAR VOIP

En mayo de 1996 un grupo de fabricantes de equipos VoIP fundaron la IMTC (International Multimedia Teleconferencing) pues sintieron la necesidad de ofrecer una interoperabilidad completa de sus productos con estándares abiertos. La interoperabilidad consiste en definir los criterios de un modelo abierto que permita a los fabricantes poder establecer comunicación de servicios de voz sobre IP en Internet sin importar la marca del equipo, ya que existen fabricantes tecnológicos que emplean técnicas propietarias de codificación de voz, supresión de silencios, manejo de llamadas, direccionamiento y planes de marcación, etc.

A finales de 1997 el VoIP forum del IMTC ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP.

El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como:

- Cancelador de eco y supresión de silencio integrados;
- Codificación de la voz y direccionamiento;

Establece nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Voice Switching para el ruteo de llamadas en la red. Plan de marcación flexible. Servicios de directorio y Transmisión de señalización por tonos multifrecuencia (DTMF).

Entre los principales protocolos de control de llamadas VoIP están los siguientes:

- H.323 es la recomendación de la ITU-T más implementado;
- SGCP (Simple Gateway Control Protocol) ó Protocolo de control de gateway simple, fue desarrollado a principios de 1998 para reducir el coste de los puntos finales (gateways) al hacer que el control de llamadas inteligente tuviera lugar en una plataforma centralizada (o controlador de gateway);
- El IDPC (Internet Protocol Device Control) ó Protocolo de control de dispositivo del protocolo Internet, es muy similar al SGCP y añade más mecanismos para las operaciones, administración, gestión y disposiciones (OAM&P, operations, administration, management, and provisioning) que el SGCP;
- El MGCP lanzado a finales de 1998 en lugar de los dos anteriores (SGCP, IDPC), es básicamente el protocolo SGCP con algo de OAM&P;
- SIP ó Protocolo de Inicio de la Sesión, es un protocolo que permite crear, modificar y terminar sesiones con uno o más participantes. Estas sesiones multimedia incluyen audio, vídeo y datos y pueden incluir múltiples participantes.

6.2 ESTÁNDAR H.323

El H.323 es una familia de estándares definidos por la ITU-T para las comunicaciones multimedia a través de una red de Protocolo Internet (IP), incluida la propia Internet. Está definido específicamente para redes de conmutación de paquetes (PBN, Packet Based Networks) que no puedan proveer una calidad de servicio. Entre las redes basadas en paquetes se incluyen Redes de Área Local, Redes de Área Empresarial, Redes de Área Metropolitana, Intra-Networks e Inter-Networks (incluyendo Internet). Además se incluyen conexiones dial-up o conexiones punto a punto sobre GSTN o ISDN que utilicen un protocolo de transporte basado en paquetes como el PPP.

Las redes pueden ser segmentos simples de red o pueden tener topologías muy complejas. Algunos ejemplos son TCP/IP e IPX sobre Ethernet, Fast Ethernet, Token Ring, FDDI, ATM. La tecnología de red más común en la que se está implementando H.323 es IP (Internet Protocol).

El H.323 define los siguientes componentes más relevantes:

- Terminal;
- GateWay (interfaces de telefonía con la red);
- Gatekeeper (componentes de conmutación ínter oficina);
- Controladores Multipunto (MC, Multipoint Controllers);
- Procesadores Multipunto (MP, Multipoint Processors);
- Unidad de Control Multipunto (MCU, Multipoint Control Units).

El H.323 sugiere además la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet. En la actualidad, se están proponiendo otras especificaciones en los consorcios industriales tales como SIP, MGCP, las cuales ofrecen ampliaciones en lo que respecta al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.

Aunque se hable del H.323 como de un estándar, el ITU lo considera una recomendación, como cualquier recomendación de un origen similar, está abierta a la interpretación de diferentes fabricantes. Una ventaja es que deja libertad a los fabricantes para implementar capacidades que cumplan con los requerimientos de aplicaciones especiales.

6.3 HISTORIA DEL H.323

Con anterioridad al H.323, el ITU se enfocó exclusivamente en la estandarización de las redes globales de telecomunicaciones. Por ejemplo, en 1985 se comenzó el trabajo en la especificación que define el envío de imagen y voz sobre redes de circuitos conmutados, tales como RDSI. La ratificación de la norma (H.320) tuvo lugar 5 años después (fue aprobada por el CCITT en Diciembre de 1990). Sólo 3 años después se dispuso de equipos que cumplieran con la norma y que permitieran la interoperabilidad entre sí.

En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores propuso la creación de un nuevo estándar ITU-T para incorporar videoconferencia en la LAN. Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo hubo de contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

El H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local, metropolitana, regional o de área extensa. Soporta así mismo Internet e Intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para "los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada".

Nótese que H.323 también soporta videoconferencia sobre conexiones punto a punto, telefónicas y RDSI. En estos casos, se debe disponer un protocolo de transporte de paquetes tal como PPP.

El H.323 puede verse como una extensión del H.320, pues utiliza los mismos algoritmos de compresión para el vídeo y el audio, aunque introduce algunos nuevos como el T.120 para la colaboración de datos. El H.323 fue diseñado específicamente con las siguientes ideas:

Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931;

- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real;
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

El H.323 toma muchas ventajas frente al H.320, muchas de ellas resultan del comportamiento inherente al tráfico de paquetes y su forma de ser transmitidos; otras resultan de mejoras en las técnicas de compresión y señalización. El H.323 es un modelo más orientado a red mientras que el H.320 se centra en los puntos terminales.

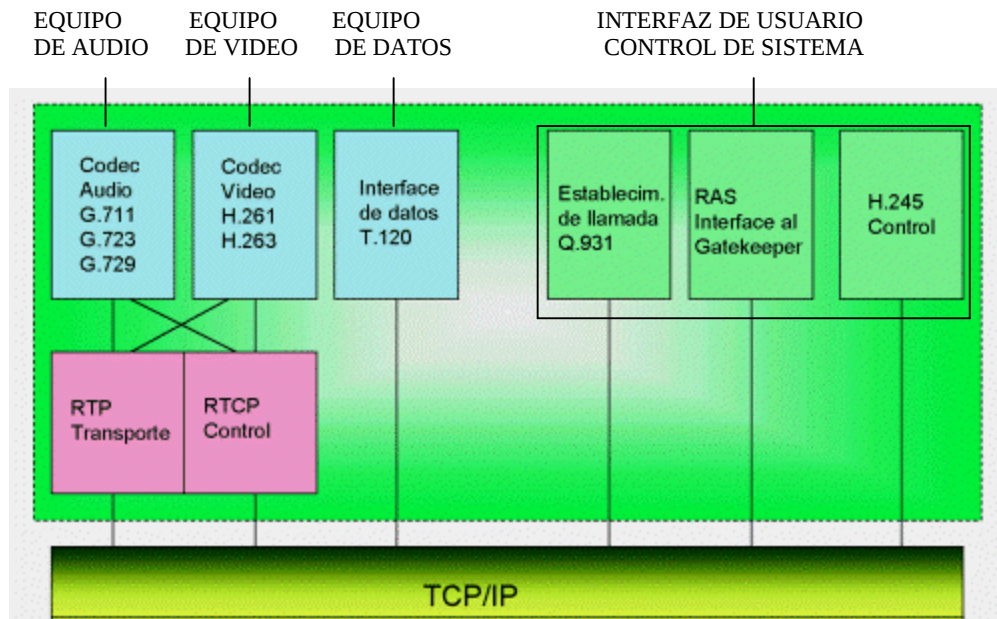
En algunos casos la tecnología H.320 deberá convivir con la H.323. En aplicaciones donde la LAN no es suficientemente robusta o el acceso IP es problemático, los sistemas basados en RDSI y H.320 serán la elección adecuada. Los fabricantes de equipos disponen ya de arquitecturas donde el mismo equipo puede ser utilizado en un entorno RDSI/H.320 o integrado en otro H.323 cuando la aplicación lo recomiende. Esta posibilidad es doblemente interesante por la garantía que nos ofrece al salvaguardar nuestra inversión a largo plazo y por permitirnos centrarnos en los requerimientos de nuestra aplicación con independencia de la tecnología.

Tabla: Normativa de la UIT para conferencia multimedia sobre redes LAN y WAN.					
	H.320	H.321	H.322	H.323	H.324
Fecha	1990	1995	1995	1996	1996
Red	RDSI-BE	RDSI-BA ATM LAN	PSTN X.25	LAN Ethernet	RTB (POTs)
Vídeo	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263	H.261 H.263
Audio	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.728	G.711 G.722 G.723 G.728 G.729	G.723
Tasa de Audio kbps	64, 48-64	64, 48-64, 16	64, 48-64, 16	64, 48-64, 16, 8, 5.3/ 6.3	8, 5.3/ 6.3
Datos	T.120	T.120	T.120	T.120	T.120
Multiplexación	H.221	H.221	H.221	H.225	H.223
Control	H.230 H.242	H.242	Hc.230 H.242	H.245	H.245
Multipunto	H.231 H.243	H.231 H.243	H.231 H.243	H.323	
Interface de comunicaciones	I.400	AAL I.363 I.400	TCP/IP I.400	TCP/IP	Módem V.34

6.4 ARQUITECTURA H.323

El H.323 consta de los siguientes componentes y protocolos:

Función	Protocolo
• Establecimiento de Llamada	Q.931
• Señalización de Llamadas	H.225
• Control de Medios	H.245
• Compresión de Voz	G.711, G.722, G.723, G.728, G.729
• Compresión de Vídeo	H.261, H.263
• Compartir datos	T.120
• Transporte de medios	RTP
• Control de Transmisión	RTCP



Ámbito de H.323 Relaciones entre los componentes de H.323

6.4.1 Definiciones

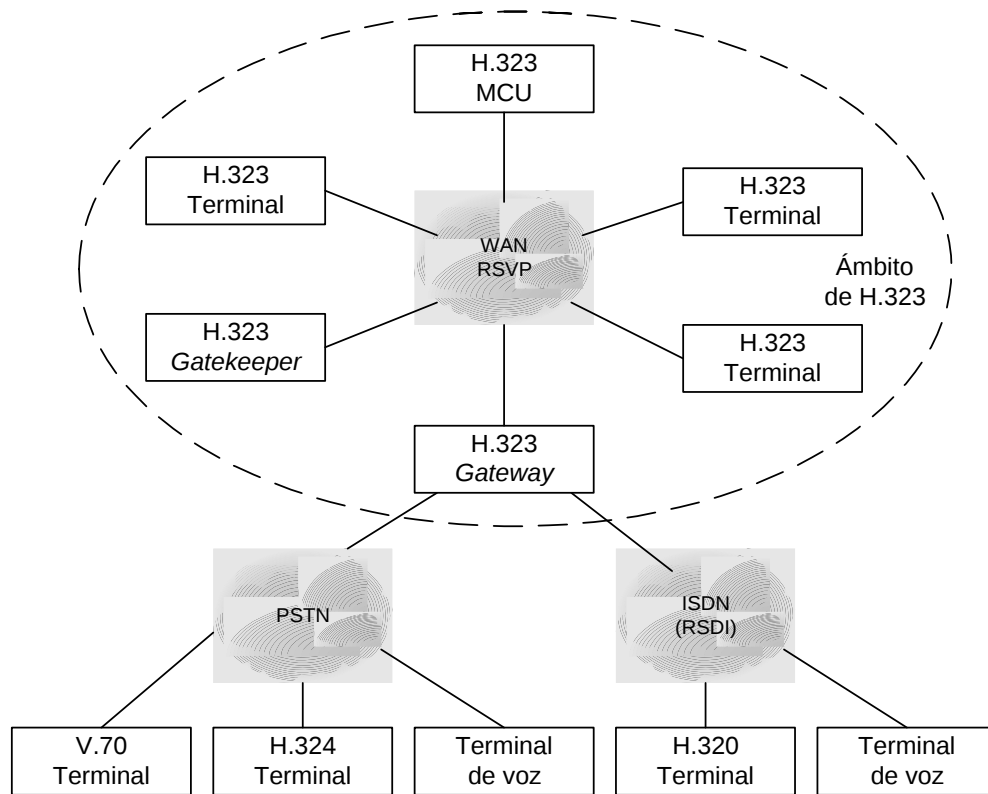
Entidad. La especificación H.323 define el término genérico entidad como cualquier componente que cumpla con el estándar.

Extremo. Un extremo H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

Zona (Zone). Es el conjunto de Gatekeeper y Puntos Finales registrados en una llamada.

6.4.2 Componentes definidos en H.323

La especificación define cuatro componentes principales para un sistema de comunicaciones en red: Terminales, Gateways, Gatekeepers y MP, MU, MCUs.



Elementos de networking H.323

6.4.2.1 Terminales

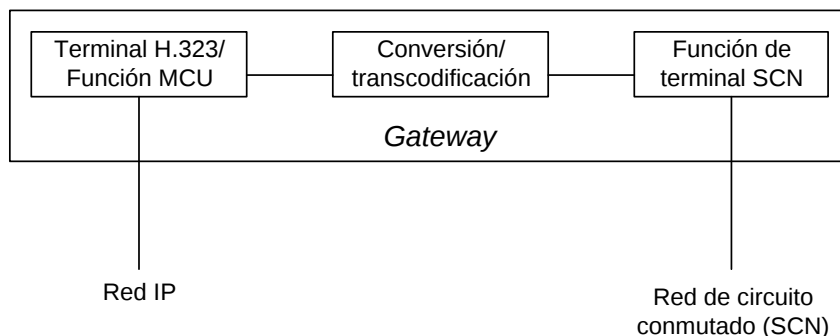
Son los clientes finales en la LAN. Es un extremo que proporciona una comunicación bidireccional en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Todos los terminales deben soportar la comunicación de voz, mientras que la de vídeo y datos son opcionales. Concretamente, deben ser capaces de codificar y decodificar audio en el algoritmo G.711. Para adaptarse a las necesidades de las diferentes redes, especialmente en conexiones con poco ancho de banda, un terminal debe ser capaz de codificar y decodificar la voz usando otros diferentes algoritmos. Si un terminal soporta la codificación de vídeo, el único modo exigido es el H.261 en resolución QCIF (Quarter Comment Intermediate Format). Más allá de este punto, un terminal puede soportar otros modos de vídeo con algoritmos propietarios o estándares. Si la compartición de datos está presente debe cumplir la norma T.120.

Además, deben soportar la norma H.245 que se emplea para la negociación del uso del canal y sus prestaciones; Q.931 para el establecimiento de la llamada y la señalización; RAS (Registration/ Admission/Status), un protocolo utilizado para la comunicación con el Gatekeeper y sólo si éste está presente en la red; soporte para RTP/RTCP (Real-time

Transport Protocol/Real-time Transport Control Protocol) que fija la secuencia de los paquetes de audio y vídeo. Opcionalmente los terminales pueden incorporar un códec para vídeo, conferencia de datos según T.120 y MCU (Multipoint Control Unit). Otro protocolo del IETF, aunque no es parte del H.323, el RSVP (Resource Reservation Protocol) se emplea para solicitar la reserva de un determinado ancho de banda y otros recursos, a lo largo de toda la red, para una conferencia y obtener la confirmación sobre si es posible hacerla, algo esencial si se quiere mantener una videoconferencia sobre una LAN.

6.4.2.2 Gateway (GW)

Un gateway H.323 (GW) es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. Es un elemento opcional en una conferencia H.323, que proporciona muchos servicios incluida la adaptación con otras normas del UIT. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa. En otras palabras, nos servirá de pasarela entre el entorno de vídeo sobre IP H.323 y el entorno vídeo sobre RDSI H.320.



Elementos de un gateway H.323.

6.4.2.3 Gatekeeper (GK)

El Gatekeeper es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

6.4.2.4 MC (Controlador Multipunto)

El Controlador Multipunto es una entidad que soporta conferencias entre tres o más puntos finales en una conferencia multipunto. Los MC transmiten el conjunto de capacidades para cada punto final en la conferencia multipunto y pueden revisar las capacidades durante la conferencia. El MC no realiza mezcla ni conmutación de audio, vídeo o datos. La función MC puede residir en un terminal, gateway, gatekeeper o MCU.

6.4.2.5 MP (Procesador Multipunto)

El procesador multipunto es la entidad que recibe audio, vídeo y/o flujos de datos y los distribuye a los puntos finales que participan en una conferencia multipunto (multiconferencia). El hardware y software de los MP mezclan, conmutan y procesan el audio, vídeo y/o los datos de los participantes.

6.4.2.6 MCU (Multipoint Control Units)

La Unidad de Control Multipunto es un extremo y está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

La comunicación bajo H.323 contempla las señales de audio y vídeo. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo el estándar T.120 que permite la compartición de aplicaciones en conferencias punto a punto y multipunto.

6.4.2.7 Servidor Proxy H.323

El servidor proxy H.323 es un proxy específicamente diseñado para el protocolo H.323. El proxy actúa en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los proxies pueden determinar el destino de una llamada y realizar la conexión si se desea. Un Proxy H.323 proporciona seguridad, por lo que únicamente el tráfico H.323 pasa por el mismo.

Los terminales que no soportan el Protocolo RSVP (Recourse Reservation Protocol) se pueden conectar a través de un acceso o redes de área local (LAN) con una calidad de servicio (QoS) relativamente buena con el proxy.

Los proxies soportan el enrutamiento del tráfico H.323 separado del tráfico de datos ordinarios a través de un enrutamiento de aplicación específico (ASR, Application-Specific Routing).

6.5 ESTÁNDARES Y PROTOCOLOS DEL H.323

Establecimiento de llamada y Control						
Presentación						
Direccionamiento		Compresión de audio G.711 ó G.723			DTMF	Direcciona- miento
RAS(H.225)	DNS	RTP/RTCP			H.245	Q.931 (H.225) DNS
Transporte UDP					Transporte TCP	
Red (IP)						
Enlace						
Físico						

El H.323 comprende una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación y que se describen a continuación:

6.5.1 Protocolos de Direccionamiento

6.5.1.1 RAS ó Señalización de registro, admisiones y estado (Registration, Admission and Status)

RAS es un protocolo de comunicaciones definido en la UIT-T H.225.0 que proporciona un control de prellamadas en las redes basadas en gatekeeper H.323.

RAS permite a una estación H.323 localizar otra estación H.323 a través del Gatekeeper (Controlador de accesos), el RAS se define entonces como *“El canal no fiable para registro, admisiones y mensajería de situación”*.

El canal RAS se establece entre puntos finales y gatekeepers. El canal RAS es independiente de la señalización de control de llamadas y de los canales de transporte de

medios, este canal establece una conexión no fiable (UDP) que transporta los mensajes RAS que realizan el registro, las admisiones, los cambios del ancho de banda, el estado y los procedimientos de desenganche.

Para iniciar una llamada primero se envía una petición de **admisión** (mensaje RAS) obligatorio por el canal RAS, seguida por un mensaje **Establecimiento** (mensaje Q.931) inicial en una dirección de transporte de canal fiable (esta dirección puede haber sido devuelta en el mensaje de *confirmación* o *admisión* o puede haberle resultado conocida al terminal llamante). A continuación comienza una secuencia de establecimiento de comunicación con mensajes Q.931 (Ver protocolo de señalización H.225) y la secuencia se completa cuando el terminal recibe en el mensaje **Conexión** una dirección de transporte fiable en la cual se enviarán los mensajes de control H.245 (Ver protocolo H.245).

Después de establecer el canal de control H.245 fiable, pueden establecerse canales lógicos adicionales para audio, vídeo y datos dependiendo de las capacidades de los terminales.

Los terminales deben ser capaces de enviar audio y vídeo utilizando RTP a través de canales no fiables para minimizar el retardo. Puede aplicarse ocultación de errores u otra acción de recuperación para superar la pérdida de paquetes; en general, los paquetes de audio/vídeo no se retransmiten, pues se originaría así un retardo excesivo en el entorno de la red de paquetes. Se debe tener muy claro que el audio/vídeo y la señalización de llamada/control H.245 nunca se envían por el mismo canal y no comparten una estructura de mensaje común. Todos los canales lógicos H.245 son unidireccionales, excepto los asociados con T.120, que son bidireccionales.

	Fiable o no fiable
Audio/RTP	No fiable
Audio/RTCP	No fiable
Vídeo/RTP	No fiable
Vídeo/RTCP	No fiable
Señalización de llamada	Fiable
H.245	Fiable
Datos (T.120)	Fiable
RAS	No fiable

6.5.1.1.1 Definiciones:

Dirección de Red (Network Address). Para cada entidad H.323 se asigna una dirección de red que identifica únicamente a esa entidad dentro de la red. Un punto final debe utilizar diferentes direcciones de Red para diferentes canales en una misma llamada.

Dirección Alias (Alias Address). El Alias provee un método alternativo de direccionamiento para un punto final. Este podría ser una dirección e-mail, un número de teléfono, o algo similar. Un punto final puede tener uno o más alias asociados con éste y es único dentro de una zona.

Identificador TSAP. Para cada dirección de Red, cada entidad H.323 puede tener diversos identificadores TSAP. El identificador TSAP permite multiplexar diversos canales compartiendo la misma dirección de red.

Esquema URL H.323. Uno de los tipos de alias definidos por H.323 es el URL-ID. El URL H.323 ayuda a resolver la dirección de una entidad a otra entidad H.323. Se compone de dos partes: el usuario y el Hostport. El usuario especifica el alias de la entidad y el hostport es el nombre del dominio del Punto Final, Gatekeeper o Extremo.

6.5.1.1.2 Mensajes RAS

Los mensajes RAS realizan el registro, las admisiones, los cambios del ancho de banda, el estado y los procedimientos de desenganche.

Descubrimiento

Un punto final puede descubrir el gatekeeper con el que debe registrarse a través de un proceso manual o automático. En el método manual, los puntos tienen en su configuración la dirección IP del gatekeeper y pueden conectarse únicamente con éste. En el método automático la relación entre los puntos finales y los gatekeepers pueden cambiar a lo largo del tiempo y requieren de un mecanismo conocido como autodescubrimiento, que consiste en descubrir al gatekeeper a través de un mensaje de multidifusión.

Los mensajes RAS utilizados para el autodescubrimiento del gatekeeper H.323 son los siguientes:

- *GRQ (Gatekeeper Request), Petición de Controlador de Acceso.* Mensaje de multidifusión enviado por el punto final que está buscando al gatekeeper;
- *GCF (Gatekeeper Confirm), Confirmación de Controlador de Acceso.* Respuesta a un GRQ, que indica la dirección de transporte del canal RAS del gatekeeper;
- *GRJ (Gatekeeper Reject), Rechazo de Controlador de acceso.* Mensaje en el que se indica al punto final que el gatekeeper no quiere aceptar su registro.

Registro

Es el proceso a través del cual los gateways, puntos finales y MCU alcanzan una zona e informan al gatekeeper sus direcciones IP y sus alias. Este proceso ocurre después del descubrimiento y es necesario para poder realizar las llamadas. Los mensajes utilizados para que un punto final registre o cancele registros son los siguientes:

- *RRQ (Registration Request), Petición de Registro.* Es un mensaje de requerimiento enviado desde el punto final a la dirección del canal RAS;
- *RCF (Registration Confirm), Confirmación de Registro.* El gatekeeper envía este mensaje confirmado un registro de punto final;
- *RRJ (Registration Reject), Rechazo de Registro.* El gatekeeper envía este mensaje cuando rechaza el registro de punto final;
- *URQ (Unregistration Request), Petición de desregistro.* El punto final o gatekeeper envían este mensaje para solicitar la cancelación de un registro;
- *UCF (Unregistration Confirm), Confirmación de desregistro.* El punto final o gatekeeper envían este mensaje para confirmar la cancelación de un registro;
- *URJ (Unregistration Reject), Rechazo de deregistro.* Indica que el punto final no estaba preregistrado con el gatekeeper.

Localización de punto final

Los puntos finales y los gatekeepers utilizan la localización de punto final para obtener la información de contacto cuando solo se dispone la información del alias. El gatekeeper responsable del punto final solicitado responde indicando su propia información de contacto o la información de contacto del punto final. Se utilizan los siguientes mensajes:

- *LRQ (LocationRequest), Petición de localización.* Solicita información de contacto del punto final o gatekeeper;
- *LCF (LocationConfirm), Confirmación de localización.* Contiene la dirección del canal RAS o del canal de señalización de llamadas;
- *LRJ (LocationReject), Rechazo de localización.* Indica que el punto final solicitado no está registrado o tiene recursos no disponibles.

Admisiones

Los gatekeepers son los que autorizan el acceso a las redes H.323 confirmando o rechazando una petición de admisión. En la petición de admisión se incluye el ancho de banda solicitado y éste puede ser reducido por el gatekeeper en la confirmación. Los mensajes utilizados son los siguientes:

- *ARQ (Admission Request), Petición de admisión.* El punto final intenta iniciar una llamada;
- *ACF (Admission Confirm), Confirmación de admisión.* Autorización del gatekeeper para admitir la llamada;
- *ARJ (Admission Reject), Rechazo de Admisión.* Negación de la petición de admisión.

Información de estado

El gatekeeper puede utilizar el canal RAS para monitorear si el punto final está (online) o no está en línea (offline) debido a una condición de fallo. Normalmente el período de sondeo es cada 10 de segundos. Otra forma de monitoreo, es solicitar en el ACF que el punto final envíe mensajes de estado periódicos durante la llamada. Mensajes utilizados:

- *IRQ (Information Request), Petición de información.* Se envía al punto final que solicita el estado;
- *IRR (Information Request Response), Respuesta a petición de información.* Es la respuesta al mensaje IRQ;
- *Status Enquiry:* Se utiliza para verificar el estado de una llamada entre puntos finales y viaja por el canal de señalización de llamadas.

Control de ancho de banda

El ancho de banda se establece inicialmente en la petición de admisión, sin embargo este ancho de banda suele cambiar durante una llamada utilizando los siguientes mensajes:

- *BRQ (Petición de anchura de banda), Petición de anchura de banda.* Solicita un incremento o disminución de ancho de banda;
- *BCF (BandwidthConfirm), Confirmación de anchura de banda.* Confirmación a la petición del cambio de ancho de banda;
- *BRJ (BandwidthReject), Rechazo de anchura de banda.* Rechazo a la petición del cambio de ancho de banda.

Resumen de mensajes RAS

- ACF Confirmación de admisiones (*admissions confirm*)
- ARJ Rechazo de admisiones (*admissions reject*)
- ARQ Petición de admisiones (*admissions request*)
- BCF Confirmación de anchura de banda (*bandwidth confirm*)
- BRJ Rechazo de anchura de banda (*bandwidth reject*)
- BRQ Petición de anchura de banda (*bandwidth request*)
- DCF Confirmación de desligamiento (*disengage confirm*)
- DRJ Rechazo de desligamiento (*disengage reject*)
- DRQ Petición de desligamiento (*disengage request*)
- GCF Confirmación de controlador de acceso (*gatekeeper confirm*)
- GRJ Rechazo de controlador de acceso (*gatekeeper reject*)
- GRQ Petición de controlador de acceso (*gatekeeper request*)
- IACK Acuse de recibo de petición de información (*information request acknowledgement*)
- INAK Acuse de recibo negativo de petición de información (*information request negative acknowledgement*)
- IRQ Petición de información (*information request*)
- IRR Respuesta a petición de información (*information request response*)
- LCF Confirmación de localización (*location confirm*)
- LRJ Rechazo de localización (*location reject*)
- LRQ Petición de localización (*location request*)
- RAC Confirmación de disponibilidad de recurso (*resource availability confirmation*)
- RAI Indicación de disponibilidad de recurso (*resource availability indication*)
- RCF Confirmación de registro (*registration confirm*)
- RIP Petición en curso (*request in progress*)
- RRJ Rechazo de registro (*registration reject*)
- RRQ Petición de registro (*registration request*)
- SCI Indicación de control de servicio (*service control indication*)
- SCR Respuesta de control de servicio (*service control response*)
- UCF Confirmación de desregistro (*unregistration confirm*)
- URJ Rechazo de desregistro (*unregistration reject*)
- URQ Petición de desregistro (*unregistration request*)

6.5.1.2 DNS (Domain Name Service). Servicio de Nombres de Dominio

Cuando un controlador de acceso (gatekeeper) viene especificado en un URL para hacer su descubrimiento se utiliza DNS.

6.5.1.2.1 Protocolo de Servicio de nombre de dominios - DNS

Un servidor DNS convierte un nombre lógico en su respectiva dirección IP, esto se logra pues técnicamente el DNS es una inmensa base de datos distribuida jerárquicamente por toda la Internet formando un árbol estructurado. Existen infinidad de servidores que interactúan entre sí para encontrar y facilitar a las aplicaciones de clientes la traducción de un nombre a su dirección de red IP asociada. Cada parte de la base de datos está replicada en al menos dos servidores, lo que asegura una debida redundancia.

Elementos de un DNS

El DNS tiene tres principales componentes:

- El Domain Name Space (Espacio de Nombres de Dominio) y Resource Records (Registros Fuente). El espacio de nombres de dominio es un árbol estructurado, cada nodo del árbol corresponde a un conjunto de recursos. Cada nodo tiene un nivel, el primer nivel tiene el valor nulo y es reservado para la raíz (root). El nombre del dominio de cada nodo es una lista de etiquetas que describe el camino desde el nodo hasta la raíz del árbol. Por convenio se estableció que las etiquetas que componen el nombre del dominio son impresas o leídas de izquierda a derecha, desde el más específico (el más lejano a la raíz) al menos específico (el más cercano a la raíz). Los Registros Fuente (RRs, Resource Records), es un conjunto de información asociada a un nodo;
- NAME SERVERS (Servidores de Nombres), son programas servidores que contienen información acerca de la estructura del árbol de dominios y su conjunto de información. Un servidor de nombres puede almacenar estructuras o un conjunto de información de cualquier parte del árbol de dominio, pero en general un servidor de nombres tiene información completa de un subconjunto del espacio de dominios y apunta a otros nombres de servidores que pueden ser usados para dirigir la información desde cualquier parte del árbol. El servidor de nombres conoce la parte del árbol de dominios de la cual tiene información completa; un

nombre de servidor es entonces una autoridad para esa parte del espacio de nombres. La información autoritaria esta organizada dentro de unidades llamadas Zonas, y esas zonas pueden automáticamente distribuirse hacia otros servidores de nombres con el propósito de obtener redundancia. Un dominio con gran número de máquinas puede dividirse en subdominios. La diferencia entre zona y dominio radica en que la primera solo incluye las máquinas del dominio, en cambio un dominio incluye todas las máquinas y subdominios de éste; y,

- RESOLVERS (Solucionadores) son programas que extraen la información del servidor de nombres en respuesta a un requerimiento de un cliente. Un solucionador debe ser capaz de acceder al menos a un servidor de nombres y usar la información de este servidor de nombres para responder una pregunta directamente, o delegar la consulta a otro servidor de nombres. La resolución es una rutina típica que está directamente accesible por el programa del usuario, no es necesario un protocolo entre el solucionador y el programa del usuario.

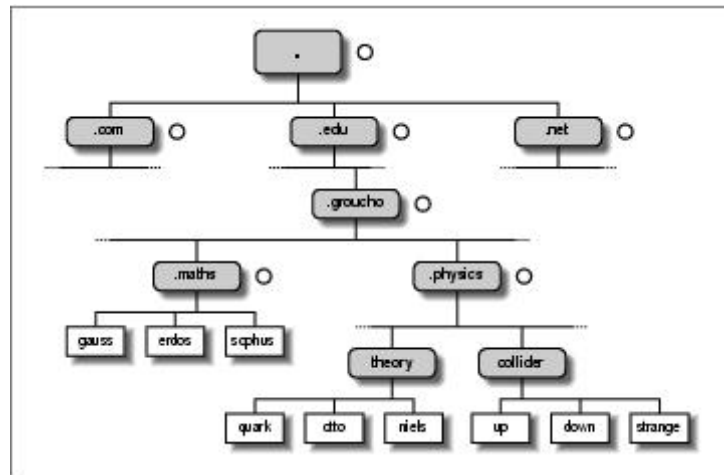
Estos tres componentes responden a tres niveles o puntos de vistas:

- Desde el punto de vista del usuario, el sistema de dominios es accedido a través de un simple procedimiento o llamado del sistema operativo hacia un solucionador local. El dominio de espacios consiste en un árbol simple y el usuario puede requerir información desde cualquier sección del árbol;
- Desde el punto de vista del solucionador, el sistema de dominios está compuesto por un número desconocido de servidores de nombres. Cada servidor de nombres tiene una o más piezas del árbol global de datos, pero el solucionador mira cada una de estas bases de datos estáticas;
- Desde el punto de vista del servidor de nombre, el dominio consiste de conjuntos separados de información local llamado zonas. El servidor de nombres tiene una copia local de algunas de estas zonas. El servidor de nombres periódicamente debe refrescar estas copias desde los archivos maestros o desde los servidores remotos. El servidor de nombres debe tener procesos concurrentes de consulta para acceder desde los solucionadores.

Una dirección DNS puede ser *relativa* o *totalmente cualificada* (fully qualified). Una dirección totalmente cualificada conocida también con las siglas FQDN incluye todos los

niveles y es única a nivel mundial. Una dirección relativa puede ser convertida al añadir la información del servidor local.

En la siguiente figura vemos una parte del espacio de nombres. La raíz del árbol, que se identifica con un punto sencillo, es lo que se denomina dominio raíz y es el origen de todos los dominios. Para indicar que un nombre es FQDN, a veces se termina su escritura en un punto. Este punto significa que el último componente del nombre es el dominio raíz.



En un nombre totalmente cualificado, la etiqueta del final (la más significativa) puede ser de una de estas tres clases:

arpa

Es usada para traducciones inversas, es decir que a partir de direcciones IP obtiene la dirección de dominio totalmente cualificada. Si todo está apropiadamente configurado una consulta para 1.4.220.134.in-addr.arpa devolverá sunc.scit.wlv.ac.uk.

Código de tres letras

El DNS fue originalmente introducido en Estados Unidos y el componente final era utilizado para identificar el tipo de organización. Algunas de estas tres letras del final de la etiqueta (edu, gov, mil) son utilizadas únicamente para organizaciones estadounidenses, otras pueden ser usadas en cualquier parte del mundo. Entre estas tres letras las más utilizadas son:

Dominio	Descripción
Edu	Instituciones universitarias, casi todas norteamericanas.
Com	Organizaciones comerciales.
Org	Organizaciones no comerciales. Las redes privadas UUCP suelen estar en este dominio.
Net	Pasarelas y otras redes administrativas.
Mil	El ejército norteamericano.
Gov	El gobierno norteamericano.
Uucp	Dominio para redes UUCP.

Código de dos letras

La etiqueta del final de dos letras indica la ciudad de origen. Fuera de los Estados Unidos, cada país suele tener su propio dominio de primer nivel codificado con las dos letras del país definidas en la tabla ISO-3166. Por debajo de cada dominio de primer nivel, cada país organiza los dominios a su manera.

Formato del mensaje DNS

El formato de mensaje utilizado para intercambiar consultas y respuestas entre hosts y servidores DNS esta especificado en el RFC 1035. Las consultas y respuestas pueden ser transferidas utilizando TCP o UDP. Estos conocerán los números de puerto para el servicio DNS utilizando cualquier protocolo.

El formato del mensaje DNS es el siguiente:

Bits 0-15	Bits 16-31
Identificador	Bandera
Número de pregunta	Numero de respuesta RRs
Número de Autoridad RRs	Numero de adicionales RRs
Preguntas	
Respuestas (RRs)	
Autoridad (RRs)	
Información Adicional	

RRs son Registros Recursivos

Los 16 bits bandera proveen información acerca de la consulta

- **QR bit.** 0 consulta, 1 respuesta
- **opcode** 4 bits cuyo valor significa

Valor	Significado
0	Query Standard
1	Consulta Inversa
2	Server status request

- **AA bit** Significa que el servidor es autoridad para el dominio en cuestion.
- **TC bit** Significa que el tamaño de la respuesta excede 512 bytes y solamente los primeros 512 bytes son realmente devueltos. Este es solamente usado cuando se utiliza UDP.
- **RD bit.** Si este bit no está seteado la recursión es denegada. Esto significa que si el servidor consultado no puede responder la consulta en lugar de pasar a la autoridad más alta y retornar el resultado que recibe, éste simplemente retornará un listado de otros servidores a examinar.
- **RA bit.** Si este bit es seteado por el servidor consultado entonces éste indica que puede manejar recursividad.
- **3 bits** que no son usados y están a cero.
- **4 rcode bits.** Que indican los siguientes estatus:

Valor	Significado
0	No error
1	Consulta mal formulada
2	Fallo Servicio
3	Nombre no existe
4	Tipo de consulta no es soportada por el servidor
5	El servidor rehúsa responder

Después de los 12 bytes de la cabecera el mensaje de consulta consiste de un bloque de preguntas las cuales a su vez consisten de un *nombre consultado*, *tipo de consulta* y *clase de consulta*.

- **Nombre consultado (Query name)**, es el nombre del sitio, cada componente del nombre envía una secuencia de caracteres precedidos por un byte que contiene el número de caracteres del componente. El nombre termina por un byte puesto a cero.
- **El tipo de consulta (Query Type)**, indica el tipo de información requerido codificado en un campo de 16 bits. Los valores más comunes son:

Nombre	Valor	Descripción
A	1	Dirección IPv4 (32 bits)
NS	2	Nombre del Servidor
CNAME	5	Nombre Canónico
PTR	12	Registro Apuntador
HINFO	13	Información del Host
MX	15	Mail Exchange Record
TXT	16	Texto de caracteres
AAAA	28	Dirección IPv6 (128 bits)
AXFR	252	Petición para la Zona a transferir
ANY	255	Petición para todos los registros

- **Clase de consulta (Query class)**, usualmente es 1 y significa que se está consultando un dominio de Internet, otros valores pueden ser usados para diferentes direcciones de dominio.

Registro de repuesta (Response Records)

El Registro de respuesta conocido como RRs forma el cuerpo de la respuesta a una consulta DNS. Éstos son usados para las contestaciones, autorizaciones y campos con información adicional.

El formato es el siguiente:

Bits 0-15	Bits 16-31
Nombre del dominio	
Tipo	Clase
Tiempo de vida	
Resource data length	Resource data
Resource data (continuación)	

- **Nombre del dominio (domain name)** corresponde al nombre consultado.
- **Tipo (type)** es el tipo de consulta.
- **Clase (class)** si está seteado a 1 es un dominio de internet.
- **Tiempo de vida (TTL, Time to live)** es el tiempo que la información será almacenada.
- **El largo del recurso de datos (resource data length)** especifica el número de bytes del recurso de datos.

Registro de Localización de servicio (SRV)

Es un nuevo registro de recurso DNS, este es devuelto cuando el tipo de consulta es igual a 33, y permite extraer información como el número del puerto, protocolo utilizado, etc. de un dominio en particular.

El formato de este registro es el siguiente:

Service._Proto.Name TTL Class SRV Priority Weight Port Target

- **Service.** El nombre simbólico del servicio deseado. El underscore (_) al principio es para prevenir confusiones con etiquetas DNS que ocurre naturalmente.
- **Proto.** El nombre simbólico del protocolo deseado. El underscore (_) al principio es para prevenir confusiones con etiquetas DNS que ocurre naturalmente. Los valores más usuales para este campo son _TCP y _UDP.
- **Name.** El dominio al que hace referencia este RR. El SRV RR es único para ese nombre.
- **TTL. (Time to live)** tiene igual significado descrito en los Registros de Respuesta.
- **Class.** Tiene igual significado descrito en los Registros de Respuesta.

- **Priority.** Valor entre 0 y 65535 que indican la prioridad dentro host. Se deberá comenzar por la más baja y continuar con la siguiente en el orden especificado en este campo hasta encontrar el objetivo deseado. Cuando tiene la misma prioridad se utiliza el campo weight.
- **Weight.** Es un mecanismo de selección para entradas que tienen la misma prioridad.
- **Port.** Indica el número de puerto en el host de este servicio. El valor puede estar entre 0 y 65535.
- **Target.** Es el nombre del dominio.

6.5.1.2.2 Descubrimiento del controlador de acceso utilizando DNS

Un controlador de acceso (gatekeeper) se identifica mediante una dirección de transporte y un gatekeeperIdentifier (identificador de controlador de acceso), que es una cadena. Un controlador de acceso es un recurso particular en Internet, y por ello es lógico especificarlo en un localizador de recurso uniforme (URL, uniform resource locator). El protocolo formulado por el controlador de acceso es RAS, por lo que el URL para un controlador de acceso puede venir dado por:

ras://gkID@domainname

gkID (ID de controlador de acceso) es el gatekeeperIdentifier, y domain name (nombre de dominio) es un nombre del sistema de nombres de dominio (DNS, domain name system) que identifica el dominio del controlador de acceso. Se señala que no necesariamente es éste un nombre de dominio totalmente cualificado (FQDN, fully qualified domain name) con un registro A; no es preciso que este nombre de dominio tenga una interfaz de transporte física con un número IP registrado en el DNS. No obstante, si es un FQDN, es razonable insistir en que su número IP es el del controlador de acceso al que se refiere el URL. En este caso, se puede añadir un número de puerto opcional al URL:

ras://gkID@domainname:port_no.

Si no se proporciona ningún número de puerto, el valor conocido de 1719 se toma como un valor por defecto.

El caso más interesante es cuando no se trata de un FQDN, y el nombre de dominio no designa, por tanto, una dirección de transporte indicada en el DNS. El nombre de dominio puede referirse entonces a una pura "zona de autoridad del controlador de acceso". En este caso el URL no resuelve el problema de localizar el controlador de acceso, sólo proporciona un formato normalizado de la información que hay que hallar. El problema consiste en cómo producir una dirección de transporte y un gatekeeperidentifier para la señalización RAS dado el nombre de dominio de un controlador de acceso.

Indagación de registro de recursos SRV

La primera solución tiene en cuenta el hecho de que el controlador de acceso es básicamente un servicio de sistema y que la dirección de transporte de un servicio de sistema nominado se puede extraer del DNS mediante la indagación de un nuevo tipo de registro de recurso DNS, denominado registro de localización de servicio (SRV, service location record). Dado un nombre de dominio, se efectuará una indagación de registro SRV de la dirección de transporte del servicio RAS para ese dominio. El propio nombre de dominio, o el que se devuelve en la respuesta SRV, se utiliza como gatekeeperidentifier. El SRV se describe en la IETF RFC 2782.

Indagación de registro TXT

Todas las implementaciones DNS actuales soportan el registro de recurso TXT. Se trata, básicamente, de algún texto libre que puede ser devuelto para cada nombre de dominio. Es posible almacenar muchos recursos TXT para un solo dominio. La norma estipula que se devuelvan todos los registros TXT cuando se efectúe una indagación sobre ellos.

Es posible utilizar indagaciones TXT si fallan las indagaciones SRV.

Para gatekeeper Identifiers pueden utilizarse cadenas conformes a (nombres de correo electrónico "-like") o cadenas conformes a IETF RFC 1768 (URL). Los registros de recursos devueltos son líneas de texto libre y el terminal buscará entonces líneas en la respuesta de la forma:

```
ras [< gk id>@]<domain name >[:<portno>] [<priority>]
```

El campo <gk id> es un ID de controlador de acceso opcional que está separado del nombre de dominio. Si este campo está ausente se supone que el propio dominio es entonces el ID de controlador de acceso.

El campo <domain name> puede ser el nombre del registro A que contiene la dirección IP del controlador de acceso, o bien una dirección IP bruta en forma de puntos.

El campo opcional [:<portno>] puede utilizarse para especificar un número de puerto distinto del puerto RAS normalizado.

El campo opcional [<priority>] especifica el orden en que se debe acceder a los controladores de acceso enumerados para el descubrimiento o las indagaciones LRQ si hay más de un registro TXT ras.

Ejemplos de registros TXT de controlador de acceso válidos:

- ras gk1
- ras gk1.company.com
- ras gk1:1500 3
- ras 172.11.22.33:1500 2

El punto extremo analiza las líneas y a partir de ellas obtiene la dirección de transporte del controlador de acceso dentro de ese dominio a la que puede enviar mensajes RAS.

Puesto que el DNS requiere un servidor para devolver todos los registros TXT asociados con un nombre de dominio, el punto extremo puede seleccionar y procesar únicamente los registros que le son útiles. Permite también al DNS devolver una lista ordenada de controladores de acceso que pueden servir como alternativas y reservas.

6.5.2 Protocolos de Señalización

6.5.2.1 Q.931 Señalización inicial de llamada

Q.931 define los mensajes de señalización de control de llamadas. A través de estos mensajes se conecta, se mantienen y desconectan las llamadas.

Los mensajes Q.931 tienen la siguiente estructura:

8	7	6	5	4	3	2	1	Octeto
Discriminador de protocolo								1
0	0	0	0	Longitud del valor de la referencia de llamada (en octetos)				2
Valor de la referencia de llamada								3
0	Tipo de mensaje							etc.
Otros elementos de información, según se requieran								

Dentro de cada octeto, el bit designado "bit 1" se transmite primero, seguido de los bits 2, 3, 4, etc. Del mismo modo, se envía primero el octeto designado como 1, seguido por el octeto 2,3, etc.

- a. **Discriminador de protocolo**, es la primera parte del mensaje y sirve para distinguir los mensajes que son para el control de llamada usuario-red de otros mensajes.

bits								Tipo Mensaje
8	7	6	5	4	3	2	1	
0	0	0	0	1	0	0	0	Mensajes de control de llamada usuario-red Q.931
0	0	0	0	1	0	0	1	Mensajes de control de llamada usuario-red Q.2931

Del 00000000 a 00000111 no son valores válidos para el discriminador.

00010000 a 00111111 y del 01010000 a 11111110 reservado para otros protocolos de red (X.25).

01000000 a 01001111 uso nacional

- b. **Referencia de llamada**, es la segunda parte del mensaje y sirve para identificar a que llamada o petición de registro/cancelación en la interfaz usuario-red se aplica un mensaje en particular.

En el primer octeto los bits del 1 a 4 indican la longitud de la información de referencia, lo máximo son 3 octetos.

El bit 8 en 0 indica que el mensaje es enviado desde el lado que origina la referencia de llamada.

El bit 8 en 1 indica mensaje es enviado hacia el lado que origina la referencia de llamada.

Del bit 1 al 7 se utilizan para el valor de la referencia de llamada.

8	7	6	5	4	3	2	1	Octeto
				Longitud del valor de la referencia de llamada				
0	0	0	0	0	0	1	1	1
Bandera	Valor de la referencia de llamada							
0/1	-	-	-	-	-	-	-	2
0	-	-	-	-	-	-	-	3
0	-	-	-	-	-	-	-	4

Ejemplo de valor de la referencia de llamada de tres octetos

- c. **Tzzipo de mensaje**, es la tercera parte del mensaje e identifica la función del mensaje que se envía:

El bit 8 se reserva para bit de ampliación en el futuro.

Del bit 7 al 1 identifican el tipo de mensaje de la siguiente manera:

bits								Tipo Mensaje
8	7	6	5	4	3	2	1	
0	0	0	-	-	-	-	-	Mensajes de establecimiento de llamada
0	0	1	-	-	-	-	-	Mensajes de la fase de información de la llamada
0	1	0	-	-	-	-	-	Mensajes de liberación de llamada
0	1	1	-	-	-	-	-	Mensajes diversos

NOTA: El detalle de los mensajes se encuentran en la referencia Q.931 de la ITU-T.

- d. **Otros elementos de información**, según se requieran. Estos elementos pueden ser de un solo octeto o de longitud variable. Los elementos de información de un solo octeto tienen dos formatos:

Formato 1

8	7	6	5	4	3	2	1	Octeto
1	Identificador del elemento de información			Contenido del elemento de información				1

Formato 2

8	7	6	5	4	3	2	1	Octeto
1	Identificador del elemento de información							1

El elemento de información de longitud variable tiene la siguiente estructura:

8	7	6	5	4	3	2	1	Octeto
0	Identificador del elemento de información							1
Longitud del contenido del elemento de información (octetos)								2
Contenido del elemento de información								3 etc.

El Identificador del elemento de información como su nombre lo dice indica la índole de la información que se envía y entre éstos tenemos:

Bits								
8	7	6	5	4	3	2	1	
1	X	X	X	-	-	-	-	Elementos de información de un solo octeto
	0	0	0	-	-	-	-	Reservado
	0	0	1	-	-	-	-	Cambio
	0	1	0	0	0	0	0	Mas datos (Formato 2)
	0	1	0	0	0	0	1	Envío Completo, etc. (Formato 2)
0	X	X	X	X	X	X	X	Elementos de información de longitud variable
	0	0	0	0	0	0	0	Mensaje Segmentado
	0	0	0	0	1	0	0	Capacidad de portadora
	0	0	0	1	0	0	0	Causa
	0	0	1	0	0	0	0	Identidad de la llamada, etc..

NOTA: El detalle de los mensajes se encuentran en la referencia Q.931 de la ITU-T, Cuadro 4-3/Q.931 – Codificación del identificador del elemento de información.

El *discriminador de protocolo*, *referencia de llamada* y *el tipo de mensaje* son comunes a todos los mensajes y estarán siempre presentes.

6.5.2.2 H.225 Señalización de Control de llamadas

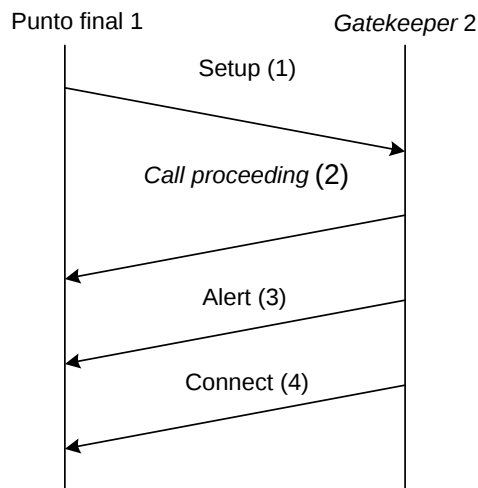
El H.225 especifica la utilización y el soporte de los mensajes de señalización Q.931, también especifica el uso de los mensajes Q.932 para servicios complementarios. Los procedimientos de control de llamadas en una red H.323 se basan en las recomendaciones del H.225.

En una red IP, en el puerto 1720 del TCP, se crea un canal de control de llamadas seguro. Este canal inicializa los mensajes Q.931 entre dos puntos finales con la finalidad de conectar, mantener y desconectar las llamadas.

Los mensajes Q.931 y Q.932 utilizados para el establecimiento de comunicación H.323 y H.225.0 en la red de paquetes son los siguientes:

Mensajes de establecimiento de la comunicación	Transmisión	Descripción
Aviso (Alerting)	Obligatorio	Indica a la parte llamada que el sonido de llamada se ha iniciado.
Llamada en curso (Call Proceeding)	Opcional	Respuesta al Setup que indica que los procedimientos de establecimiento de llamada están iniciados.
Conexión (Connect)	Obligatorio	Indica a la entidad llamante que la conexión esta lista. El mensaje de conexión puede contener la dirección de transporte UPD/IP para la señalización de control H.245.
Acuse de conexión	Prohibido	
Progresión	Opcional	
Establecimiento (Setup)	Obligatorio	Este mensaje será enviado por una entidad H.323 llamante para indicar su deseo de establecer una conexión a la entidad llamada.
Acuse de establecimiento (Setup Acknowledge)	Opcional	
Mensajes de liberación de llamada		
Desconexión	Prohibido	
Liberación	Prohibido	
Liberación completa (Release Complete)	Obligatorio	Indica que la llamada ha sido liberada.
Mensajes de la fase de información de llamada		
Reanudación	Prohibido	
Acuse de reanudación	Prohibido	
Rechazo de reanudación	Prohibido	
Suspensión	Prohibido	
Acuse de suspensión	Prohibido	
Rechazo de suspensión	Prohibido	

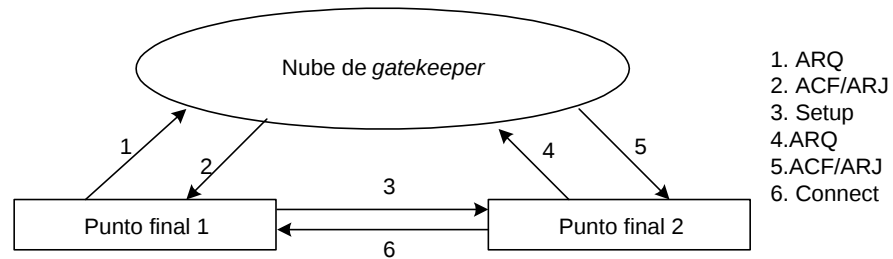
Información de usuario	Opcional	
Mensajes varios		
Control de congestión	Prohibido	
Información	Opcional	Este mensaje puede enviarse para proporcionar información adicional. Puede utilizarse para entregar características privadas
Notificación	Opcional	
Estado (Status)	Obligatorio	El mensaje de Estado se utilizará para responder a un mensaje de señalización de llamada desconocido o a un mensaje indagación de estado.
Indagación de estado (Status Inquirí)	Opcional	El mensaje Indagación de estado puede utilizarse para solicitar el estado de la llamada.
Mensajes Q.932/H.450		
Facilidad (Facility)	Obligatorio	Solicita o confirma servicios complementarios.
Retención	Prohibido	
Acuse de retención	Prohibido	
Rechazo de retención	Prohibido	
Recuperación	Prohibido	
Acuse de recuperación	Prohibido	
Rechazo de recuperación	Prohibido	



Mensajes de señalización de configuración de llamada.

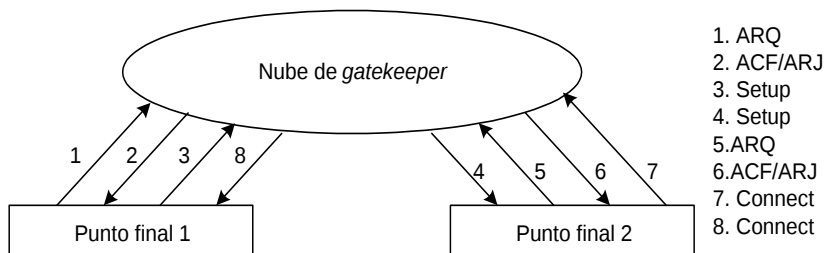
Se puede enrutar el canal de señalización de llamada de dos maneras en una red H.323:

- **Señalización de llamada directa de punto final (Direct endpoint call signaling).** En redes que no tienen un gatekeeper los mensajes se envían directamente entre los dos puntos finales;



Señalización de llamada directa de punto final.

- **Señalización de llamada de gatekeeper enrutado (GKRCS, Gatekeeper Routed Call Signaling).** Los mensajes de señalización de las llamadas entre dos puntos finales son enrutadas a través del gatekeeper.



Se

Señalización de llamada de gatekeeper enrutado.

6.5.2.3 H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz

La recomendación H.245 especifica los mensajes de control extremo a extremo entre entidades H.323 y los procedimientos para utilizar estos mensajes.

Los procedimientos se definen para permitir el intercambio de capacidad audiovisuales y de datos; para solicitar la transmisión de un modo audiovisual y de datos determinado; para gestionar los canales lógicos utilizados para transportar la información audiovisual y de datos; para establecer qué terminal es el terminal principal y cuál el subordinado con fines de gestión de los canales lógicos bidireccionales; para transportar distintas señales de control e indicación; para controlar la velocidad de bits de los canales lógicos individuales y

de la totalidad del múltiplex; y para medir el retardo de ida y vuelta entre un par de terminales.

Para el uso de esta recomendación se ha previsto el uso de un protocolo de transporte fiable, que proporcione una entrega garantizada de datos correctos.

Este protocolo establece canales lógicos para la transmisión de audio, vídeo, datos y canal de control. Un punto final establece un canal H.245 para cada llamada con el punto final que está participando. El canal de control seguro se crea sobre IP utilizando el puerto TCP dinámicamente asignado en el último mensaje de señalización de llamada (Connect protocolo H.225).

A través del canal de control se lleva a cabo el intercambio de capacidades, apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes. El intercambio de capacidades puede ser diferente para la transmisión que para la recepción.

Algunos de los mensajes utilizados en la operación de control H.245 son:

- Intercambio de Capacidades (Capability_Exchange). Los procedimientos de intercambio de capacidades tienen por finalidad asegurar que únicamente las señales multimediales que deben transmitirse son aquellas que el terminal de recepción puede recibir y manejar adecuadamente. Los mensajes utilizados permitirán conocer la capacidad del terminal para transmitir y recibir audio, vídeo y datos al terminal que está participando. No es necesario que un terminal comprenda o almacene todas las capacidades entrantes;
- Determinación Principal Subordinado (Master-Slave Determination). Procedimientos que indican que punto final es el principal (maestro) y qué punto final es el secundario (esclavo) en una llamada determinada;
- Determinación del retardo de ida y vuelta (Round-Trip Delay). Procedimientos que determinan el retraso entre un terminal transmisor y un terminal receptor. Este procedimiento nos permitirá conocer si o detectar si un terminal está funcionando todavía;
- Procedimientos de Señalización de canal lógico (Logical Channel Signaling). Los mensajes utilizados en este procedimiento abren y cierra el canal lógico que transporta la información de audio, vídeo y datos. La finalidad de estos procedimientos es garantizar que un terminal es capaz de recibir y decodificar los

datos que se transmitirán por un canal lógico en el momento en que se abra tal canal, en vez de en el momento en que se transmita el primer dato por él y para asegurar que el terminal de recepción está preparado para recibir y decodificar los datos que se transmitirán por el canal lógico antes del comienzo de la transmisión. Este protocolo se aplica también al establecimiento de canales unidireccionales y bidireccionales;

- Petición de cierre de canal lógico por el terminal receptor. Define los mecanismos que permiten a un terminal receptor solicitar el cierre de un canal lógico entrante puesto que el canal lógico se abre y se cierra desde el lado del transmisor únicamente;
- Modificación de entrada en la tabla múltiplex H.223. Define el mecanismo para informar al receptor sobre las nuevas entradas en la tabla múltiplex H.223. La tabla H.223 asocia cada octeto dentro de un mensaje MUX H.223 con un determinado número de canal lógico. La tabla múltiplex H.223 puede tener hasta 15 entradas;
- Petición de modo audiovisual y de modo datos. Después del intercambio de capacidades, ambos terminales conocerán las capacidades del otro para transmitir y recibir. Este procedimiento define el mecanismo por el cual un terminal puede pedir que se le transmita en un modo determinado;
- Instrucciones e indicaciones. Las instrucciones e indicaciones pueden utilizarse para determinar señales de vídeo/audio, para determinar señales de activo/inactivo, para informar al usuario, para petición de actualización rápida, etc. Los mensajes utilizados no provocan mensajes de respuesta del terminal sino una ejecución de una acción.

Los mensajes de esta recomendación son codificados para la transmisión aplicando las reglas de codificación especificadas en la recomendación UIT-T X.691. La sintaxis de estos mensajes utiliza la notación ASN.1 definida en la recomendación UIT-T X.680. El H.245 describe también la sintaxis de los mensajes que utiliza, los cuales pueden ser consultados en la documentación de la UIT-T H.245.

Los mensajes H.245 pueden ser encapsulados dentro del canal de señalización de llamadas H.225. Esto se conoce como Tunneling H.245 y permite mejorar el tiempo de conexión de llamada y la asignación de recursos.

La terminación de una llamada puede ser iniciada por cualquier punto final participante. Primero deben terminar las transmisiones tanto de audio, vídeo o datos, y se deben cerrar los canales lógicos. Luego, se finaliza la sesión H.245 y se envía un mensaje de liberación (release complete message) en el canal de señalización de llamada. Si un gatekeeper estuvo participando de la llamada se envían adicionalmente los siguientes mensajes a través del canal RAS:

- Disengage Request (DRQ). Indican la terminación de la llamada;
- Disengage Confirm (DCF). Confirman la desconexión de la llamada;
- Disengage Reject (DRJ). Indica el rechazo de la desconexión de la llamada.

6.5.3 Protocolos de Compresión de Voz

Las recomendaciones de la serie G de la ITU-T son normalizaciones a los esquemas de codificación CELP, MP-MLQ PCM y ADPCM. Entre estos estándares los más utilizados para la telefonía y voz por paquetes son:

- Requeridos: G.711 y G.723;
- Opcionales: G.728, G.729 y G.722

En las codificaciones efectuadas con muestras, cada muestra de audio está representada por un número fijo de bits. La duración de un paquete de audio viene determinada por el número de muestras en el paquete. Un paquete de audio RTP puede contener cualquier número de muestras de audio, siempre que el número de bits por muestra multiplicado por el número de muestras por paquete sea igual a cuenta de octetos entera.

Las codificaciones efectuadas con tramas codifican un bloque de longitud fija de audio en otro bloque de datos comprimidos, que también suele ser de longitud fija. La duración de la trama se define como parte de la codificación. Pueden estar codificadas varias tramas consecutivas dentro de un solo paquete.

Codificación	Muestra/trama	Bits/muestra	ms/trama
G722	Muestra	8	
G722.1	Trama	N/A	20
G728	Trama	N/A	2,5
MIC-A	Muestra	8	
MIC-μ	Muestra	8	
G723.1	Trama	N/A	30
G729	Trama	N/A	10
GSM	Trama	N/A	20
ISO/CEI 14496-3	Trama	N/A	N/A

G.711 Modulación por impulsos codificados (MIC). Describe la técnica de codificación de voz de PCM de 64 Kbps. La voz codificada con G.711 está en un formato correcto para la entrega de voz digital en la red telefónica pública o a través de intercambio privado de ramas (PBX). G.711 recomienda dos leyes de codificación, designadas ley A y ley μ . El número de valores cuantificados viene dado por la ley de codificación. La ley A y la ley μ utilizan compresión logarítmica que le permite alcanzar de 12 a 13 bits de calidad PCM lineal en 8 bits. La ley A se utiliza en Europa. La ley μ tiene una ventaja con respecto a la anterior en cuanto al rendimiento en relación señal a ruido. La ley μ se utiliza en América del Norte.

MIC-A se especifica en UIT-T G.711. Los datos de audio se codifican con ocho bits por muestra, previo escalamiento logarítmico.

MIC-μ se especifica en UIT-T G.711. Los datos de audio se codifican con ocho bits por muestra, previo escalamiento logarítmico.

G. 726. Describe la codificación de ADPCM a 40, 32, 24 y 16 Kbps, codifica utilizando muestras de 4 bits. Los 4 bits codifican las diferencias de la amplitud, así como la velocidad de cambio de esta amplitud empleando alguna predicción lineal. Puede intercambiar voz ADPCM entre voz por paquetes y telefonía pública o redes PBX suponiendo que estas últimas tienen la capacidad ADPCM.

G. 728. Codificación de señales vocales a 16 kbit/s utilizando CELP (Predicción Lineal con excitación por código de bajo retardo). Una trama G.728 se organiza en 5 octetos o en 4 vectores de 10 bits cada uno. Los bits de los vectores más antiguos son más significativos que los bits de los vectores más nuevos.

G.729. Describe la compresión CELP que permite que la voz sea codificada en corrientes de 8 Kbps; dos variaciones de este estándar (G.729 y G.729, Anexo A) difieren ampliamente en cuanto a complejidad de computación, y ambas proporcionan generalmente una calidad de voz tan buena como la ADPCM de 32 Kbps. Este codificador se optimizó para representar la señal vocal con una calidad similar a la de los enlaces de larga distancia o alámbricos en 8kbit/s. Tiene robustez inherente contra errores aleatorios en los bits así como contra tramas borradas de manera aleatoria y por ráfagas. Representa la señal de vocal con alta calidad cuando funciona en un entorno ruidoso.

G.723.1 Describe una técnica de compresión que se puede utilizar para comprimir voz u otros componentes de señales de audio de servicios multimedia a una baja velocidad binaria, como parte de la familia de estándares H.324. Dos velocidades de bit están asociadas con este codificador: 5,3 (20 octetos) y 6,3 Kbps (24 octetos). Las tramas de 4 octetos se utilizan para especificar parámetros de ruido de confort y se denomina SID (descriptor de inserción de silencio). La velocidad de bit más alta se basa en la tecnología MP-MLQ y proporciona una mayor calidad, y permite que los diseñadores del sistema tengan flexibilidad adicional. Este codificador se optimizó para representar la señal vocal con una calidad próxima a la de los enlaces de larga distancia en las velocidades mencionadas utilizando un grado de complejidad limitado. La transmisión se realiza siempre desde el bit menos significativo al bit más significativo. Los dos bits menos significativos del primer octeto de la trama indican el tamaño de la trama y el tipo de códec. El intervalo de paquetización es de 30 ms. La frecuencia de muestreo es de 8000 Hz.

G.722.1 Define una codificación de audio de 7 kHz dentro de 64 kbit/s. Codifica señales de audio de banda ancha con frecuencias de 50 Hz a 7 kHz a una o dos velocidades binarias, 24 kbit/s o 32 kbit/s utilizando tramas de 20 ms y una velocidad de muestreo de 16 kHz. En el caso de 24 kbit/s se producen 480 bits (60 octetos) por trama y en el caso de 32 kbit/s se producen 640 bits (80 octetos) por trama. Una trama consta de un número fijo de bits, sin embargo en esta codificación se utiliza una codificación de longitud variable para representar la mayor parte de los parámetros codificados.

G.722 Describe las características de un sistema de codificación de audio (banda de 50 a 7000 Hz) que puede utilizarse en diversas aplicaciones para señales vocales de alta calidad. El sistema de codificación utiliza Modulación por Impulsos Codificados Diferencial

Adaptativa de Subbanda (MICDA-SB) a una velocidad binaria de hasta 64 kbit/s. El sistema tiene tres modos básicos de funcionamiento, correspondientes a las velocidades binarias utilizadas para la codificación de audio de 7 kHz: 64, 56 y 48 Kbit/s. A los códecs que funcionan con este protocolo se los conoce también como 7 Khz a 64 kbit/s.

Según la calificación MOS (Mean Opinion Score) que es una prueba subjetiva de la calidad de voz y sonido con una amplia gama de oyentes y material de prueba (los oyentes otorgan a cada muestra de material de voz una puntuación entre 1 baja y 5-excelente, luego se obtiene la puntuación media), los códecs (codificador–decodificador) de la ITU-T han recibido las siguientes puntuaciones:

Método de compresión	Velocidad de bit (kbps)	Tamaño de muestra (ms)	Puntuación MOS
G.711 PCM	64	0,125	4.1
G.726 ADPCM	32	0.125	3.85
G.728 LD-CELP	15	0.625	3.61
G.729 CS-ACELP	8	10	3.92
G.729 ^a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5,3	30	3,65

Fuente Laboratorios Cisco

6.5.4 Protocolos de Transmisión de Voz

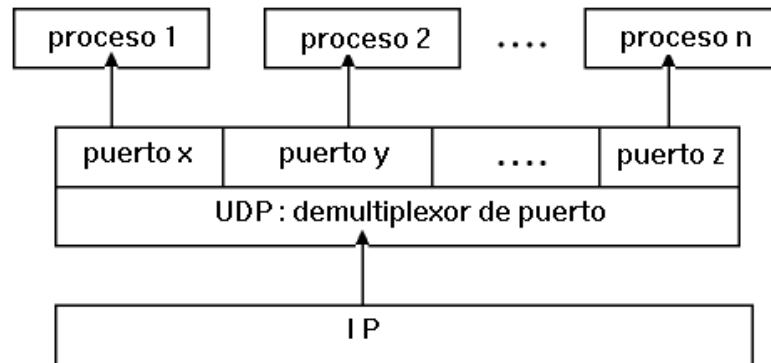
6.5.4.1 UDP (User Datagram Protocol)

La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP. El protocolo UDP se describe en el RFC 768 – Protocolo de Datagrama de Usuario.

La principal razón para utilizar UDP en VoIP radica en que no se puede tolerar el retardo producido por ACKs, retransmisiones y todo el complejo proceso de cálculo que desarrolla TCP.

El protocolo UDP es un servicio no orientado a conexión y no fiable (es decir no confirma o no acusa recibo por las TPDUS enviadas). Las TPDUs (Transport Protocol Data Unit, Unidad de datos para el protocolo de transporte) intercambiadas por UDP se denominan mensajes o datagramas UDP.

UDP es básicamente una interfaz de aplicación para IP. No soporta confiabilidad, control de flujo o recuperación de errores para IP. Simplemente sirve como "multiplexor/demultiplexor" para enviar y recibir datagramas, usando puertos para dirigir los datagramas como se muestra en la siguiente figura:



Si se van a enviar mensajes múltiples, por ejemplo vídeo o audio en tiempo real, se deberán tomar las medidas adecuadas para asegurar la capacidad suficiente en la red (uso de RSVP por ejemplo) y evitar la congestión no excediendo lo solicitado en el momento de hacer la reserva (en estos casos se suele conocer con bastante aproximación el tráfico que se va a introducir en la red).

En caso de congestión en la red o saturación del receptor, los datagramas IP correspondiente a mensajes UDP serán descartados por la red sin informar al emisor, ni al receptor, por lo cual en algunos casos se implementan mecanismos de control para informar al emisor para que baje el ritmo de emisión si rebasa un umbral determinado.

El valor 17 en el campo protocolo del datagrama IP identifica un mensaje UDP.

Los mensajes UDP se dirigen de una aplicación a otra mediante el puerto de destino, que está especificado en la cabecera del datagrama UDP. Cada datagrama UDP se envía con un único datagrama IP. Aunque el datagrama IP se puede fragmentar durante la transmisión, la implementación de recepción IP lo re-ensamblará antes de presentarlo a la capa UDP. Análogamente a TCP los puertos UDP son números entre 0 y 65535, pero aún en el caso de coincidir en número son TSAPs diferentes a los de TCP.

Los TSAPs son mecanismos que permiten distinguir a qué aplicación van dirigidos los datos. Un TSAP en Internet está especificado por:

- Dirección donde ‘conecta’ el nivel de red: dirección IP de los dos hosts;
- Dirección donde conecta el nivel de transporte (campo protocolo del datagrama IP): normalmente TCP (ya que UDP al ser no orientado a conexión no puede establecer conexiones);
- Dirección donde conecta el nivel de aplicación: esto es el puerto.

Un puerto es un número entero entre 0 y 65535. Por convenio los números del 0 a 1023 están reservados para uso de servicios estándar por lo que se les denomina puertos bien conocidos. Cualquier número por encima de 1023 está disponible para ser utilizado libremente por los usuarios.

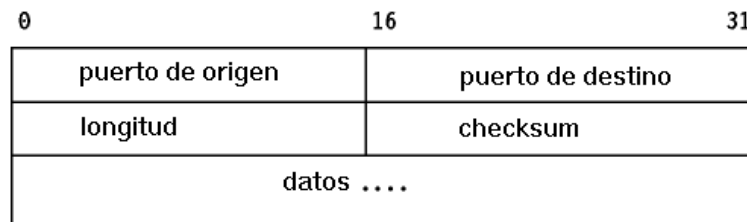
Los tipos de puertos existentes son los siguientes:

- **Puertos Bien conocidos (well-known ports):** Estos puertos pertenecen a servidores estándares, por ejemplo TELNET usa el puerto 23. El rango de este tipo de puerto está comprendido entre 1 y 1023. Los números de puertos bien-conocidos son típicamente impares porque los primeros sistemas usaban el concepto de puerto como una pareja de puertos impar/par para operaciones duplex. La mayoría de los servidores requieren sólo un puerto. Una excepción es el servidor BOOTP que usa dos: el 67 y el 68 (ver Protocolo BOOTstrap - BOOTP). El motivo de la utilización de los puertos bien-conocidos es permitir a los clientes tener la capacidad de encontrar servidores sin información de configuración. Los números de dichos puertos están definidos en STD 2 - Números de Internet Asignados;
- **Puertos emíferos:** Los clientes no necesitan números de puertos bien-conocidos porque inician la comunicación con servidores y el número de puerto que usan ya está contenido en los datagramas UDP enviados al servidor. Cada proceso del cliente está localizado en un número de puerto mientras el host lo necesite y se esté ejecutando. Los números de puerto efímeros tienen valores mayores que 1023, normalmente en el rango de 1024 a 5000. Un cliente puede usar cualquier número localizado dentro de dicho rango, mientras que la combinación de <protocolo de transporte, dirección IP, número de puerto> es única.

Los puertos UDP más utilizados son los siguientes:

Servicio	Puerto	Descripción
Echo	7	Devuelve el datagrama al emisor
Discard	9	Descarta el datagrama
Daytime	13	Devuelve la hora del día
Quote	17	Devuelve una 'frase del día'
Chargen	19	Generador de caracteres
Nameserver	53	Servidor de nombres de dominio
Bootps	68	Puerto servidor utilizado para cargar información de configuración Bootp
Bootpc	68	Puerto cliente utilizado para recibir información de configuración
TFTP	69	Trivial File Transfer Protocol
SunRPC	111	Sun Remote Procedure Call
NTP	123	Network Time Protocol
SNMP	161	Usado para recibir consultas de gestión de red
SNMP-trap	162	Usado para recibir avisos de problemas en la red

La estructura de un mensaje UDP se describe en la figura siguiente:



donde:

- Puerto de origen: (16 bits) Indica el puerto del proceso que envía. Este valdrá normalmente cero, salvo que la aplicación solicite una respuesta. Este es el puerto que se direcciona en las respuestas.
- Puerto destino (16 bits) Especifica el puerto del proceso al que va dirigido el mensaje en el host de destino.
- Longitud (16 bits) Es el tamaño (en bytes) de este datagrama de usuario incluyendo la cabecera.
- Suma de comprobación (checksum) (16 bits) Es un campo opcional de 16 bits que sirve para detectar errores en el segmento recibido. El uso de este campo puede omitirse cuando se envía información en tiempo real (audio o vídeo digitalizado). El algoritmo aplicado para su cálculo es el siguiente: sumar todos los campos de 16

bits usando aritmética de complemento a 1, y calcular el complemento a 1 del resultado. Para el cálculo se utiliza todo el mensaje incluida la cabecera y se antepone una pseduocabecera (la cabecera pseudo-IP contiene la dirección IP fuente y destino, el protocolo y la longitud del mensaje) de forma que se verifica que sean correctos los datos y la información de control. Si el checksum da error el mensaje es simplemente descartado sin notificar al emisor.

- Datos: contiene los datos a transmitir 0-524056 bites (65507 bytes). Un mensaje UDP ha de estar contenido necesariamente en un datagrama IP, lo cual fija la longitud máxima de este campo.

6.5.4.2 RTP (Real Time Protocol).

RTP es el protocolo estándar para transmitir tráfico sensible al retraso (audio y vídeo) por las redes basadas en paquetes.

Las aplicaciones suelen hacer pasar el RTP encima del UDP para hacer uso de sus servicios de multiplexación y de suma de control (checksum). Sin embargo, el RTP puede utilizarse con otros protocolos de red o de transporte dependiendo de las necesidades.

El RTP proporciona servicios para: - la identificación de carga útil (carga útil hace referencia a las muestras de voz o vídeo comprimidos), - para indicar la secuencia de los paquetes, - la marca de temporización que se utiliza para determinar el tiempo de llegada entre los paquetes (fluctuación de fase), y; - la monitorización que permite detectar pérdidas.

RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y la QoS.

La Recomendación define el RTP compuesto de dos partes estrechamente vinculadas:

- El protocolo de transporte en tiempo real (RTP), para transportar datos que tienen propiedades de tiempo real.
- El protocolo de Control del RTP (RTCP), para supervisar la calidad de servicio y transmitir información sobre los participantes en una conferencia en tiempo real de grupos de cualquier tamaño (El RTCP se describirá en los protocolos de control de transmisión).

Debido a que existen servicios que ocupan un gran ancho de banda cuando utilizan RTP, como es el vídeo, que podrían degradar seriamente la calidad de servicio en el Internet, la actual Internet no puede aún soportar la demanda potencial completa de servicios en tiempo real.

Definiciones:

Mezclador: “El mezclador es un sistema intermedio que recibe paquetes RTP de una o más fuentes, posiblemente cambia el formato de datos, combina los paquetes de alguna manera y remite entonces un nuevo paquete RTP. Dado que la temporización entre múltiples fuentes de entrada no estará generalmente sincronizada, el mezclador hará ajustes de temporización entre los trenes y generará su propia temporización para el tren combinado. Así, todos los paquetes originarios de un mezclador se identificarán como paquetes que tienen el mezclador como su fuente de sincronización” ITU-T-H225.0s.

“Considérese el caso en que los participantes de una zona están conectados mediante un enlace de baja velocidad a la mayoría de los participantes de la conferencia, quienes disfrutan de acceso de red a alta velocidad. En lugar de obligar a todos a utilizar una anchura de banda menor, codificación de audio de calidad reducida, puede disponerse un relé de nivel RTP denominado mezclador cerca del área de baja anchura de banda. Este mezclador resincroniza los paquetes de audio entrantes para reconstruir el espaciamiento de 20 ms constante generado por el emisor, mezcla estos trenes de audio reconstruidos en un solo tren, traduce la codificación a una anchura de banda inferior y remite el tren de paquetes de anchura de banda inferior a través del enlace de baja velocidad. Estos paquetes podrían ser unidifundidos a un único destinatario o multidifundidos en una dirección diferente a múltiples destinatarios. El encabezamiento RTP incluye un medio para que los mezcladores identifiquen las fuentes que han contribuido a un paquete mixto para que pueda proporcionarse indicación correcta del hablante en todos los receptores.” ITU-T-H225.0s.

Traductor: “Sistema intermedio que remite paquetes RTP con su identificador de fuente de sincronización intacto.” ITU-T-H225.0s.

“Considérese que algunos de los participantes previstos en la conferencia de audio pueden conectarse con enlaces de gran anchura de banda, pero no podrían ser directamente alcanzables mediante multidifusión IP. Por ejemplo, podrían hallarse detrás de un

cortafuego a nivel de aplicación que no deje pasar paquetes IP. Para estos puestos, el mezclador podría no ser necesario, en cuyo caso puede utilizarse otro tipo de relé a nivel RTP denominado "traductor". Se instalan dos traductores, uno a cada lado del cortafuego, con el del lado exterior encauzando todos los paquetes multidifusión recibidos a través de una conexión segura al traductor interior al cortafuego. El traductor interior al cortafuego los envía de nuevo como paquetes multidifusión a un grupo multidifusión restringido a la red interna del puesto." ITU-T-H225.0s.

Fuente de sincronización (SSRC, synchronization source): Es el emisor de un tren de paquetes derivado de una fuente de señal, como un micrófono o una cámara. El "identificador SSRC" identifica a la fuente de sincronización, es un número de 32 bits elegido aleatoriamente y es único dentro de una determinada sesión RTP. Todos los paquetes procedentes de una fuente de sincronización forman parte del mismo espacio de temporización y de número secuencial por lo que un receptor agrupa paquetes por fuente de sincronización para su reproducción. Si un participante genera múltiples trenes en una sesión RTP, por ejemplo, desde cámaras de vídeo separadas, cada uno debe ser identificado por un SSRC diferente.

Fuente contribuyente (CSRC, contributing source): El mezclador inserta una lista de los identificadores de SSRC de las fuentes que han contribuido a la generación de un determinado paquete. Esta lista se denomina la lista de CSRC. Un ejemplo de aplicación es la audioconferencia, en la que un mezclador indica a todos los hablantes cuyo discurso se combinó para producir el paquete saliente, permitiendo al receptor indicar al hablante en ejercicio, aún cuando todos los paquetes contienen el mismo identificador SSRC (el del mezclador).

Estructura de la cabecera RTP

0										1										2									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9
V=2		P	X	CC				M	PT							NUMERO DE SECUENCIA													
Identificador de tiempo																													
Identificador de fuente de sincronizacion (SSCR)																													
Identificador de fuente contibuyente (CSRC)																													

Los octetos son transportados desde el más significativo hasta el menos significativo. Este orden de los octetos suele conocerse como el del gran final.

Todos los datos de encabezamiento están alineados en su longitud alineal, es decir, los campos de 16 bits están alineados en desplazamientos pares, los campos de 32 bits están alineados en desplazamientos divisibles por cuatro, etc. Los octetos designados como relleno tienen el valor cero.

El tiempo de reloj (tiempo absoluto) se representa utilizando el formato del protocolo de señales horarias de red (NTP, network time protocol), que se indica en segundos con relación a las 0h UTC del 1 de enero de 1900.

La lista de identificadores de CSRC sólo está presente cuando ha sido insertada por un mezclador, todo el resto de campos están siempre presentes en cada paquete RTP.

- versión (V, version): 2 bits. Versión del RTP. 2 es el valor de la recomendación actual.
- relleno (P, padding): 1 bit.. 0 Si no tiene octetos de relleno. 1 si el paquete contiene octetos de relleno (no forman parte de la cabida útil). El último octeto del relleno indica cuántos octetos de relleno deben ser ignorados.
- extensión (X, extensión): 1 bit. 1 indica que el encabezamiento fijo va seguido por una extensión de encabezamiento.
- cuenta de CSRC (CC, CSRC count): 4 bits. La cuenta de CSRC contiene el número de identificadores de CSRC que siguen al encabezamiento fijo.
- marcador (M): 1 bit. Permite marcar las fronteras de las tramas.

- tipo de cabida útil (PT): 7 bits. Este campo identifica el formato de la cabida útil RTP (cabida útil hace referencia a los datos transportados por RTP en un paquete, por ejemplo muestras de audio o datos de vídeo comprimidos). Los tipos de cabida útil se especifican en la siguiente tabla:

PT	Nombre de codificación	Audio / vídeo (A/V)	Frecuencia de reloj (Hz)	Canales (audio)
0	MIC-μ	A	8 000	1
8	MIC-A	A	8 000	1
9	G722	A	8 000	1
Dinámico	G722.1	A	16 000	1
4	G723.1	A	8 000	1
15	G728	A	8 000	1
18	G729	A	8 000	1
31	H261	V	90 000	N/A
34	H263	V	90 000	N/A
3	GSM	A	8 000	1
Dinámico	ISO/CEI 14496-2	V	90 000	N/A
Dinámico	ISO/CEI 14496-3	A	90 000	1-5.1 (nota 2)
96-127	Dinámica	?		

En este cuadro se listan los valores estáticos para los tipos de cabida útil, además, pueden definirse valores de tipo de cabida útil en la gama 96-127 dinámicamente.

- número secuencial: 16 bits. El número secuencial aumenta en uno por cada paquete de datos RTP enviado, y puede ser utilizado por el receptor para detectar pérdida de paquetes y restablecer la secuencia de paquetes.
- indicación de tiempo (temporizador): 32 bits. La indicación de tiempo refleja el instante de muestreo del primer octeto del paquete de datos RTP. Permitirá medir la fluctuación de llegada de paquetes. La frecuencia de reloj depende del formato de los datos transportados como cabida útil.
- SSRC: 32 bits. El campo SSRC identifica la fuente de sincronización. Este identificador se elige aleatoriamente, con el propósito de que no haya dos fuentes de sincronización dentro de la misma sesión RTP que tengan el mismo identificador de SSRC.
- lista de CSRC: 0 a 15 elementos, de 32 bits cada uno. La lista de CSRC identifica las fuentes contribuyentes para la cabida útil contenida en este paquete. Por ejemplo, para los paquetes de audio se enumeran los identificadores de SSRC de todas las fuentes que se mezclaron juntas para crear un paquete, permitiendo una indicación correcta del hablante en el receptor.

6.5.5 Protocolos de Control de la Transmisión:

6.5.5.1 RTCP (Real Time Control Protocol)

Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.

El protocolo de Control RTP (RTCP) se basa en la transmisión periódica de los paquetes de control a todos los participantes en la sesión. El RTCP efectúa cuatro funciones:

- La primera función es proporcionar realimentación sobre la calidad de la distribución de los datos. Esta realimentación de calidad de recepción es de utilidad no sólo para el emisor quien podrá modificar sus transmisores sobre la base de la realimentación, sino también para otros receptores que pueden determinar si los problemas son locales, regionales o globales, y para supervisores de terceras partes pues con mecanismos de distribución como es la multifusión IP, se pueden identificar problemas en la red.
- La segunda función del RTCP es transportar el CNAME (Nombre canónico). Debido que el identificador SSRC puede cambiar si se reinicia un programa, el campo CNAME permite seguir la pista de cada participante, pues mantiene una vinculación del identificador de SSRC a un identificador que permanece constante.
- Una tercera función es controlar la velocidad para que se pueda escalar hasta un gran número de participantes. Haciendo que cada participante envíe sus paquetes de control a todos los demás, se puede obtener el número de participantes que es utilizado para calcular la velocidad a la que se envían los paquetes.
- Esta cuarta función opcional se encarga de transportar información mínima de control de sesión como el ID del participante que se va a visualizar en la interfaz de usuario.

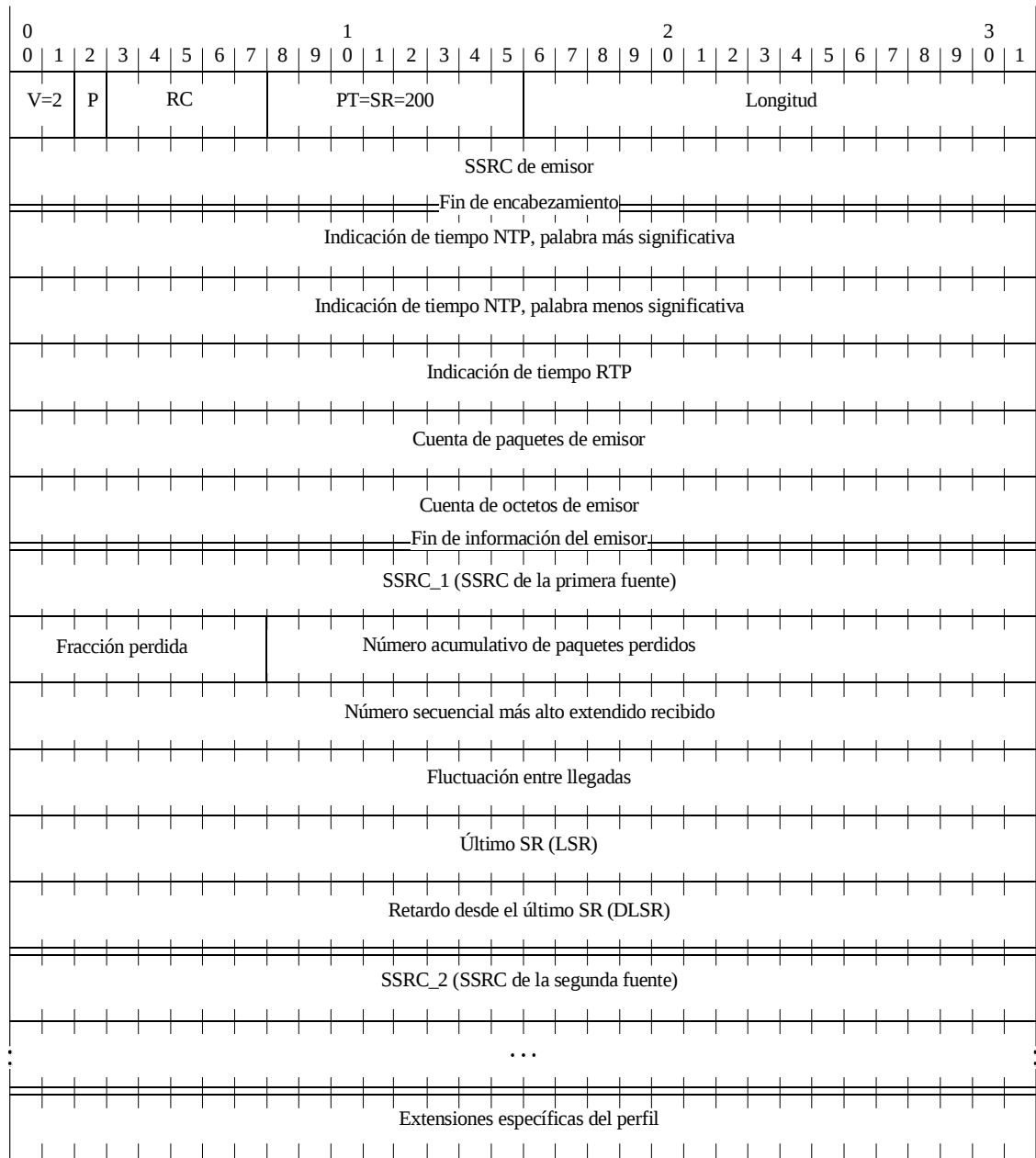
Las funciones 1 a 3 son obligatorias cuando se utiliza RTP en el entorno multidifusión IP, y se recomiendan para todos los entornos. Se aconseja que los diseñadores de aplicaciones RTP eviten mecanismos que sólo puedan funcionar en modo unidifusión y que no los escalen a números mayores.

Formato de paquetes RTCP

Existen varios tipos de paquetes RTCP:

- **SR: Informe de emisor**, con los datos estadísticos de transmisión y recepción de los participantes que son emisores activos. A través de estos paquetes se obtiene la realimentación que es la función principal del RTCP.
- **RR: Informe de receptor**, con los datos estadísticos de recepción de los participantes que no son emisores activos. A través de estos paquetes se obtiene la realimentación que es la función principal del RTCP.
- **SDES: Elementos fuente de descripción**. Entre los elementos fuente de descripción se tienen los siguientes: CNAME (nombre canónico) obligatorio, NAME (nombre de usuario), EMAIL (dirección de correo electrónico), PONE (número telefónico), LOC: ubicación de usuario geográfico, etc.
- **BYE**: Indica fin de la participación.
- **APP**: Funciones específicas de la aplicación.

Cada paquete RTCP comienza por una parte fija similar a la de los paquetes de datos de RTP, seguida por elementos estructurados que pueden ser de longitud variable según el tipo de paquete, pero que siempre terminan en una frontera de 32 bits. El requisito de alineación y un campo de longitud en la parte fija se incluyen para hacer los paquetes RTCP "apilables". Múltiples paquetes RTCP pueden concatenarse sin separadores intermedios para formar un paquete RTCP compuesto que es enviado en un solo paquete del protocolo de capa inferior, por ejemplo, UDP. No hay cuenta explícita de paquetes RTCP individuales en el paquete compuesto, ya que los protocolos de capa inferior se cree que proporcionarán la longitud total para determinar el fin del paquete compuesto.

SR: Paquete RTCP de informe de emisor

T1527590-97

Fuente del grafico ITU-T, Recomendacion H.245

El paquete de informe de emisor consta de tres secciones. La primera sección, el encabezamiento, tiene 8 octetos de largo. Los campos tienen el siguiente significado:

- versión (V): 2 bits. Versión de RTP. Esta recomendación tiene el valor 2.

- relleno (P): 1 bit. 1 indica que el paquete RTCP contiene algunos octetos del relleno adicionales al final.
- cuenta de informe de recepción (RC, report count): 5 bits. El número de bloques de informe de recepción contenido en este paquete. El valor cero es válido.
- tipo de paquete (PT): 8 bits. Contiene la constante 200 para identificar éste como un paquete RTCP SR.
- longitud: 16 bits. La longitud de este paquete RTCP en palabras de 32 bits menos uno, incluido el encabezamiento y cualquier relleno.
- SSRC: 32 bits. El identificador de fuente de sincronización del que origina este paquete SR.

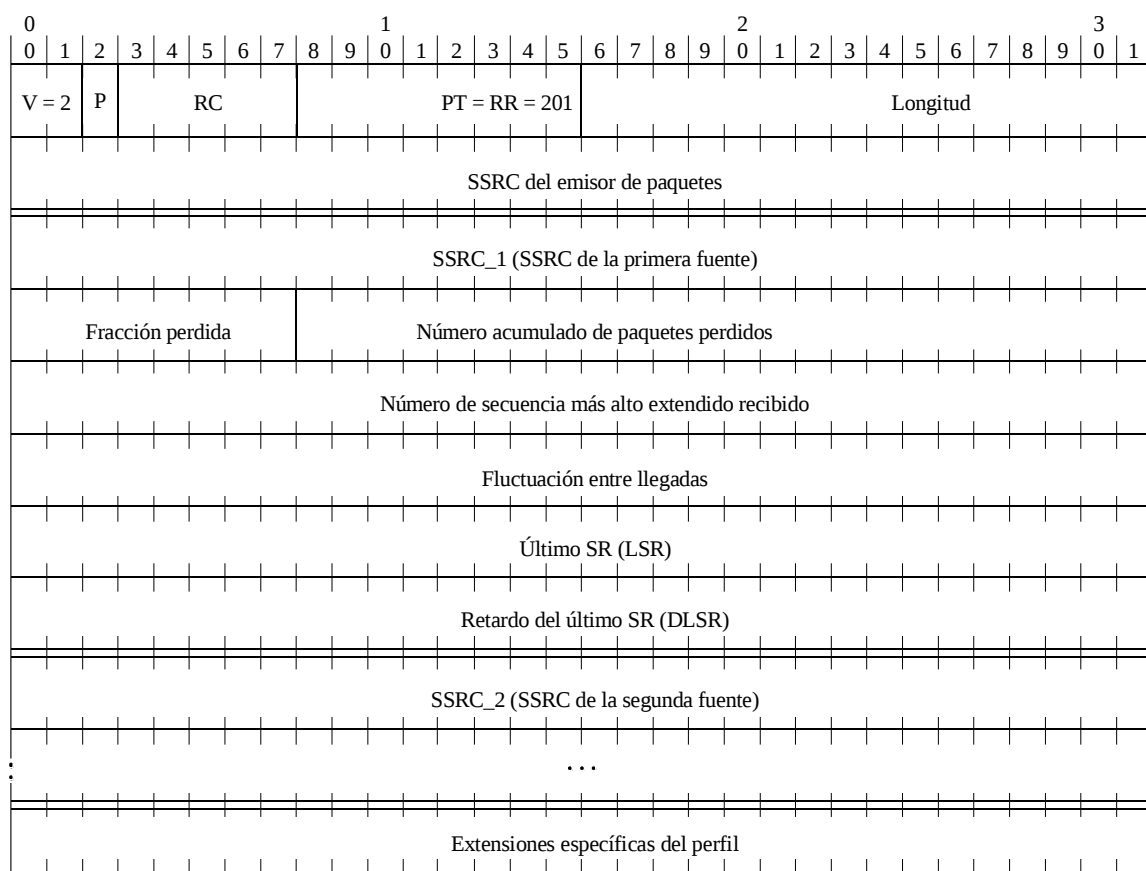
La segunda sección, la información de emisor, tiene 20 octetos de largo y está presente en cada paquete de informe de emisor. Hace un sumario de las transmisiones de datos desde este emisor. Los campos tienen el siguiente significado:

- indicación de tiempo NTP: 64 bits. Indica el tiempo de reloj cuando se envió este informe de manera que pueda utilizarse en combinación con indicaciones de tiempo devueltas en informes de recepción procedentes de otros receptores para medir la propagación de ida y vuelta a esos receptores.
- indicación de tiempo RTP: 32 bits. Corresponde al mismo tiempo que la indicación de tiempo NTP (véase más arriba), pero en las mismas unidades y con el mismo desplazamiento aleatorio que las indicaciones de tiempo RTP en los paquetes de datos. Esta correspondencia puede utilizarse para la sincronización intramedios e intermedios de fuentes cuyas indicaciones de tiempo NTP están sincronizadas, y puede ser utilizada por receptores independientes de los medios para estimar la frecuencia de reloj RTP nominal.
- cuenta de paquetes del emisor: 32 bits. El número total de paquetes de datos RTP transmitidos por el emisor.
- cuenta de octetos del emisor: 32 bits. El número total de octetos de cabida útil (es decir, sin incluir encabezamiento ni relleno) transmitidos en paquetes de datos RTP por el emisor. Este campo puede utilizarse para estimar la velocidad de datos de cabida útil media.

La tercera sección contiene cero o más bloques de informe de recepción. Cada bloque de informe de recepción transporta datos estadísticos sobre la recepción de paquetes. Estos datos estadísticos son:

- SSRC_n (identificador de fuente): 32 bits. El identificador de SSRC de la fuente a la que pertenece la información de este bloque de informe de recepción.
- fracción perdida: 8 bits. Esta fracción se define como el número de paquetes perdidos dividido por el número de paquetes esperados. Si la pérdida es negativa debido a duplicados, la fracción perdida se pone a cero.
- número acumulativo de paquetes perdidos: 24 bits. El número total de paquetes de datos RTP procedentes del SSRC_n de fuente que se han perdido desde el comienzo de la recepción.
- número secuencial más alto extendido recibido: 32 bits. Los 16 bits bajos contienen el número de secuencia más alto recibido en un paquete de datos RTP procedente del SSRC_n de fuente, y los 16 bits más significativos extienden ese número secuencial con la cuenta correspondiente de ciclos de números secuenciales.
- fluctuación entre llegadas: 32 bits. Una estimación de la varianza estadística del tiempo entre llegadas de paquetes de datos RTP, medido en unidades de indicación de tiempo y expresado como un entero sin signo.
- última indicación de tiempo SR (LSR, last SR timestamp): 32 bits. Se toma de la indicación de tiempo NTP del más reciente paquete de informe de emisor RTCP (SR) procedente del SSRC_n de fuente. Si aún no se ha recibido ningún SR, el campo se pone a cero.
- retardo desde el último SR (DLSR, delay since last SR): 32 bits. El retardo, expresado en unidades de $1/65536$ segundos, comprendido entre la recepción del último paquete SR procedente de la fuente SSRC_n y el envío de este bloque de informe de recepción. Si no se ha recibido aún ningún paquete SR del SSRC_n, el campo DLSR se fija a cero.

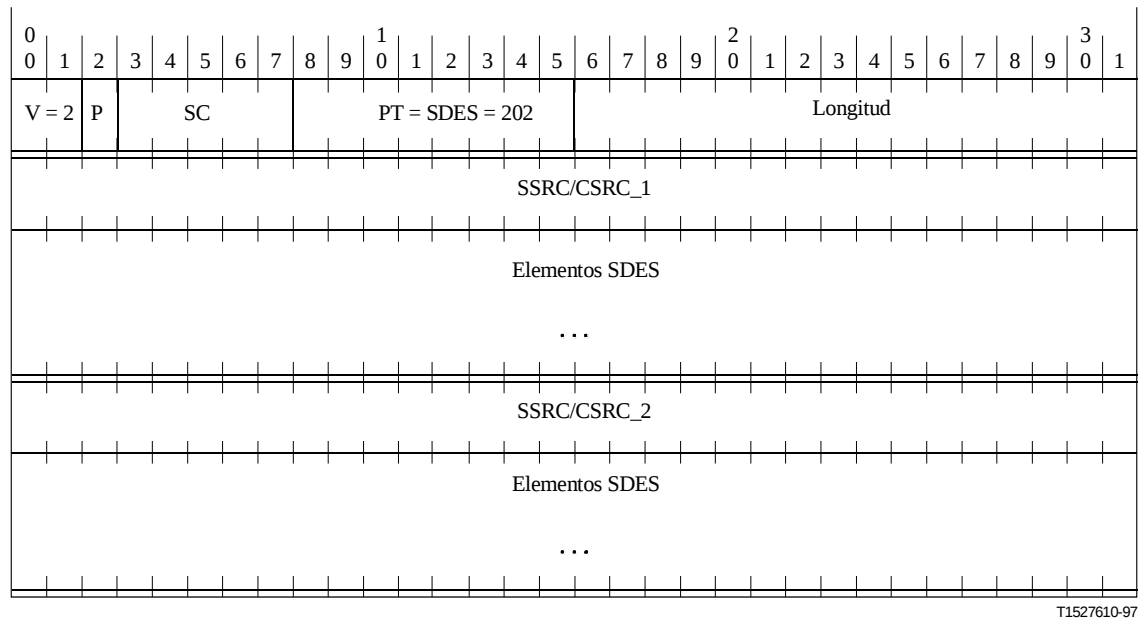
Paquete RTCP de informe de receptor



T1527600-97

Fuente del grafico ITU-T, Recomendacion H.245

El formato del paquete de informe de receptor (RR) es el mismo que el paquete SR, salvo en que el campo de tipo de paquete contiene la constante 201 y se omiten las cinco palabras de la información de emisor (son éstas las indicaciones de tiempo NTP y RTP y las cuentas de paquetes y octetos del emisor). Los campos restantes tienen el mismo significado que para el paquete SR.

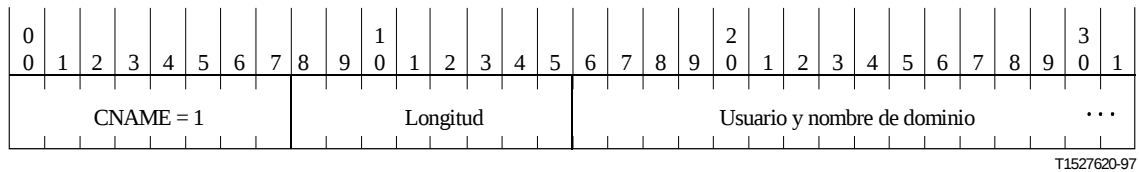
SDES – Paquete RTCP fuente de descripción

Fuente del grafico ITU-T, Recomendacion H.245

El paquete SDES es una estructura trinivel compuesta de un encabezamiento o cero o más pedazos, cada uno de los cuales se compone de elementos que describen la fuente identificada en ese pedazo. Los elementos se describen individualmente en las subcláusulas que siguen.

- versión (V), relleno (P), longitud: Como se describe para el paquete SR.
- tipo de paquetes (PT): 8 bits. Contiene la constante 202 para identificar éste como un paquete RTCP SDES.
- cuenta de fuente (SC, source count): 5 bits. Número de pedazos SSRC/CSRC contenido en el paquete SDES. Un valor cero es válido pero inútil.

Cada pedazo consta de un identificador de SSRC/CSRC seguido por una lista de cero o más elementos, que transportan información sobre la SSRC/CSRC. Cada pedazo empieza en una frontera de 32 bits. Cada elemento consta de un campo de tipo de 8 bits, una cuenta de octetos de 8 bits que describe la longitud del texto (por tanto, sin incluir este encabezador de dos octetos) y del propio texto.

CNAME – Elemento SDES identificador de punto extremo canónico

Fuente del grafico ITU-T, Recomendacion H.245

El identificador de CNAME tiene las siguientes propiedades:

- Dado que el identificador SSRC aleatoriamente atribuido puede cambiar si se descubre un conflicto o si se reinicia un programa, el elemento CNAME ha de proporcionar la vinculación del identificador de SSRC a un identificador para la fuente, que permanece constante;
- Como el identificador de SSRC, el identificador CNAME debe también ser exclusivo entre todos los participantes dentro de una sesión RTP;
- Para proporcionar una vinculación entre múltiples herramientas de medios utilizadas por un participante en un conjunto de sesiones RTP relacionadas, el CNAME debe ser fijado para ese participante;
- Para facilitar la supervisión por terceros, el CNAME debe ser adecuado para que un programa o una persona localice la fuente.

Por tanto, el CNAME debe derivarse algorítmicamente y no introducirse manualmente, a ser posible. El elemento CNAME debe tener el formato "user@host" o "host" y un nombre de usuario. Para ambos formatos "host" es el nombre de dominio perfectamente cualificado del computador principal del cual se originan los datos en tiempo real. Si una aplicación permite a un usuario generar múltiples fuentes a partir de un computador principal, dicha aplicación tendría que especificar una sintaxis adicional para el identificador CNAME para que sea exclusivo.

6.5.6 Protocolos de Datos

6.5.6.1 T.120 (*Protocolo de datos para conferencias multimedios*)

El T.120 básicamente se encarga de especificar los requisitos para el intercambio de datos en videoconferencia, rige la distribución de archivos e información gráfica en tiempo real, de manera que se perciban en forma eficaz y fiable durante el intercambio de múltiples medios en conferencias multipunto. Sus especificaciones se pueden resumir en:

- Asegurar la interoperabilidad transparente entre los diferentes puntos;
- Permite compartir datos entre los participantes de una videoconferencia a través de las redes ISDN, PSDN, CSN, TCP/IP y IPX LAN.

Debido a que este protocolo no se utiliza en VoIP no será descrito más a detalle.

6.5.7 Protocolos para transmisión en tiempo real

6.5.7.1 RSVP (Protocolo de configuración de reserva de recursos)

Los retrasos en la red y la Calidad de Servicio (QoS) son factores muy importantes en transmisiones de Voz y Datos. La solución más prometedora a estos problemas es el RSVP desarrollada por la IETF. El protocolo RSVP es usado por un host para especificar requerimientos de calidad de servicio desde la red para una aplicación en particular. RSVP es usado además por routers para entregar calidad de servicio (QoS) a todos los nodos en el camino de datos.

RSVP puede priorizar y garantizar fluidez para tráfico específico IP. RSVP habilita una red de conmutación de paquetes para emular una red de voz de conmutación de circuitos. Con RSVP habilitado, podemos lograr comunicaciones de voz con un retraso tolerable sobre una red de datos.

Para que el RSVP de resultado requiera reservar los recursos en cada nodo lo largo del camino de datos. RSVP requiere recursos en una sola dirección, por consiguiente trata a un emisor y a un receptor lógicamente distinto, la aplicación puede procesar tanto como emisor o receptor. RSVP no es por si mismo un protocolo de ruteo, este está diseñado para operar actualmente y en el futuro como unicast y multicast ruteando protocolos.

Hay dos mensajes RSVP fundamentales, Resv y Path. Una aplicación solicita participar en una sesión RSVP como emisor, enviando un mensaje Path en el mismo sentido que el flujo de datos, por las rutas uni/multicast proporcionadas por el protocolo de routing. A la recepción de este mensaje, el receptor transmite un mensaje Resv, dirigido hacia el emisor de los datos, siguiendo exactamente el camino inverso al de los mismos, en el cual se especifica el tipo de reserva a realizar en todo el camino.

En general, sin especificar tipos de QoS un mensaje Path, contiene:

- Sender Template: Parámetro por el cual se describe el formato de los paquetes que el emisor generará;
- Sender Tspec: Describe el tráfico que la aplicación estima que generará;
- Adspec: Información sobre la QoS y propiedades de la aplicación;
- Dirección del PHOP: Necesaria para poder encaminar los mensajes Resv.

Algunas características o aspectos fundamentales en el RSVP son:

- Merging: En los diferentes nodos que se van atravesando en la red por el camino de datos, se va realizando un proceso de concentración de los diferentes mensajes de petición de reservas;
- Estado de reserva en cada nodo: El estado soft RSVP se crea y refresca periódicamente por mensajes Path y Resv;
- Estilos de reserva: Una petición de reserva incluye un conjunto de opciones que se conocen como el estilo de reserva. Las distintas combinaciones de estas opciones conforman los tres estilos de reserva en uso, Wildcar-Filter (WF), Fixed-Filter (FF) y Shared-Explicit (SE).

Para la gestión de la QoS el protocolo RSVP, define tres objetos propios, como son el FLOWSPEC, ADSPEC y SENDER_TSPEC.

En cada elemento de red, el ADSPEC se pasará al módulo de control de tráfico, el cual determinará si el servicio QoS especificado está implementado en el nodo. Por defecto se generará un objeto que soportará todos los servicios QoS que admite el emisor. Cuando el mensaje Path llega a un receptor, los datos del SENDER_TSPEC y ADSPEC se pasan a través de la API (Application Programming Interface) a la aplicación, la cual interpretará estos datos, y los utilizará para seleccionar parámetros de reserva de recursos.

El grupo de trabajo Integrated Services del IETF ha considerado la existencia de varias clases de QoS, si bien actualmente sólo dos de éstas han sido formalmente especificadas para ser utilizadas con RSVP:

Guaranteed Service (service_number 2)[RFC2211]:

Este servicio proporciona un nivel de ancho de banda y un límite en el retardo, garantizando la no existencia de pérdidas en colas. Está pensado para aplicaciones con requerimientos en tiempo real, tales como ciertas aplicaciones de audio y vídeo. Cada router caracteriza el SG para un flujo específico asignando un ancho de banda y un espacio en buffer.

Controlled-Load Service (service_number 5) [RFC2212]:

A diferencia del SG este servicio no ofrece garantías en la entrega de los paquetes. Así, será adecuado para aquellas aplicaciones que toleren una cierta cantidad de pérdidas y un retardo mantenidos en un nivel razonable. Los routers que implementen este servicio deben verificar que el tráfico recibido siga las especificaciones dadas por el Tspec, y cualquier tráfico que no las cumpla será reenviado por la red, como tráfico best-effort.

6.6 MECANISMOS PARA MANTENER LA CALIDAD DE SERVICIO (QOS)

La Recomendación H.225 proporciona también un medio para determinar que los problemas de calidad son resultado de la congestión de las redes de paquetes, así como procedimientos para acciones correctivas.

Hay dos tipos de retraso relacionado con la congestión que podrían medirse:

- Aumentos de corta duración del retardo que producirían una reducción perceptible, pero no molesta, de la velocidad de trama; y,
- Un aumento general del retardo debido a la congestión de la red de paquetes en el tiempo de manera que sea de utilidad un mecanismo basado en la realimentación.

Se adopta la hipótesis de que todos los terminales multimedia red de paquetes son terminales H.323, y todos intentarán reducir la utilización de la red de paquetes a medida que la congestión aumenta, más que "robarse" anchura de banda entre sí.

Cuando existe pérdida de paquetes se exige que el receptor pueda compensar los paquetes perdidos de una manera que oculte los errores en la máxima medida posible. Para datos y control, se utiliza retransmisión en la capa de transporte. Para audio y vídeo, la retransmisión queda en estudio.

La QOS de audio/vídeo percibida por el usuario resulta de la efectividad de los métodos utilizados para superar problemas de QOS de transporte.

Los informes de emisor y de receptor de RTPC (descritas en los protocolos de control) serán el medio por el que se evaluará la QOS.

Informes de emisor

El informe de emisor cumple tres fines principales:

1. Permite la sincronización de múltiples trenes RTP, tales como audio y vídeo;
2. Permite al receptor conocer la velocidad de datos y la velocidad de paquetes esperadas; y,
3. Permite al receptor medir la distancia en tiempo al emisor.

De estos tres fines, 1) es el más pertinente para esta Recomendación. Los fabricantes pueden utilizar los informes del remitente de otros modos a su discreción.

Informes de receptor

Se utilizan cuatro partes de los informes de receptor en esta Recomendación para medir la QOS:

1. Fracción perdida;
2. Los paquetes acumulativos perdidos;
3. El número secuencial más alto extendido recibido; y,
4. Fluctuación entre llegadas.

Los apartados 2) y 3) se utilizan para calcular el número de paquetes perdidos desde el informe de receptor anterior. Esta medida puede tomarse como una medida a corto plazo de la congestión de la red de paquetes. Si el apartado 1) sobrepasa un valor fijado por el administrador, puede también ser conveniente ejercer una acción correctiva.

El apartado 4) debe utilizarse como una indicación de congestión inminente. Si la fluctuación entre llegadas aumenta en tres informes de receptor consecutivos, el terminal emisor H.323 debe ejercer acción correctiva.

Procedimientos para mantener la calidad de servicio

Respuestas a corto plazo:

- Reducción de la velocidad de trama durante un breve período de tiempo;
- Reducción de la velocidad de paquetes por conmutación al modo opcional, en el que el audio/vídeo se mezclan en un paquete (queda en estudio).
- La velocidad de paquetes puede también reducirse mediante el uso de fragmentación MB del tren de vídeo.

Respuestas a más largo plazo:

- Reducción de la velocidad binaria de medios (Ej. conmutación de 384 kbit/s a 256 kbit/s): Estos cambios se señalizan mediante instrucciones control de flujo (FlowControl) H.245, o mediante señalización de canal lógico, según convenga;
- Desactivación de medios de menor importancia (Ej. Vídeo);
- Devolución de una señal de ocupado (ocupado adaptativa) al receptor como una indicación de congestión de la red de paquetes. Ocupado adaptativo es señalizado mediante un valor de causa Q.931 en Liberación completa (Release Complete).

6.7 RENDIMIENTOS VOIP CON H.323

Existen muchos puntos a evaluar para determinar el rendimiento de VoIP con H.323. Entre ellos se encuentra la interoperatividad real del protocolo después de que éste ya ha sido implementado, la calidad y la seguridad que ofrece y la aparición de un nuevo protocolo como es el SIP que viene con muchas ventajas sobre el H.323

6.7.1 Interoperatividad e Implementación

H.323 es largo, complejo y un estándar flexible. Una interpretación diferente o equivocada en la implementación dará como consecuencia dispositivos incompatibles o no obedientes. Este asunto es crítico y ha sido considerado el impedimento fundamental para el despliegue total de H.323 tanto en productos como en servicios. Además la ITU-T no provee una guía o línea directa a la que se pueda acudir en el momento de la implementación para asegurar la correcta implementación y por tanto la interoperatividad de los dispositivos. Todos los puntos finales deben ínter operar antes de que una llamada multimedia H.323 se establezca. Consideremos, por ejemplo, una llamada teléfono a teléfono sobre el Internet. Esta configuración implica que los teléfonos (terminales) estén ínter operando, los gateways estén ínter operando y que los teléfonos y sus respectivos gateways estén ínter operando. Si el puntofinal es de una marca de fabricación diferente es muy posible que ocurran problemas.

Soluciones Logradas

La baja interoperatividad de puntos finales H.323 es reconocida a nivel mundial. La IMTC (International Multimedia Teleconferencing Consortium) estableció como objetivo primario garantizar que los productos y servicios son ínter operables. La IMTC es una organización sin fines de lucro con más de 150 miembros que regularizan conductas de operatividad y prueban su conformidad en productos y servicios.

En 1998, ITXC, Lucent Technologies, y VocalTec establecieron el perfil iNOW! como una línea directa para consultas de implementación de gateway-to-gateway y terminal-to-gateway ínter operables. Recientemente, el Perfil de implementación iNOW! se convirtió en un grupo activo IMTC (http://www.imtc.org/act_inow.htm). El Perfil iNOW! ha incluido interoperatividad entre gatekeepers y otros puntos finales. Los productos y servicios que se adaptan a estas normas son certificados por la IMTC.

Varios vendedores de software tienen desarrollado pilas de protocolo H.323 para la mayoría de sistemas operativos. Estos módulos permiten a los desarrollares de productos y servicios H.323 trabajar con un alto nivel API (application programming interface) en lugar de niveles bajos como detalles de implementación, minimizando de esta manera los riesgos de interoperatividad. Entre los vendedores que ofrecen pila de protocolos H.323

están: -DataBeam, Trilium, Hughes, Software Systems, Elemedia, RAD Vision, OpenH323 Project.

6.7.2 Carencia de servicios de valor añadido

La visión de H.323 es una interoperabilidad global entre redes de paquetes y circuitos conmutados. H.323 también promete nuevos e integrados servicios de valor para los clientes usando tecnología de circuitos conmutados exclusivamente. Estos objetivos todavía no han sido logrados. Desde el punto de vista comercial una tecnología no puede tener éxito solamente en base a sus bajos costos operacionales. Debe también suministrar valor adicional y funcionamiento en el sentido de facilitar su uso y mejorar sus características para suplantar una tecnología rezagada como es la PSTN. El ITSP (Internet telephony service providers) y ISP (Internet service providers) se han anticipado para proveer este nivel de interoperatividad con mejores servicios y valores comparados al POTS (plain old telephone service). Sin embargo la calidad de servicios ofrecidos es aún inferior al POTS. Dos factores claves obstaculizan el esfuerzo de los ITSPs y ISPs. El primero es la carencia de interoperabilidad de puntos finales (especialmente gateways) de diferentes marcas. Y el segundo es la baja escalabilidad de las comunicaciones H.323.

6.7.3 Calidad y Seguridad

La calidad de vídeo en redes públicas como el Internet es pobre. Igual el audio sobre Internet no se compara al favorable de la PSTN. Sin embargo H.323 es un protocolo de capa alta y puede usar cualquier QoS que existan en las capas bajas. Por ejemplo una Red H.323 IP puede usar RSVP. El auge de codecs más eficientes también juega un importante papel para mejorar la calidad.

Los encargados de los departamentos de sistemas en las empresas son también renuentes a facilitar el despliegue de soluciones H.323 en voz e integración de datos a causa generalmente de la baja confianza que por su naturaleza ofrecen las redes basadas en paquetes en comparación con la PSTN.

La seguridad de las comunicaciones H.323 es también un gran asunto. Preocupa sobre manera la privacidad para comunicaciones intra e inter Oficina. Parte de este problema fue resuelto al introducir recomendaciones de seguridad en la Versión 2.0 del H.323 al incorporar la recomendación H.235.

6.7.4 Nuevos estándares para Voz sobre IP

La IETF (Internet Engineering Task Force) ha trabajado paralelamente al H.323 para establecer estándares para telefonía IP. El Protocolo SIP (Protocolo de Inicio de Sesión), definido en la RFC2543 es un nuevo protocolo que presenta muchas ventajas sobre el H.323.

6.7.4.1 SIP (Protocolo de inicio de la sesión)

El protocolo de inicio de sesión (SIP) se utiliza para establecer, mantener y terminar sesiones multimedia que incluyen telefonía Internet, las conferencias y otras aplicaciones similares que proporcionan medios como audio, vídeo y datos. SIP soporta sesiones unidifusión y multidifusión, así como llamadas punto a punto y multipunto. SIP puede operar en conjunción con otros protocolos de señalización, como el H.323.

SIP es un protocolo que por su versatilidad está preparado para futuros requerimientos como son posibilidades adicionales de señalización, pues la telefonía IP se sigue desarrollando. Además los mensajes SIP tienen una cabecera versátil y se pueden registrar funciones adicionales con la IANA (Agencia de asignación de números Internet), también permite que los elementos construyan servicios telefónicos avanzados, incluidos los servicios de tipo de movilidad.

La arquitectura de SIP es similar a la http (Protocolo Cliente – Servidor). Los requerimientos son generados por el cliente y enviadas al servidor. El SIP tiene entonces dos componentes que son los agentes de usuario y los servidores de red.

Los agentes de usuario son aplicaciones cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como cliente y servidor, respectivamente. El cliente inicia las peticiones SIP y el servidor genera la respuesta y la envía al cliente. Todas estas peticiones y respuestas están consideradas como parte de una transacción SIP. Las partes que llaman y son llamadas se identifican con direcciones SIP.

Existe dos tipos de servidores de red SIP:

- Servidor proxy: Recibe el requerimiento y lo reenvía al siguiente servidor el cual tiene información acerca de la localización de la parte llamada; y,
- Servidor de redirección. Recibe el requerimiento, determina el siguiente servidor y devuelve la dirección del siguiente servidor al cliente en lugar de reenviar el requerimiento.

Las direcciones SIP, llamadas también localizadores universales de recursos (URL) SIP, existen en la forma de usuarios @ hosts. Similar a una dirección de correo electrónico en URL. La parte de usuario puede ser un nombre de usuario o número telefónico y la parte de host puede ser un nombre de dominio o una dirección de red. Ej. Sip:ciscopress@cisco.com ó sip:408562222@171.171.171.1

La localización de un servidor se realiza enviando una petición SIP directamente a un servidor proxy configurado localmente o bien a la dirección IP y puerto del correspondiente URL SIP. Una vez que se tiene la dirección, el cliente envía una o más peticiones SIP y recibe una o más respuestas desde el servidor especificado. Las transacciones SIP puede ser transmitidas en los protocolos UDP y TCP.

Las facetas para establecer una comunicación con SIP son los siguientes:

1. Localización de usuario. Determina el punto final a ser usado para la comunicación;
2. Capacidad de usuario: Determina el medio y los parámetros del medio a ser usados;
3. Disponibilidad de usuario: Determina la disponibilidad de la parte llamada para dar lugar a la comunicación;
4. Configuración de la llamada. Timbra y establece parámetros de llamada;
5. Manejo de la llamada: Transferencia y terminación de llamadas.

SIP presume de tener algunas ventajas sobre H.323, tales como una configuración de la llamada más rápida y menos compleja, una implementación parecida a http con una arquitectura modular que contiene funciones que residen en protocolos separados. La implementación de SIP es también “sin estado”, lo que significa que los servidores no necesitan mantener el estado de la llamada.

SIP define los siguientes mensajes:

- INVITE para invitar a un usuario para una llamada;
- BYE para terminar una conexión entre dos puntos;
- ACK para confirmar el mensaje de invitación;
- OPTIONS para tomar información acerca de las capacidades de la llamada;
- REGISTER toma información acerca de la localización de un usuario para registrarlo en el servidor SIP;
- CANCEL para terminar la búsqueda de un usuario.

6.7.4.2 H.323 o SIP?

La recomendación H.323 tiene vigencia desde 1996, pero ha fallado para capturar el mercado. El Protocolo SIP (Protocolo de Inicio de Sesión), definido en la RFC2543 para establecer comunicaciones multimedia ha ganado impulso. SIP propone los siguientes aspectos que tienen su ventaja sobre H.323:

- Basado en IP. IP es el protocolo dominante en el Internet. Como consecuencia, la interoperatividad con ATM y ISDN no es cuestionada;
- H.323 lleva mucho equipaje para asegurar que esta interoperatividad con otros estándares en las series. SIP es libre de estos extras, raramente necesita equipaje;
- Baja complejidad. SIP es un estándar mucho más pequeño y menos complicado porque esta basado en una arquitectura de protocolos de conocimiento público como es el http y FTP. Por otra parte, H.323 es largo y complicado. Como resultado los productos y servicios H.323 no se han expandido;
- Fácil para decodificar/depurar. SIP usa un simple formato para comandos y mensajes. Estos son cadenas de textos que son fácilmente decodificados y, por lo tanto, fáciles de depurar. El conjunto completo de mensajes es también mucho menor que en H.323;
- Arquitectura Cliente / servidor. Los mensajes SIP son intercambiados entre un cliente y un servidor parecido a los mensajes http. Este modo de operación cliente servidor permiten seguridad y control, características implementadas fácilmente en SIP en comparación con las llamadas H.323;
- Fácil diseño y configuración de firewall/proxy. Los comandos SIP pueden fácilmente ser interpretados por servidores Proxy y firewalls, los mismos que

pueden ser diseñados para habilitar/deshabilitar comunicaciones SIP. Recibir H.323 a través de firewalls y proxies es mucho más complicado;

- Extensible y escalable. Como el SIP esta basado en arquitectura distribuida cliente/servidor es mas escalable que H.323 que a menudo requieren comunicaciones punto a punto. El simple formato de los mensajes SIP y la gran experiencia con protocolos similares como el http lo hacen fácilmente extensible.

Analistas a menudo hacen una analogía entre H.323 y ATM como estándares que ofrecen demasiado en un corto plazo, el mercado no estuvo listo para ellos. SIP y H.323 coexistirán en productos y servicios en los años venideros.

6.7.5 Futuros desarrollos en H.323

El estándar H.323 aún está en desarrollo. La versión 2.0 fue lanzada en Enero de 1998 y se está trabajando continuamente en añadir nuevas características. El punto fue cambiar desde LANs a grandes redes como el Internet y el reto que lo asocia. Se trabaja también en incluir capacidades de comunicación móvil y la interoperatividad con GSM, como estándares en comunicación inalámbrica. Otra iniciativa es la preparación de una guía de implementación para facilitar la interoperatividad.

Capítulo 7 GATEWAYS Y GATEKEEPER

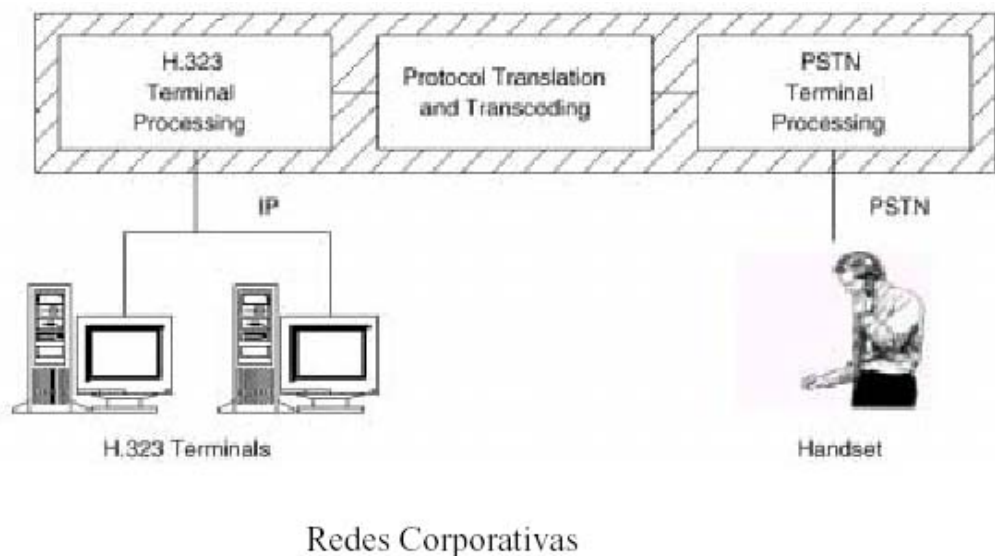
Como se vió en el capítulo anterior, los gateways y gatekeeper son elementos en una arquitectura H.323, en este capítulo se detallarán las funciones que cada uno de ellos realiza.

7.1 GATEWAY (GW)

En general se trata de una pasarela entre dos redes. Técnicamente se trata de un dispositivo repetidor electrónico que intercepta y adecua señales eléctricas de una red a otra. En Telefonía IP se entiende que estamos hablando de un dispositivo que actúa de pasarela entre la red telefónica y una red IP. Es capaz de convertir las llamadas de voz y fax, en tiempo real, en paquetes IP con destino a una red IP, por ejemplo Internet.

Originalmente sólo trataban llamadas de voz, realizando la compresión/descompresión, paquetización, enrutado de la llamada y el control de la señalización. Hoy en día muchos son capaces de manejar fax e incluir interfaces con controladores externos, como gatekeepers, soft-switches o sistemas de facturación

Un gateway realiza funciones de interconexión entre sistemas H.323 y sistemas de otro tipo (Por ejemplo redes ISDN o PSTN). El gateway es un elemento opcional en una conferencia H.323 cuyo propósito general es el reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.



Los gateway VoIP dependiendo del fabricante pueden ofrecer los siguientes tipos de conexiones:

- Teléfono-Teléfono
- PC-Teléfono
- Teléfono-PC
- Fax – Fax

Los gateways utilizan técnicas de compresión y descompresión de voz para minimizar el ancho de banda requerido para la transmisión de los paquetes de voz sobre la red, estas técnicas están implementadas según los estándares G 711, G.723, etc.

Un gateway VoIP puede encaminar todas las llamadas recibidas hacia la red IP, o bien capturar el tráfico de salida de la centralita y desviar el tráfico corporativo hacia la Red IP, conmutando transparentemente el resto de las llamadas hacia salidas analógicas de RTC.

Permite a las oficinas remotas realizar comunicaciones entre cualquier combinación de teléfonos analógicos, conectados directamente al gateway a través de centralita, cursar faxes convencionales o comunicar teléfonos con PCs multimedia.

Para comunicaciones no corporativas, el gateway puede reencaminar el tráfico hacia la Red Telefónica Convencional (RTC) o bien dialogar con cualquier sistema remoto conectado a la Internet/Intranet, siempre que se ajuste a los estándares H.323 (gateways de otros fabricantes, PCs con Microsoft Netmeeting, teléfonos Ethernet, etc.).

Gateway de medios (MG)

El gateway de medios lleva a cabo las siguientes funciones:

- Terminación física de la instalación T1/E1 TDM desde la PSTN o PBX (Private Branch eXchanges);
- Comunicación con el VSC para la configuración y borrado de la llamada utilizando SGCP o MGCP;
- Cancelación de eco en la red de circuito conmutado;
- Equilibrado de los búferes de fluctuación de fase.

Gateway residencial

El gateway residencial es un dispositivo de equipo terminal del abonado (CPE) de voz y datos que proporciona entre dos y cuatro puertos de capacidad de Servicio telefónico analógico convencional (POTS).

7.2 GATEKEEPER (GK)

El Gatekeeper es una entidad que realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN. El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

Las funciones obligatorias del gatekeeper son:

- Traducción de Direcciones
 - De números de teléfonos o nombres a direcciones de red
- Control de Admisión
 - Autorización de uso a los diversos dispositivos (terminales, gateways, MCU'S)
- Control de Ancho de banda
 - Manejo del ancho de banda permitido para cada servicio y/o teminal.

Funciones opcionales del gatekeeper:

- Autorización de llamadas
- Control de llamadas (con fines administrativos – costos)
- Control de la señalización

Capítulo 8 Ventajas y aplicaciones de Voz sobre IP

Integrar redes de voz y de datos es beneficioso en muchos sentidos, comenzando por el ahorro económico en llamadas de largar distancia. A continuación se describen las principales ventajas de tener una infraestructura de red con VOIP.

8.1 PRINCIPALES VENTAJAS

El ahorro económico se ha convertido en la principal razón para combinar las redes de voz y de datos.

Al utilizar teléfonos IP se puede ahorrar el costo de mover el teléfono de un lugar a otro. En una infraestructura IP se pueden utilizar funciones de datos como el Protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol). El DHCP permite que un dispositivo reciba dinámicamente una dirección IP, por lo tanto, si se tiene un teléfono IP configurado con DHCP, se puede mover el teléfono de un lugar a otro y éste mantendrá el mismo número de teléfono.

Con una infraestructura VOIP existe la posibilidad de tener un departamento de Servicio de Información (IS, Information Services) que soporte ambas redes de voz y datos.

Los puertos físicos para servicios como el correo de voz podrán ser reemplazados por un servidor de correo de voz que tenga una conexión IP.

8.2 OTRAS VENTAJAS

Algunas otras ventajas que se pueden obtener con VoIp:

- Integración sobre su intranet de la voz como un servicio más de su red, tal como otros servicios informáticos;
- Las redes IP son la red estándar universal para la Internet, intranets y extranets;
- Interoperabilidad de diversos proveedores;
- Uso de las redes de datos existentes;

- Independencia de tecnologías de transporte (capa 2), asegurando la inversión;
- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay).

8.3 APLICACIONES DE VOIP

Algunas aplicaciones de VoIP son las siguientes:

- **Clic-2-Dial**, permite a las empresas poner un enlace en sus sitios web que pasará automáticamente la llamada de un cliente a un representante comercial;
- **Microsoft Netmeeting**, permite integrar servicios de teléfono tradicionales con aplicaciones compartidas y videoconferencias basadas en H.323;
- **El teléfono IP de Cisco**, tiene la apariencia y comportamiento de un microteléfono tradicional con la funcionalidad añadida de la conectividad IP. Un teléfono IP al funcionar en conjunción con los PBX basados en IP puede utilizar no sólo los servicios de VoIP sino también cualquier otra aplicación multiservicio basada en IP que esté disponible en la red;
- Los **soft-phones** basados en PC de Cisco amplían la funcionalidad del microteléfono en el PC con una interfaz gráfica de usuario que proporciona la misma funcionalidad que el microteléfono y se integra con otras aplicaciones multiservicio como el navegador web, Netmeeting o los servicios de directorio basados en el protocolo ligero de acceso a directorios (LDAP, Lightweight Directory Access Protocol). El Soft-phone utiliza auriculares y altavoces lo que elimina la necesidad de tener un microteléfono en cada puesto informático;
- **Real Server/Playern** Esta herramienta también se basa en el empleo de RTP y tiene la ventaja de que puede arrancarse vía Web. Sin embargo, su principal problema reside en el hecho de que no permite interacción. Los receptores deben limitarse a atender a las sesiones sin poder en ningún momento interaccionar con el interlocutor.

Capítulo 9 Soluciones de Proveedores

Hoy en día hay fabricantes de equipos de Voz sobre IP que ofrecen las siguientes alternativas de solución:

- Un sistema que consta de tres componentes: Hardware que conecta el teléfono a la PC, Software que convierte la voz en paquetes de IP y un Gateway encargado de enviar los paquetes de voz sobre IP a través de las redes públicas;
- Un sistema que conecta directamente el PBX a la red IP; esto se realiza por medio de un Gateway de voz sobre IP contenido en una tarjeta que puede ser colocada en un equipo o PC, estas tarjetas pueden soportar una o dos llamadas simultáneas FXS, FXO o E&M, o bien soportar 24 llamadas simultáneas sobre una tarjeta T1 ó 30 llamadas sobre una tarjeta E1.

Para las soluciones de redes privadas en las que se requiere tener beneficios en el costo de la red para el transporte de tráfico de voz y datos sobre enlaces de 64 Kbps, la tecnología de voz sobre IP es la alternativa viable de solución ya que ofrece compresión de voz a 16 ó 8Kbps (16 Kbps representa muy buena calidad y 8 Kbps representa aceptable calidad) que permitirá explotar el ancho de banda para el transporte de voz y datos. Además, con la supresión de silencios, la voz sobre IP ofrece aprovechar más el ancho de banda al eliminar todos los paquetes vacíos originados durante una llamada telefónica.

9.1 MOTOROLA

MOTOROLA es un fabricante de equipos de comunicación que en nuestro medio tiene gran acogida.

MOTOROLA propone dos caminos para minimizar los costos de comunicaciones: por un lado, con equipos flexibles, capaces de adaptarse a distintos entornos LAN (Ethernet, Token Ring, SDLC) y WAN (X.25, FR, PPP); y por otro, con equipos con capacidad de tráfico multimedia (voz y vídeo), a fin de sacar el máximo rendimiento de las líneas de comunicaciones.

Los equipos de Motorola son a la vez router y conmutador y pueden comunicarse utilizando redes WAN, públicas o privadas, de líneas punto a punto, RDSI, X.25, Frame Relay o IP. Además, dependiendo del modelo, los routers de Motorola tienen interfaces

Ethernet, Token Ring, Serie y RDSI. Este amplio abanico de interfaces, junto con las funcionalidades de routing disponibles (RIP, OSPF, NAT), permiten procesar distintos tipos de tráfico con un único equipo.

Por otro lado, Motorola ofrecer la posibilidad de aumentar el rendimiento de los enlaces de datos mediante la multiplexación de datos, voz y vídeo vigilancia, con el consiguiente ahorro de costes que ello implica.

En 1.995 MOTOROLA fue la pionera en integrar la transmisión de voz en redes WAN Frame Relay. En la actualidad Motorola tiene una completa gama de equipos VoIP, que utilizan tanto protocolos propietarios (SoTCP) como protocolos estándar (H.323).

Los equipos de Motorola ofrecen una calidad excelente en transmisión de voz, tanto analógica (FXS, FXO, E&M) como digital (T0, E1), sobre líneas Frame Relay y/o IP.

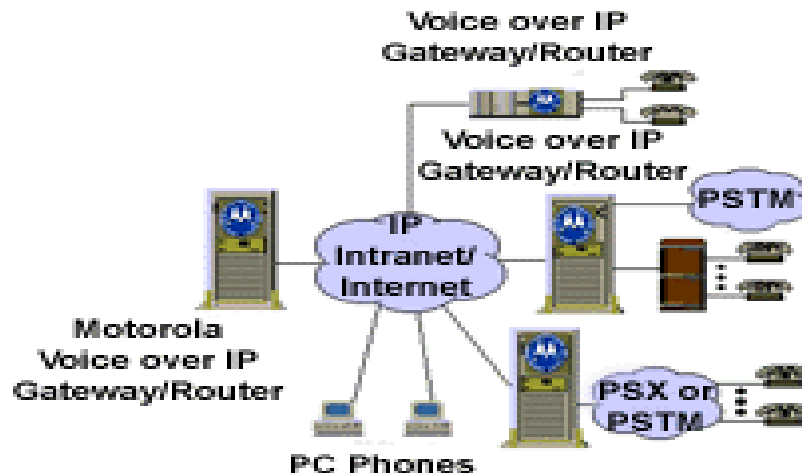
Hoy en día Motorola ofrece soluciones de voz sobre redes Frame Relay y voz sobre redes IP con el mismo equipo, incluso de manera simultánea. Este hecho permite a los equipos de Motorola funcionar de forma simultánea como VoIP Gateway y router voz/datos sobre Frame Relay.

Los equipos de Motorola que soportan VoIP son:

- Vanguard 320/6430/6450 para el manejo de canales de voz FXO o FXS en tarjeta Daughtercard;
- MPRouter 6560/6520 para el manejo de canales de voz FXO, FXS, E&M, T1 y E1 (la conexión hacia PBX con soporte de señalización CAS y Canal Común).

Para la aplicación de voz sobre IP, los equipos Motorola encapsulan la voz en tramas de IP para ser transmitidas hacia el puerto de la tarjeta Ethernet ELAN la cual se encargará del ruteo de los paquetes hacia la red IP, como se muestra en el siguiente diagrama:

SOLUCION MOTOROLA Aplicación de Voz Sobre IP



La solución de voz sobre IP de Motorola soportan las siguientes facilidades:

- Alta calidad en la compresión de voz a 8 Kbps y 16 Kbps para audio compresión;
- Cancelador de eco y supresión de silencio integrados Voice Switching para el ruteo de llamadas en la red Plan de marcación flexible.

9.2 CISCO

CISCO es el segundo proveedor que hemos analizado, y hace frente a la competencia de otros fabricantes no solo con equipos VoIP sino que también ha desarrollado un servicio de soporte llamado AVVID.

A través del Servicio y soporte Cisco AVVID Architecture for Voice, Video and Integrated Data), Cisco trabaja con cada cliente para crear un "mapa de carreteras" individualizado que conduce a una migración rápida de datos, voz, y vídeo sobre una red única y convergente. Para que esta solución sea prometedora CISCO pone a disposición de los clientes su equipo de socios en todo el mundo.

CISCO es quizá el mayor fabricante de equipos de comunicación en todo el mundo y la gama de productos que saca el mercado en cuanto a VoIP son muy variadas dependiendo de la solución requerida por el cliente.

Dentro de las soluciones que Cisco presenta tanto para las empresas pequeñas, medianas y grandes se encuentran las siguientes:

9.2.1 Soluciones Pequeñas

Para las pequeñas empresas el internet y la convergencia de las redes de comunicaciones pueden ser de mucha ayuda en esta economía de rápidos cambios, en una red integrada de voz, video y datos se pueden reducir los costos e ir preparando la empresa para el futuro.

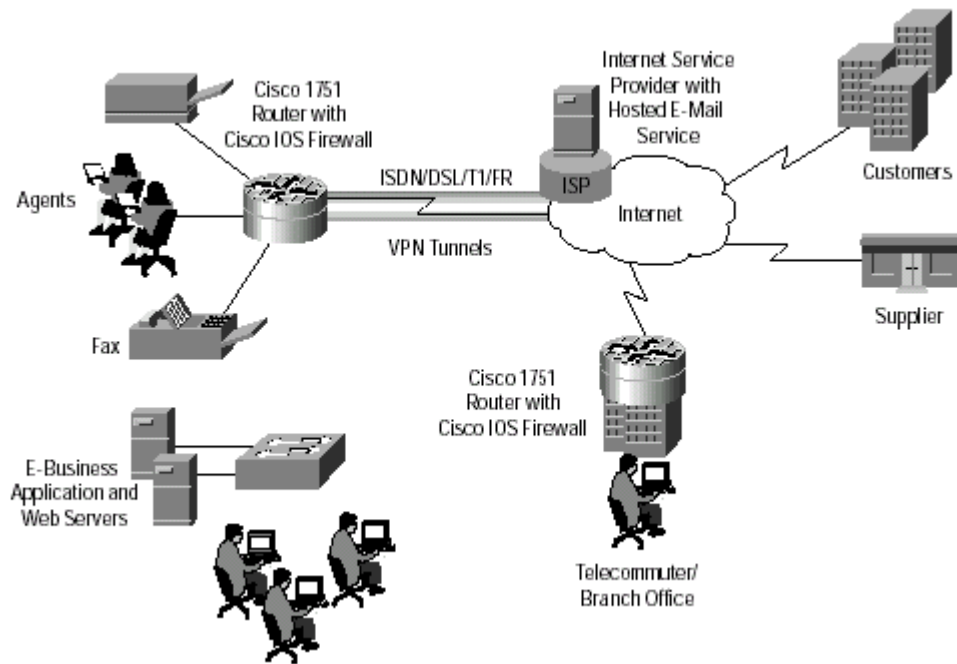
Basados en el Cisco AVVID (Architecture for Voice, Video and Integrated Data), los siguientes pasos pueden ser utilizados por las organizaciones para integrar en sus redes de datos tráfico de voz:

1. Cambiar las llamadas de voz y de fax que están por la red de telefonía pública a la red de datos con routers habilitados para transmitir voz;
2. Invertir en switch de LAN listos para telefonía IP, preparando el camino para que todo el tráfico de llamadas en la oficina y el que está a través de ella esté sobre la red de datos;
3. Mover todo el modelo de las comunicaciones para que operen completamente en Voz sobre IP, incluyendo IP o redes de PBX y teléfonos de la organización que puedan recibir beneficios de las nuevas aplicaciones de la telefonía.

Para esto Cisco ofrece un completo paquete de soluciones multiservicio para empresas pequeñas que igualmente son robustas, escalables y confiables como una solución a gran escala.

Desde nuestro punto de vista los routers que podrían brindar servicio de voz sobre IP para empresas pequeñas en nuestro medio serían los router Cisco de la familia 17xx, que tienen las siguientes características:

- Flexibilidad para adaptarse a los cambios de requerimientos;
- Modularidad ya que permite configuraciones individuales del sistema para las necesidades de negocios específicos;
- Protección con características y desempeño que soportan nuevas WAN, servicios de banda ancha como DSL y acceso por cable, multiservicios como la integración de voz y datos, y VPN's;
- VLAN's soporta (IEEE 802.1Q).



9.2.2 Soluciones Medianas

Las empresas medianas con manejadores de redes preparan ya sus redes para el tráfico de voz, ellos necesitan diseños más robustos que el de las empresas pequeñas.

Para negocios medianos que están ya en capacidad de desarrollar telefonía IP, se ha desarrollado el Cisco Integrated Communications System (ICS) 7750 que sería una plataforma ideal en la que se construiría un sistema VoIP sobre una base abierta y escalable Cisco AVVID.

Al igual que en el caso anterior desde nuestro punto de vista los routers que pueden dar el servicio de VoIP para el tipo de empresas medianas de nuestro medio son los routers de la serie 36xx.

Los ruteadores Cisco 3600 son la primera plataforma multifunción con la versatilidad necesaria para utilizarla con aplicaciones de acceso telefónico, aplicaciones LAN a LAN, aplicaciones de enrutamiento y aplicaciones multiservicio en una sola plataforma. Este sistema ofrece opciones de modularidad y cuenta con una amplia gama de módulos de red, flexibilidad con diversas configuraciones para las aplicaciones específicas de cada cliente, con una alto rendimiento.

9.2.3 Soluciones Grandes

Para las empresas grandes que tienen varias sucursales dispersas en un área geográfica amplia, la construcción de una infraestructura para utilizar voz sobre las líneas de datos se convierte en una efectiva opción para disminuir los costos y para facilitar nuevas aplicaciones. La voz y los datos de red equipados para varias sucursales debería proveer de una amplia variedad de interfaces, versatilidad, y un balanceado mix de precio-desempeño que necesitaría cada una de las sucursales.

Con la solución de Cisco de voz sobre datos, las compañías pueden realizar la migración del tráfico de voz en fases de acercamiento que reúnan de mejor manera los objetivos del negocio.

1. Asegurarse de que tienen una red LAN que puede soportar sin problemas el tráfico de voz.
2. Pasar el tráfico de voz del PBX sobre el backbone de WAN habilitando los routers de voz.
3. Adicionar telefonía IP para las sucursales de la LAN .

Los routers que se pueden utilizar para este tipo de organizaciones, son routers que deben presentar mucho mejores características, versatilidad y desempeño como serían los routers cisco de la serie 70xx.

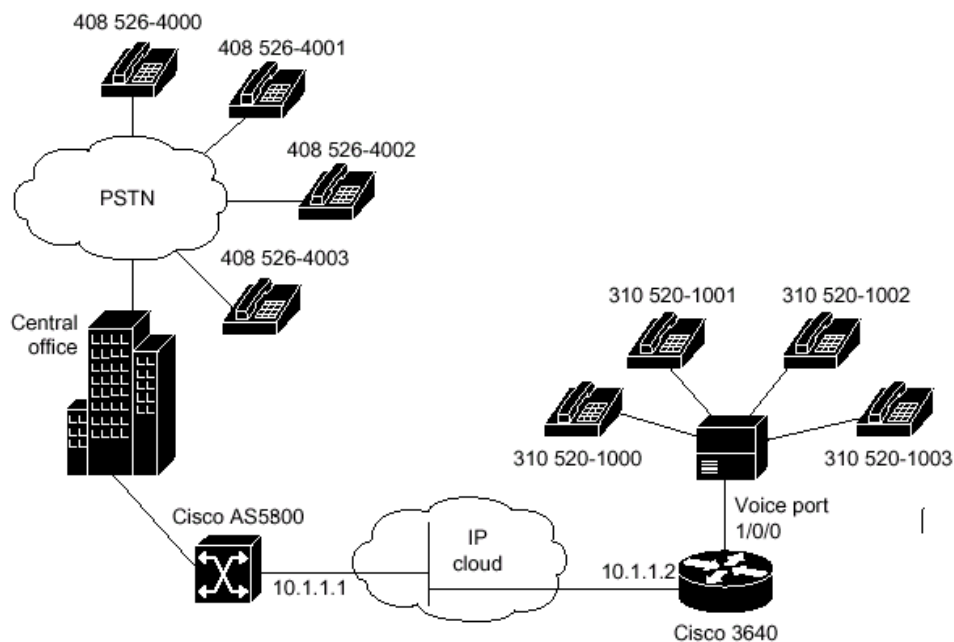
Los routers cisco 7200 satisfacen estos requerimientos ya reúne en una sola plataforma de bajo costo las funciones que antes desempeñaban varios dispositivos independientes. Mediante la integración de funciones, la plataforma de multifunción de alto rendimiento Cisco 7200 ofrece una sola plataforma con las siguientes características:

- Interfaces LAN y WAN de alta densidad;
- Conectividad ATM y packet over SONET;
- Conectividad directa Circuit Emulation Standard (CES) ATM para voz, datos y video;
- T3/E3 y T1/E1 multicanal de alta densidad con una unidad de servicio canal/unidad de servicio de datos (CSU/DSU) integrada;
- Conectividad directa con el canal del procesador central de IBM;
- Commutación Ethernet capa 2 de baja densidad;

- Conectividad digital con el codificador-descodificador de voz y vídeo (CODEC) de centralitas telefónicas (PBX) T1/E1.

9.2.4 Otras soluciones

El Equipo Cisco 5800 es un servidor de acceso de la serie Cisco AS5x00 de clase portadora que proporciona la mayor concentración de terminaciones de módems, voz y RDSI. Cisco AS5800 se ha diseñado especialmente para satisfacer las exigencias de los grandes proveedores de servicios, como son las operadoras de correo, teléfono y telégrafos, empresas telefónicas regionales y grandes proveedores de servicios Internet (ISP). El Cisco 5800 admite un máximo de 2.016 llamadas (3 x CT3) con lo que ofrece características de alta disponibilidad: intercambio en actividad para todas las tarjetas, fuentes de alimentación redundantes y con reparto de carga, controladores de estante de acceso telefónico y estantes de routers que garantizan una disponibilidad de un 99,999 por ciento.



El gateway de voz de Cisco AS5800 permite una distribución altamente ampliable de servicios de voz y fax de calidad telefónica a través de redes de datos. Admite aplicaciones como tarjetas telefónicas post y prepago, redirección de llamadas 800, marcación activada por voz, correo de voz y correo por fax. El gateway de voz Cisco AS5800 admite un máximo de 1.344 puertos de voz en un sistema individual, con lo que ofrece la mayor concentración de capacidad de VoIP de todos los gateways de voz individuales.

Las características de telefonía de paquetes de Cisco permite ofertar servicios de voz a través de una infraestructura IP. Los servicios ofrecidos son los siguientes: desviación de llamadas, teléfono del PC a PSTN, correo de voz, correo de fax, fax en tiempo real y servicios administrados para los servicios de llamadas y fax dentro de la propia empresa.

Cisco también provee los Teléfonos IP. La serie de teléfonos IP de Cisco se compone de dispositivos de comunicaciones basados en los estándares. El teléfono IP de Cisco puede interoperar con los sistemas de telefonía IP basados en la tecnología Cisco CallManager, H.323 o el protocolo Session Initiative Protocol (SIP) y (en el futuro) el protocolo Media Gateway Control Protocol (MGCP), con sencillas actualizaciones del software (firmware). Esta capacidad multiprotocolo es una primicia en la industria y proporciona protección de la inversión y capacidad de migración.

Conclusiones

La tecnología de Voz sobre IP es nueva alternativa que está revolucionando el mundo de las comunicaciones, su fortaleza radica en la disminución de costos de planillas telefónicas.

En nuestro medio, el despliegue de esta tecnología se ha visto obstaculizado pues los costos de los enlaces entre los puntos que se desea implementar son muy altos, pero aún así, para empresas medianas y grandes el costo de los enlaces se ve recompensado por el ahorro que representa el no utilizar el servicio telefónico prestado por las empresas nacionales. Entre las empresas que han implementado o que están implementando VoIP podemos mencionar las siguientes: Centro Cerámico, Ecuaelectricidad, Hidropaute, Imprenta Monsalve Moreno.

En cuanto a VoIP utilizando la red de Internet está siendo muy prometedor para comunicarse con personas que viven en el exterior. Comparando costos en una llamada a Europa utilizando el servicio de Net2Phone el costo por minuto es de US \$ 0.25 desde un café internet y de USD \$ 0.11 desde un computador personal (al que se le debe sumar el costo de la llamada local de conexión al ISP), y utilizando los servicios de Etapa es de USD \$ 0.35.

Es necesario mencionar que no todas las redes IP están preparadas para brindar una buena calidad de servicio en la transmisión de VoIP:

- Internet. El estado actual de la red no permite un uso profesional para el tráfico de voz;
- Red IP pública. Esta red ofrece a las empresas la posibilidad de interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad;
- Intranet. Es una red IP implementada por la propia empresa. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

La definición de estándares están orientados a lograr la interoperabilidad entre equipos de diferentes fabricantes logrando de esta forma que los usuarios tengan una gama más amplia de opciones en cuanto a equipos en el mercado.

Las marcas de ruteadores más utilizados en nuestro medio para la implementación de VoIP en enlaces particulares son Cisco y Motorola debido a la fiabilidad y al prestigio que han logrado.

PARTE II

PRACTICA: IMPLEMENTACION VoIP

En la segunda parte de esta tesis se describe la parte práctica que consistió en establecer un enlace VoIP mediante la configuración de los equipos en una empresa de la ciudad que posea la infraestructura necesaria para la implementación de VoIP.

IMPLEMENTACIÓN DE VOIP

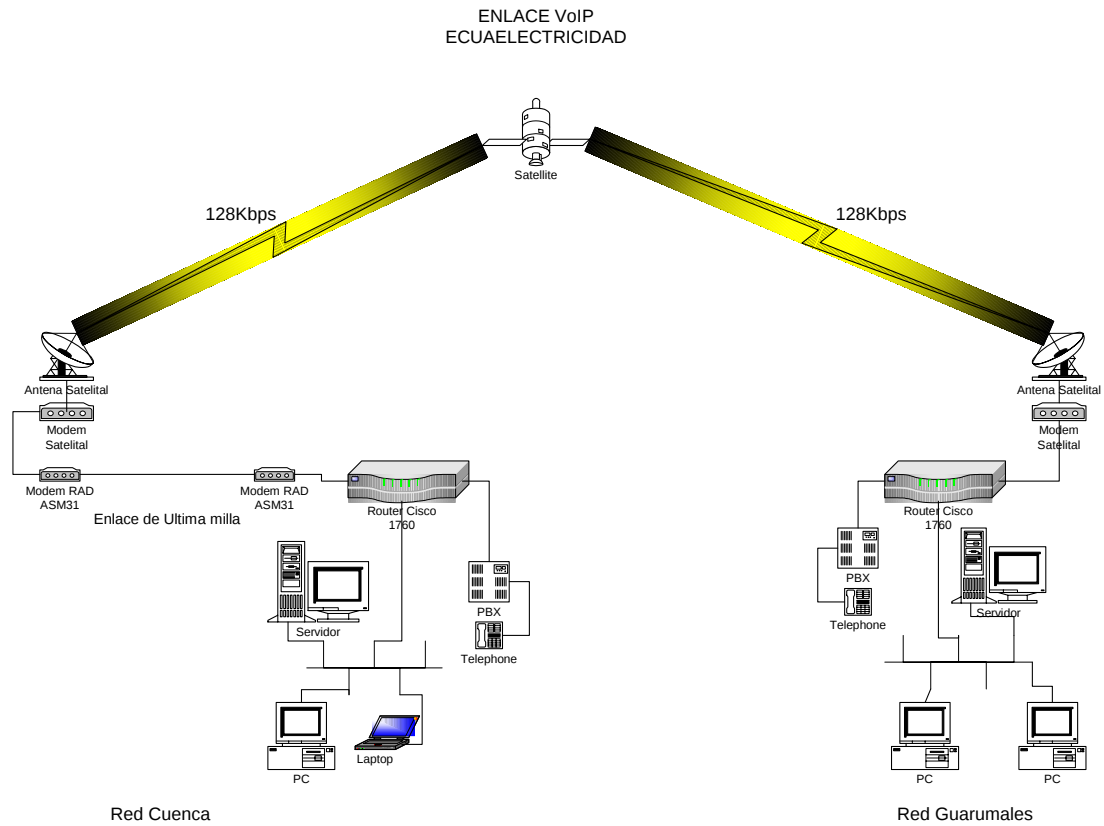
Para poder desarrollar la parte práctica se buscó una empresa que posea la infraestructura necesaria para poder montar la tecnología VoIP. ECUALECTRICIDAD es una empresa que posee esta infraestructura y que necesitaba ahorrar costos de comunicación con sus instalaciones en Guarumales, y de esta forma aprovechar óptimamente la red que se tiene montada para la transmisión de datos entre los dos extremos, con estos antecedentes procedieron a adquirir los routers VoIP 1760 adecuados para poder implementar el proyecto que describimos a continuación.

CONFIGURACION DE LA RED DE DATOS

La empresa Ecuaelectricidad posee un enlace satelital de 128kbps entre sus oficinas de Cuenca y Guarumales. A continuación damos una breve explicación sobre los equipos utilizados para este enlace tanto por parte de la empresa carrier (que brinda el servicio de enlace), como también de Ecuaelectricidad.

Ecuaelectricidad está utilizando para la comunicación entre sus dos puntos (Cuenca, Guarumales) routers Cisco de la serie 1760, con tarjetas VICs de voz, los routers están trabajando con la versión Cisco IOS Release 12.2.

En lo que respecta a la parte del enlace en Cuenca, la red local se conecta con el nodo satelital del proveedor de enlace (SURATEL) por medio de una LP de última milla con un par de módems (ASM31), el módem ASM31 que recibe el enlace en el nodo de SURATEL se conecta a su vez al módem satelital(SDM300), en Guarumales recibe la señal otro MODEM satelital (SMD300) que se conecta directamente al router Cisco.



Nuestro interés se centrará en la función VoIP que realizan los equipos Cisco 1760 y los comandos utilizados para este propósito.



Router Cisco 1760

A continuación detallamos algunas características relacionadas con VoIP de los equipos Cisco 1760.

Todos los modelos Cisco 1760 disponen de cuatro ranuras modulares para tarjetas de interfaz de voz y datos, dos puertos pueden ser usados por tarjetas WIC's o VIC's o la combinación de ambas, los otros dos pueden ser usados por tarjetas VIC's, un puerto de detección automática Ethernet 10/100 BaseT, un puerto de consola y un puerto auxiliar.

Las tarjetas de interfaz de voz incluyen compatibilidad con Foreign Exchange Office (FXO), Foreign Exchange Station (FXS) y Ear & Mouth (E&M). Estas interfaces se combinan para admitir a un conjunto completo de aplicaciones, incluyendo integración multiservicio de voz/fax/datos, Frame Relay, acceso básico ISDN (RDSI), SMDS, X.25, servicios de banda ancha DSL y cable, VPN y otros.

Las ranuras modulares de voz y datos permiten a los usuarios definir servicios de voz y datos de acuerdo con sus necesidades.

Gracias a la capacidad del router Cisco 1760 para proporcionar una sólida compresión de voz, seis llamadas de voz pueden ocupar un solo canal de 64K de modo simultáneo, sin que esto afecte al rendimiento de los datos.

Compatibilidad de Codec: G.711, G.729, G.729a, G.723.1, G.726

COMANDOS UTILIZADOS PARA LA CONFIGURACIÓN DE VOIP

A continuación detallamos los comandos correspondientes a la configuración de VoIP de los ruteadores utilizados en este enlace.

Voice-port

Este comando nos permite entrar en el modo de configuración de la interfaz de voz en el ruteador.

Description

El comando description nos permite ingresar una cadena de caracteres en la interfaz de voz la cual nos describe acerca de la conexión de dicha interfaz.

Dial-type

Este comando nos permite especificar el tipo de marcado que se utilizará, este puede ser: dtmf ó pulse.

- dtmf: Marcación por tonos
- pulse: Marcación por pulsos

Dial-peer voice

Se utiliza este comando para especificar el método de encapsulación relacionada con la VoIP que puede ser VoIP y POTS.

Destination-pattern

Este comando nos permite configurar el número telefónico utilizado para el dial-peer.

Session Target

Se utiliza este comando para especificar una dirección de red específica para el dial-peer.

También hacemos una breve descripción de los comandos que nos permiten revisar la configuración de las interfaces de voz y de comandos que nos indican en estado de la comunicación.

Show call active voice

Use este comando para mostrar una tabla con todas las llamadas actualmente conectadas a través del router. Este comando debe ser utilizado en el modo privilegiado.

Show call history voice

Este comando nos permite tener una tabla con un listado en orden descendente de todas las llamadas conectadas a través de este router. Este comando debe ser utilizado en el modo privilegiado.

Show controllers voice

Este comando se usa para desplegar información correspondiente al estado de la interfaz, específicamente sobre el hardware relacionado con la voz. Este comando debe ser utilizado en el modo privilegiado.

Show diag

Este comando despliega información para la EEPROM, motherboard, WAN cards y VICs cards. Este comando debe ser utilizado en el modo privilegiado.

Show dial-peer voice

Este comando despliega la configuración de todos los VoIP y POTS dial-peers configurados en el ruteador. Este comando debe ser utilizado en el modo privilegiado.

Show num-exp

Utilice este comando para desplegar todos los números de expansión configurados para este ruteador. Este comando debe ser utilizado en el modo privilegiado.

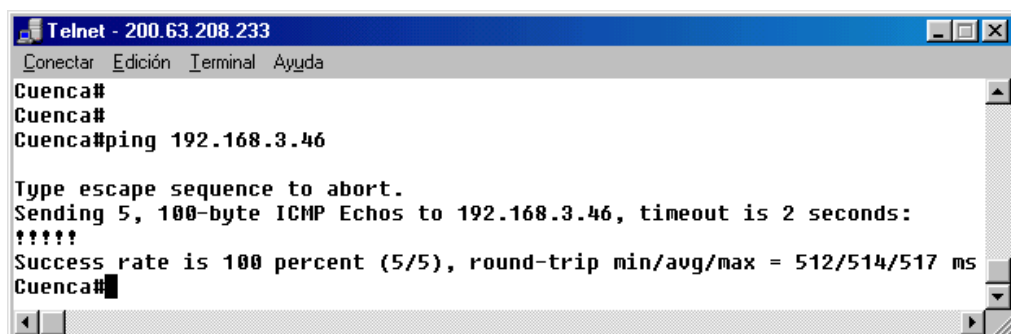
Show voice porte

Este comando despliega configuración y VIC-especificados acerca de un puerto específico.

PRUEBAS Y EJECUCIÓN

En lo que se refiere a las pruebas y ejecución, las misma se han centrado que en el enlace entre Ecuaelectricidad Cuenca y Guarumales, este enlace tiene un retardo promedio de 514 ms, hay que tomar en cuenta que se trata de un enlace satelital.

El siguiente es un gráfico de una prueba de ping desde el router de Ecuaelectricidad Cuenca hacia el router de Guarumales.



```

Telnet - 200.63.208.233
Conectar Edición Terminal Ayuda
Cuenca#
Cuenca#
Cuenca#ping 192.168.3.46

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.46, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 512/514/517 ms
Cuenca#

```

Actualmente se encuentra funcionando el enlace con dos canales de voz, conectados de la siguiente forma.

En el ruteador cisco 1760 de Ecuaelectricidad Cuenca se encuentra instalada una tarjeta de voz con 2 puertos FXS, los mismos que se encuentran conectados a troncales de la central telefónica. En el caso del ruteador de Guarumales se encuentra instalada una tarjeta de

voz con 2 puertos FXO, los mismos que se encuentran conectados a extensiones de la central telefónica.

Por medio de esta conexión se puede establecer dos llamadas simultaneas entre Cuenca y Guarumales, sobre las cuales se han realizado las pruebas correspondientes al canal de voz, encontrandose en perfecto funcionamiento.

Con respecto a las configuraciones que mantienen ambos ruteadores, estas se hallan descritas en el ANEXO 1.

CONCLUSIONES Y RECOMENDACIONES TÉCNICAS

Es importante tener en cuenta que la configuración expuesta es para equipos CISCO 1760 que son los que se utilizaron para este enlace. Las características de calidad de servicio que ofrecen estos equipos permiten establecer prioridades de tráfico en la red, garantizando así que los datos importantes de la empresa y el tráfico de voz sensible a los retardos reciban la prioridad necesaria en su tránsito a través de la red.

ECUAELECTRICIDAD ha visto reducido el costo de sus planillas telefónicas en un 25%, por lo que la inversión para la implantación de esta tecnología se ve justificada. Se ha reducido el uso de las líneas telefónicas convencionales en un 50% para las comunicaciones entre las oficinas de Cuenca y las de Guarumales (pues solo disponen de 2 canales VoIP) y se espera en un futuro utilizar solamente este tipo de comunicación.

Tenemos que considerar que la calidad de la voz depende directamente del tráfico de la red, por lo que se recomienda tener un ancho de banda asignado para la transmisión de Voz en la red. Actualmente se utiliza el enlace de datos para tráfico de Voz, Internet y Soporte, pero en un futuro se utilizará también para aplicaciones en línea (Sistema de Gestión de Información) donde se entrará a una segunda etapa que será la priorización de la información a transmitir.

No existe el soporte técnico profesional de CISCO a nivel local, pero tiene un buen nivel de soporte en Internet.

La interoperabilidad de ciertos equipos con otras marcas se vuelve un factor determinante en el momento de pensar en incluir nuevos servicios en la red, en este caso al tener una central telefónica NORTELL el costo de la inversión aumenta ya que se tiene que adquirir un dispositivo especial que permita conectar teléfonos con tecnología IP de cisco.

Se recomienda también que en una implementación de esta tecnología se capacite al personal en cuanto al cambio, pues aunque la calidad de voz es muy buena, siempre existe un retardo al que la gente debe acostumbrarse. Además es una tecnología nueva que aún tiene ciertos problemas que se van superando con el transcurso del tiempo.

Creemos que estamos en una nueva etapa de las comunicaciones la misma que dará un giro completo a la forma en como se manejan las empresas que actualmente brindan servicios de comunicación de voz, obligandoles a tener una visión diferente en cuanto a tecnología y servicio brindado.

LISTADO DE ACRÓNIMOS

ADPCM:	Adaptive Differential Pulse Code Modulation.
CIF:	Common intermediate format
CODEC:	Compression/decompression
DCT:	Discrete cosine transform
GCC:	Generic conference control
IETF:	Internet Engineering Task Force
IP:	Internet protocol
ISDN:	Integrated services digital network
ISO:	International Organization for Standardization
ITSP:	Internet telephony service provider
ITU:	International Telecommunications Union
ITU-T:	International Telecommunication Union - Telecommunications Sector
MCS:	Multipoint communication service
MCU:	Multipoint Control Unit
MGCP:	Media Gateway Control Protocol
OSI:	Open systems interconnection
PBX:	Private branch exchange
POTS:	Plain old telephone service
PSTN:	Public switched telephone network
QCIF:	Quarter common intermediate format
RAS:	Registration, Admission and Status
RDSI:	Red Digital de Servicios Integrados.
RFC:	Request for comments
RSVP:	Resource Reservation Protocol
RTCP:	Real-time transport control protocol
RTP:	Real-time transport protocol
SAP:	Session Announcement Protocol
SCN:	Switched circuit network
SDP :	Session Description Protocol
SIP:	Session Initiation Protocol
TCP:	Transmission control protocol
TPDU:	Transport Protocol Data Unit
TSAP:	Transport layer Service Access Point
UAC:	User Agent Client
UAS:	User Agent Server
UDP:	User datagram protocol
VPN:	Virtual Private Network
DSL:	Digital Subscriber Line

Bibliografía

Jonahan Davidson y James Peters, FUNDAMENTOS DE VoIP Pearson Educación, S.A., Madrid, 2001. Cisco Systems

Allian Leinward y Bruce Pinsky, CONFIGURACIÓN DE ROUTERS CISCO, 2da Edición. Pearson Educación, S.A., Madrid, 2001. Cisco Systems.

IBM International Technical Support Centers, TCP/IP Tutorial and Technical Overview, September 1991.

Cisco Systems, Cisco 2500 Series Installation and Configurations Guide, Copyright 1996 Cisco Systems, Inc.

Cisco Systems, Cisco 3640 Routers Installation and Configuration Guide, Copyright 1996 Cisco Systems, Inc.

Cisco Systems, Cisco WAN Interface Cards Hardware Installation Guide, Copyright 1998 Cisco Systems, Inc.

Motorola, VANGUARD 320 Installation Manual, Copyright 2000 Motorola, Inc.

Motorola, Motorola University Maintenance Course Student Guide, Copyright 1998 Motorola, Inc.

Documentos

ITU-T, RECOMMENDATION H.323: Packet-Based Multimedia Communications Systems, ITU -T (11/2000).

ITU-T, RECOMENDACIÓN H.225.0: Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedios por paquetes, ITU-T (11/2000).

ITU-T, RECOMENDACIÓN H.245: Protocolo de control para comunicación multimedios, ITU-T (07/2001).

ITU-T, RECOMENDACIÓN Q.931: Especificación de la capa 3 de la interfaz de usuario red de la red digital de servicios integrados para el control de llamada básica, ITU-T (05/1998).

Cisco, Cisco IOS Multiservice Applications Configuration Guide

RFC 1034, Domain Names – Concepts And Facilities, (11, 1987)

RFC 1889, RTP: A transport Protocol for Real-Time Applications, (01, 1996)

RFC 2205, Resource Reservation Protocol (RSVP), (09, 1997)

Rakesh Arora, Voice Over IP: Protocols And Standards, (11, 1999)

Paginas Web relevantes

ITU-T, Recomendaciones ITU-T, www.itu.int/rec/recommendation.asp

Cómo Funciona el DNS, <http://garl2.dramor.net/garl2/x-087-resolv.named.html>

PC-Web, Domain Name Service, www.sandybay.com/pc-web

Estandar H.323, <http://dit.teleco.ulpgc.es/usuarios/pas/nacho/h323/index.htm>

Asim Karim, H.323 And Associated Protocols, www.hut.fi/tttoivan/index4.html#intro

Motorola, Boletín Informativo Motorola, [www, www.redsat.com/entrada.html](http://www.redsat.com/entrada.html), (11,2000)

Cisco, Cisco VoIp Readiness Net Audit, www.cisco.com/public/ordering_info.shtml

Unitronics, El Estandar VoIp, www.comunicaciones.unitronics.es/tecnologia/h323.html, (1998)

ANEXO 1 – CONFIGURACION DE LOS EQUIPOS

Router Ecuaelectricidad - Cuenca

```
Cuenca#show conf
Using 2890 out of 29688 bytes
!
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname Cuenca
!
boot system flash:c1700-k8o3sv3y7-mz.122-4.YB.bin
enable password 7 070A22594F5941
!
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
!
no ip domain-lookup
!
ip inspect max-incomplete low 500
ip inspect max-incomplete high 1100
ip inspect one-minute low 500
ip inspect one-minute high 1100
ip inspect name FastEthernet_0 tcp
ip inspect name FastEthernet_0 udp
ip inspect name FastEthernet_0 cuseeme
ip inspect name FastEthernet_0 ftp
ip inspect name FastEthernet_0 h323
ip inspect name FastEthernet_0 rcmd
ip inspect name FastEthernet_0 realaudio
ip inspect name FastEthernet_0 smtp
ip inspect name FastEthernet_0 streamworks
ip inspect name FastEthernet_0 vdolive
ip inspect name FastEthernet_0 sqlnet
ip inspect name FastEthernet_0 tftp
ip inspect name Serial_0_1 smtp
ip inspect name Serial_0_1 tcp
ip inspect name Serial_0_1 ftp
ip audit notify log
ip audit po max-events 100
```

```
ip ssh time-out 120
ip ssh authentication-retries 3
multilink virtual-template 1
!
interface FastEthernet0/0
description connected to EthernetLAN
ip address 200.63.208.233 255.255.255.248 secondary
ip address 192.168.1.89 255.255.255.0
ip access-group 100 in
speed auto
!
interface Serial0/0
description connected to Guarumales
bandwidth 128
ip address 192.168.3.45 255.255.255.252
encapsulation ppp
ppp multilink
!
interface Serial0/1
description Ecuaelectricidad - SATNet
ip address 10.105.1.130 255.255.255.252
!
interface Virtual-Template1
description connected to Guarumales
ip unnumbered Serial0/0
ip tcp header-compression iphc-format
fair-queue 64 256 1
ppp multilink
ppp multilink fragment-delay 30
ppp multilink interleave
ip rtp header-compression iphc-format
ip rtp reserve 16384 100 24
!
router rip
version 2
network 192.168.1.0
network 192.168.2.0
no auto-summary
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.105.1.129
ip route 192.168.2.0 255.255.255.0 192.168.3.46
ip route 200.63.206.0 255.255.255.0 10.105.1.129
ip route 200.63.208.0 255.255.255.0 10.105.1.129
no ip http server
ip pim bidir-enable
!
access-list 100 permit ip any any
!
snmp-server community public RO
call rsvp-sync
```

```
!  
voice-port 2/0  
  description connected to Phone (523)  
!  
voice-port 2/1  
!  
dial-peer cor custom  
!  
dial-peer voice 2 pots  
  destination-pattern 523  
  port 2/0  
!  
dial-peer voice 4 voip  
  destination-pattern 675...  
  session target ipv4:192.168.2.90  
  ip qos dscp cs5 media  
!  
dial-peer voice 5 pots  
  destination-pattern 590  
  port 2/1  
!  
dial-peer voice 6 voip  
  destination-pattern 667...  
  session target ipv4:192.168.2.90  
  ip qos dscp cs5 media  
!  
line con 0  
  exec-timeout 0 0  
  password 7 08244F5B084952  
  login  
line aux 0  
line vty 0 4  
  password 7 070A22594F594E  
  login  
line vty 5 15  
  login  
!  
end
```

Cuenca#

Router Ecuaelectricidad – Guarumales

```
Guarumales#show conf  
Using 1723 out of 29688 bytes  
!  
version 12.2  
service timestamps debug uptime  
service timestamps log uptime  
service password-encryption
```

```
!  
hostname Guarumales  
!  
enable password 7 1412111E0D5472  
!  
ip subnet-zero  
!  
no ip domain-lookup  
!  
multilink virtual-template 1  
!  
interface FastEthernet0/0  
description connected to EthernetLAN_1  
ip address 192.168.2.90 255.255.255.0  
speed auto  
!  
interface Serial0/0  
description connected to Cuenca  
bandwidth 128  
ip address 192.168.3.46 255.255.255.252  
encapsulation ppp  
ppp multilink  
!  
interface Serial0/1  
no ip address  
shutdown  
!  
  
interface Virtual-Template1  
description connected to Cuenca  
ip unnumbered Serial0/0  
ip tcp header-compression iphc-format  
fair-queue 64 256 1  
ppp multilink  
ppp multilink fragment-delay 30  
ppp multilink interleave  
ip rtp header-compression iphc-format  
ip rtp reserve 16384 100 24  
!  
router rip  
version 2  
network 10.0.0.0  
network 192.168.1.0  
network 192.168.2.0  
no auto-summary  
ip classless  
ip route 0.0.0.0 0.0.0.0 192.168.3.45  
no ip http server  
!  
snmp-server community public RO  
call rsvp-sync
```

```
!  
voice-port 2/0  
  description connected to PBX (523-xx)  
  dial-type pulse  
!  
voice-port 2/1  
  dial-type pulse  
!  
mgcp profile default  
!  
dial-peer cor custom  
!  
dial-peer voice 1 pots  
  destination-pattern 667  
  port 2/0  
!  
  
dial-peer voice 3 voip  
  destination-pattern +523  
  session target ipv4:192.168.1.89  
  ip qos dscp cs5 media  
!  
dial-peer voice 9 pots  
  destination-pattern 675  
  port 2/1  
!  
dial-peer voice 10 voip  
  destination-pattern +590  
  session target ipv4:192.168.1.89  
  ip qos dscp cs5 media  
!  
line con 0  
  exec-timeout 0 0  
  password 7 06030C344D1E5E  
  login  
line aux 0  
line vty 0 4  
  password 7 110C1A1016425C  
  login  
line vty 5 15  
  login  
!  
end  
Guarumales#
```

Anexo 2 - DISEÑO DE TESIS