UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRONICA

IMPACTO DE LAS CENTRALES IP EN LA TELEFONIA TRADICIONAL

INFORME DE SUFICIENCIA

PARA OPTAR EL TITULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

DANTE RUBEN AGUILAR ASNARAN

PROMOCION
2003-II

LIMA – PERU
2008

IMPACTO DE LAS CENTRALES IP EN LA TELEFONIA TRADICIONAL

DEDICATORIA

Para aquellas personas que me han apoyado en este camino, por su compresión, ejemplo y el amor que me brindan: mi linda esposa, mis queridísimos padres y mi buena hermana.

SUMARIO

En esta nueva era en que las redes de datos han invadido nuestros hogares y son capaces de brindarnos diferentes servicios tanto de información, educación, entretenimiento y sobre todo comunicación en diferentes magnitudes; surge la Telefonía IP como uno de lo grandes servicios integrales que nos permite realizar comparaciones con la forma de comunicarnos en forma tradicional a través de líneas analógicas que eran las que dominaban el mercado.
Veremos como la tecnología ha evolucionado y nos permite diferentes protocolos de comunicación, diferentes medios de transporte, componentes y equipos necesarios para poder tener en funcionamiento una central IP que se están volviendo mas populares en diferentes empresas de Telecomunicaciones por la diversidad de servicios que ofrecen.

Trataremos de analizar en forma simple y concisa que ventajas y desventajas nos ofrecen en la actualidad estas nuevas centrales y compararlas con el tipo de Telefonía Tradicional, verificaremos si dichas centrales son capaces de coexistir para brindar diferentes servicios, mediante la integración de telefonía a través de distintos tipos de redes de Telefonía.
Esquematizaremos un servicio de telefonía integral regional para visualizar como estas nuevas centrales nos ayudan en tener comunicaciones mas abiertas.

ÍNDICE

INTRODUCCIÓN

Las tecnologías de VoIP retan el futuro de Internet. La red de datos es un medio mas por donde transitan diferentes servicios lo que representa el principal desafió para el modelo comercial que sustenta hoy en día la web, para los carriers la telefonía IP equivale a centrales telefónicas que presentan una capacidad diferencial con respecto a la telefonía tradicional.

Realizando una comparación entre los servicios de telefonía tradicional con los servicios de telefonía IP, se precisa que los servicios IP integran acceso a Internet y a servicios tradicionales a través de un mismo medio, esto permite a las empresas y usuarios tener ahorros significativos en el rubro de telecomunicaciones; beneficiándose así tanto las empresas como usuarios finales dentro de una red de alta calidad y disponibilidad; ya que la funcionalidad de telefonía IP nos permite tener servicios globalizados a nivel mundial centralizados en un solo punto de administración.

Los beneficios que se puede tener con la implementación de una red de Telefonía IP es que los costos por llamadas se aminoran, la inversión que se realiza para la implementación de la red de telefonía IP es menor a comparación de estar colocando E1's; es posible tener una capacidad variable y de mayor capacidad. Se puede incluir mayor aplicaciones por el mismo medio de transmisión con costos mas accesibles, al contar con integración de voz y datos sobre la misma infraestructura: IPTV, Video Streaming, Videoconferencia; el acceso al cliente puede ser mas versátil ya sea en forma física como en forma inalámbrica.

A nivel mundial el aumento del trafico de VoIp continua experimentando un crecimiento muy acelerado; por dar un ejemplo en un carrier internacional transportan hasta 7.6 mil millones de minutos VoIP; por lo cual este aumento también esta a la par con el uso de aplicaciones como video streaming por Internet; IPTV; estas consumen una grana cantidad de ancho de banda. Se tiene que los mayores usuarios a nivel mundial de estos servicios son carries de telecomunicaciones del mismo modo se ve que hay un crecimiento en los sectores corporativos y de gobierno por utilizar esta tecnología.

Vale la pena no confundir Telefonía Ip con Voz sobre la red de Internet, la primera es una tecnología usada, probada y segura para brindar todo tipo de servicios como calidad y garantía; la segunda consiste en utilizar la red con sus ventajas y desventajas para realizar llamadas de voz.

El protocolo IP permite ofrecer soluciones de voz, datos video de manera más eficiente que los medios tradicionales y con la misma calidad, siempre y cuando se lleven sobre una red controlada por el operador. Las bases para que las empresas adopten Telefonía IP consiste en tener vanguardia tecnológica que permita que los clientes tengan funcionalidades avanzadas de comunicación; así como el ahorro en costos de telefonía e infraestructura.

La tendencia de unificación de redes de voz y datos es un hecho que no tiene discusión, la discusión se centra en determinar el impacto tanto en la red como en la calidad de voz entregada de este tipo de implementaciones; Teniendo en cuenta que la voz compartirá recursos de una red de datos concebida y dimensionada para condiciones de operación diferentes.

Se han realizado distintos estudios para verificar pruebas de funcionalidad de voz y calidad entregada en diversas condiciones de congestión, pero su aproximación deja de lado conceptos tan importantes como tamaño de la cola en los buffers (que esta directamente relacionada con la calidad de la voz, medidas de retardo y perdida de paquetes), y tampoco

se preocupan demasiado por probar los diferentes CODEC´s implementados por los fabricantes; algo que sorprende ya que la utilización de uno u otro hace que un proyecto de VoIP sea viable o no.

La metodología seguida para este estudio contempla varias aproximaciones, que en conjunto deben dar una idea clara de lo que esta pasando tanto con la aplicación de VoIP, los diferentes tipos de plataformas usadas en Telefonía, el desempeño global de los enlaces WAN que son los encargados del transporte a través de las redes de datos, que son el eslabón más débil de la cadena. A partir de esta es posible tomar decisiones ya sea de implementar VoIP en la red o no, crecer el tamaño de los equipos de red o aumentar la velocidad de los enlaces WAN, de una manera planificada para poder soportar los distintos servicios que se ofrecen a través de las centrales IP.

C A P Í T U L O I

PROTOCOLOS DE SEÑALIZACION EN TELEFONIA IP

1.1.- Protocolos de Señalización

Por señalización se entiende el conjunto de informaciones intercambiadas entre dos puntos de la red telefónica que permiten efectuar operaciones de:

-Supervisión (detección de condición o cambio de estado).

-Direccionamiento (establecimiento de llamada).

-Explotación (gestión y mantenimiento de la red).

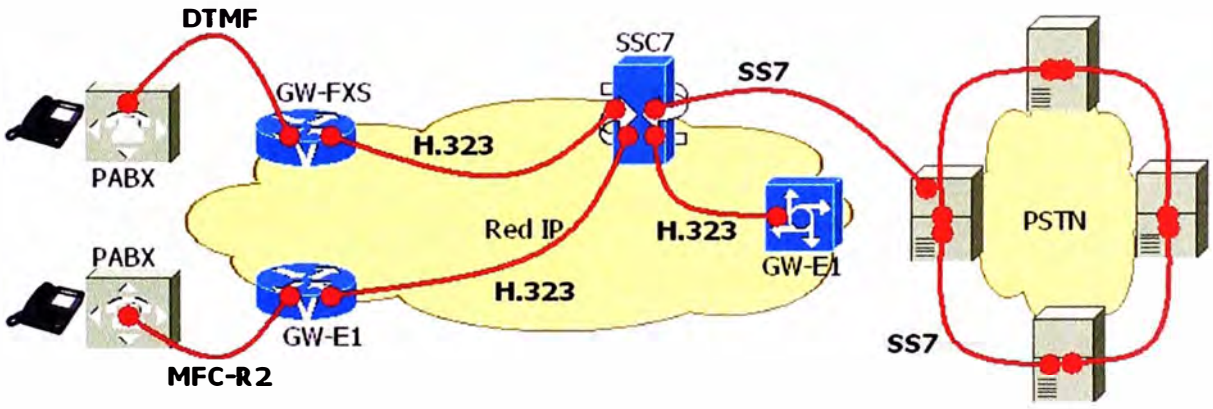


Figura 1.1. Protocolos involucrados en una red telefónica.

1.1.1.- Evolución de los protocolos de señalización

El ITU-T se ocupó de recomendar los sistemas de señalización a fin de ser usados en las comunicaciones internacionales. El primer sistema fue el SS1, que se inició en 1934. Es monofrecuente con un valor de 500 o 1000 Hz interrumpida con una cadencia de 20 Hz para la selección de llamada. Se lo utilizó para algunos servicios manuales bidireccionales.

Desde el SS1 hasta el SS5 son sistemas de señalización analógicos. El SS6 fue diseñado para USA y el SS7 por el ITU-T para Interconexión en forma global.

Cuando se inició la señalización en multifrecuencia se distinguió entre los procedimientos de código de impulsos como el SS5 y los de señales obligadas como el MFC-R2. En el caso del SS5 la señal tiene un período de duración fijo y determinado; el SS5 y normas anteriores de señalización dentro de banda, donde la información del establecimiento de la llamada era enviada a través de tonos especiales por las líneas telefónicas (canales portadores), ocasionaba gran cantidad de problemas de seguridad cuando los usuarios descubrían en ciertos aparatos telefónicos que ellos podían simular estos tonos en sus propios terminales y controlar la red incluso sin las "teclas especiales" de los operadores. Los llamados phreaks consiguieron crear sus propios tonos de señalización usando pequeñas cajas con equipamiento electrónico llamadas *Blueboxes*, mientras cuando se trata de señalización MFC-R2 el paso de mensaje se espera la respuesta de confirmación por el canal de retorno para cortar la señal de ida. Esto implica que la señalización por secuencia obligada requiere de mayor tiempo y una duración no determinada.

La señalización por corriente continua se realiza mediante los Hilos E&M (*Exchange & Múltiplex*). Se denomina hilo M al hilo de transmisión (salida de central) y E al hilo de recepción (entrada a central). Las señales se representan aplicando y desconectando potenciales o mediante la apertura y cierre de un bucle. La tensión es la que alimenta la central (-48 V). Se dispone de los estados P1 (-48 V sobre hilo a) y P2 (-48 V sobre hilo b).

La señalización puede ser del tipo de señales de impulsos o por niveles indicativos de estados; mientras el primero permite un plan complejo de señalización el segundo garantiza una supervisión sencilla de la línea. Prácticamente, este método solo se usa en líneas bifilares y se pueden distinguir dos tipos: el procedimiento de señalización en bucle (mientras un extremo maneja los potenciales el otro lo hace con el bucle cerrado o abierto) y la señalización por un solo hilo (potencial positivo o negativo en cada sentido).

La señalización multifrecuente se trata de una codificación que transmite un juego de 2 entre 6 frecuencias, dentro de la banda del canal telefónico en ambos sentidos: hacia

adelante (1380, 1500, 1620, 1740, 1860, 1980 Hz) y hacia atrás (1140, 1020, 900, 780, 660, 540 Hz). Su denominación es DTMF (*Dual Tone MultiFrequecy*).

En el sistema de multiplexación de 30 canales a 2048 kb/s (tramas E1) se recurre a un concepto mediante el MFC-R2 digital del año 1968. El Intervalo de Tiempo TS:16 de la trama se usa exclusivamente para información de señalización de los 30 canales vocales.

Ambos sistemas de señalización digital (MFC-R1 y R2) se usan en la actualidad, el primero en USA y el segundo en Europa y Latinoamérica.

Cuando los sistemas de conmutación son manejados por procesadores se requiere un concepto distinto al mencionado. Hasta ahora se puede decir que se tiene una correspondencia entre el canal vocal y el de señalización; a este método de lo llama Señalización por Canal Asociado CAS, observar grafico 1.2. en donde se aprecia que por el mismo canal va tanto la voz como la señalización haciéndola deficiente.

Cuando se trabaja con procesadores la señalización se transforma totalmente traduciéndose en un diálogo entre extremos. No se distingue una correspondencia entre el canal vocal y el canal de señalización; es más, la vía de transmisión puede ser distinta. Así, el canal de señalización pasa a ser un canal de datos dentro de una red de señalización; este tipo de señalización se denomina Señalización por Canal Común CCS (La nomenclatura SS7 corresponde al ITU-T y CCS7 a ANSI), según se observa el grafico 1.3 en donde el trafico de voz y señalización utilizan diferentes caminos.

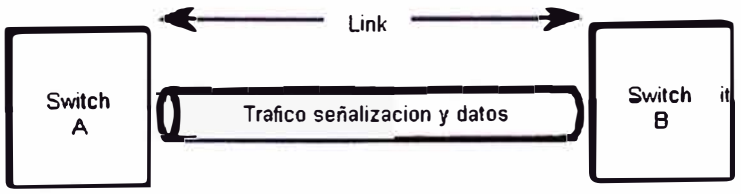


Figura 1.2: Señalizacion dentro de banda CAS

Figura 1.3: Señalizacion fuera de banda CCS

Las principales características que identifican a la señalización CCS frente a CAS son:

- Tiempo de conexión menor.
- Número de mensajes prácticamente ilimitados.
- Flexibilidad para nuevos servicios.
- Encaminamiento alternativo.
- Corrección de errores mediante retransmisión de tramas.
- La capa 2 utiliza un protocolo de corrección de error ARQ tipo *go-back-N*.
- La capa 3 está prevista para mensajes en tiempo real de la red telefónica y es del tipo orientado sin-conexión.

1.2.- Sistema de Señalización SS7.

SS7 es un medio por el cual los elementos de una red de telefonía intercambian información. La información es transportada en forma de mensajes. SS7 provee una estructura universal para señalización de redes de telefonía, mensajería, interconexión, y mantenimiento de redes. Se ocupa del establecimiento de una llamada, intercambio de información de usuario, enrutamiento de llamada, estructuras de abonado diferentes, y soporta servicios de Redes Inteligentes (IN). Para mover alguna funcionalidad no crítica en tiempo fuera de la trayectoria de señalización principal, y para flexibilidad futura, fue introducido el concepto de un "servicio plano" separado por la tecnología IN. El inicial, y actual uso más importante de la tecnología IN ha sido para servicio de traducción de servicios, por ejemplo, cuando se traducen números de llamada libre a números regulares PSTN. SS7 es también importante al enlazar tráfico VoIP a la red PSTN. SS7 es usado en las redes de telefonía móvil celular como GSM y UMTS para aplicaciones de voz (Conmutación de Circuitos) y datos (Conmutación de paquetes).

El SS7 es el sistema de señalización utilizado en la red PSTN y corresponde a la interconexión de la red de Telefonía-IP en iplan con la PSTN.

En el grafico 1.4 se observa los diferentes mensajes usados para el establecimiento de una llamada a través del SS7.

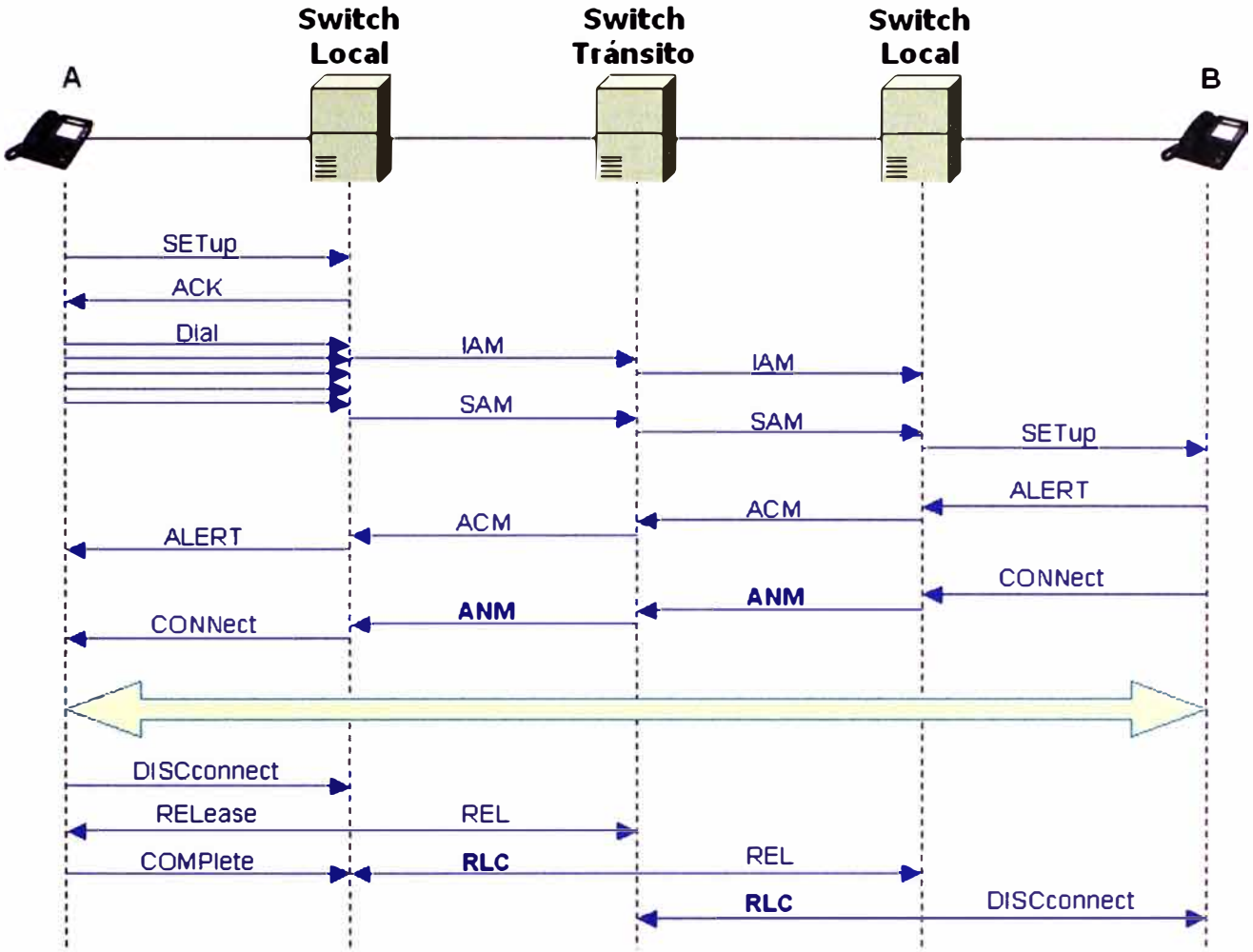


Figura 1.4. Intercambio de mensajes en el protocolo de señalización SS7.

1.2.1 Principales protocolos de la suite SS7.

a) MTP-2. Corresponde a la capa 2 del modelo OSI de 7 capas. Se ocupa del alineamiento de paquete mediante banderas (*Flag*) al inicio y final. Permite la detección de errores mediante un código denominado CRC-16. Realiza el proceso de numeración secuencial de mensajes e indicación de retransmisión. Efectúa la confirmación o rechazo del mensaje para la retransmisión automática en mensajes con errores. Los paquetes son numerados en forma secuencial con módulo-7. Indica también a longitud total del mensaje transmitido. Con la numeración de paquetes y la detección de errores, es posible la retransmisión de mensajes que se ven afectados por errores.

b) MTP-3. Posee una dirección de punto de acceso que permite identificar a la capa superior (TCAP o ISUP sobre el protocolo MTP3). En la red PSTN se dispone de

las direcciones de procesador CPU de origen y destino (14 bits de dirección). Por otro lado, identifica el enlace de señalización utilizado cuando existe más de uno. Realiza las funciones de Routing dentro de la red de señalización SS7.

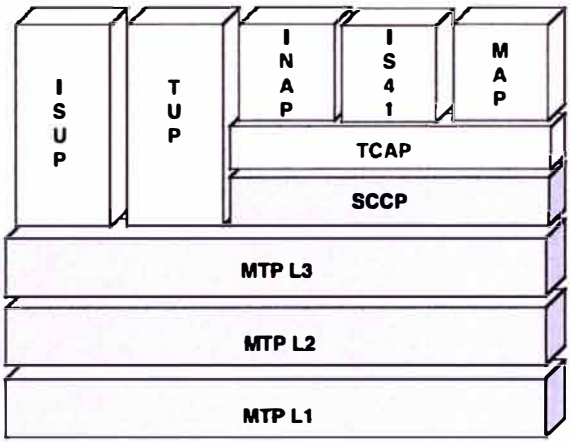


Figura 1.5. Suites de protocolo de señalización SS7

c) ISUP. Son los mensajes de señalización propiamente dichos. En la Figura 12 se muestra el intercambio de mensajes para la apertura y cierre de una llamada telefónica. Desde el usuario a la central se utiliza señalización MFC-R2 o DTMF. Los mensajes típicos de ISUP entre centrales son:

d) IAM (*Initial Address Message*). Contiene la información inicial de llamada para el encaminamiento. Son los primeros dígitos seleccionados por el usuario.

e) SAM (*Subsequent Address Message*). Transporta las cifras no enviadas en el mensaje IAM. Se completa el número del usuario B llamado.

f) ACM (*Address Complete Message*). Indica que se ha obtenido en acceso al destino. SE entrega al usuario A el tono de llamada.

g) ANM (*Answer Message*). Indica que el usuario llamado ha respondido. Se cierra el circuito vocal.

h) BLO (*Blocking Message*). Permite el bloqueo del canal útil.

i) UBL (*Unblocking Message*). Desbloquea el canal útil.

j) REL (*Release Message*). Permite iniciar la liberación del canal. La comunicación se cierra.

k) RLC (*Release Complete Message*). Informa que la liberación ha sido completada.

l) TCAP. Facilita la transferencia de mensajes en tiempo real entre HLR (*Home Location Register*), VLR (*Visitor LR*), MSC (*Mobile Switching Center*), EIR (*Equipment ID Register*),. Se aplica también para enlaces con O&M. En tarjetas de crédito permite verificar la autenticidad y movimientos de cuenta. Realiza el control de diálogo con el terminal remoto. Es un servicio de transporte.

La información contiene los siguientes componentes:

Tipo de mensaje (unidireccional, inicio, final, intermedio, aborto).

Longitud del mensaje (número de bytes total).

Identificador de origen y destino de transacción.

Tipo de componente (retorno de resultado, reporte de error y de reject).

Contenido de información (código de operación, de error, de problema, parámetros, etc).

1.3.- Codecs usados en Telefonía IP.

La comunicación de voz es analógica, mientras que la red de datos es digital. El proceso de convertir ondas analógicas a información digital se hace con un codificador-decodificador (el CODEC). Hay muchas maneras de transformar una señal de voz analógica, todas ellas gobernadas por varios estándares. El proceso de la conversión es complejo. Es suficiente decir que la mayoría de las conversiones se basan en la modulación codificada mediante pulsos (PCM) o variaciones.

Además de la ejecución de la conversión de analógico a digital, el CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda. Esto es especialmente interesante en los enlaces de poca capacidad y permite tener un mayor numero de conexiones de VoIP en forma simultanea. Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio, que es el proceso de no enviar los paquetes de la voz entre silencios en conversaciones humanas.

A continuación se muestra en la tabla 1.1 de la siguiente hoja un resumen con los códecs más utilizados actualmente:

El Bit Rate indica la cantidad de información que se manda por segundo.

El Sampling Rate indica la frecuencia de muestreo de la señal vocal.(cada cuanto se toma una muestra de la señal analógica).

El Frame size indica cada cuantos milisegundos se envía un paquete con la información sonora.

El MOS indica la calidad general del codec (valor de 1 a 5)

El codec g711 tiene dos versiones conocidas como alaw (usado en Europa) y ulaw (usado en USA y Japón). U-law se corresponde con el estándar T1 usado en Estados Unidos y A-law con el estándar E1 usado en el resto del mundo. La diferencia es el método que se utiliza para muestrear la señal. La señal no se muestrea de forma lineal sino de forma logarítmica. A-law tiene un mayor rango.

Existen varias versiones del codec g729 que es interesante explicar por su extendido uso G729: es el códec original G729A o anexo A: es una simplificación de G729 y es compatible con G729. Es menos complejo pero tiene algo menos de calidad.
G729B o anexo B: Es G729 pero con supresión de silencios y no es compatible con las anteriores. G729AB: Es g729A con supresión de silencios y sería compatible solo con G729B. Aparte de esto G729 (todas las versiones) en general tienen un bit rate de 8Kbps pero existen versiones de 6.4 kbps (anexo D) y 11.4 Kbps (anexo E).

Nombre	Estandarizado	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS
G.711 *	ITU-T	Pulse code modulation (PCM)	64	8	Muestreada	Tiene dos versiones u-law (US, Japan) y a-law (Europa) para muestrear la señal	4.1
G.721	ITU-T	Adaptive differential pulse code modulation (ADPCM)	32	8	Muestreada	Obsoleta. S e ha transformado en la G.726.	
G.722	ITU-T	7 kHz audio-coding within 64 kbit/s	64	16	Muestreada	Divide los 16 Khz en dos bandas cada una usando ADPCM	
G.722.1	ITU-T	Codificación a 24 y 32 kbit/s para sistemas sin manos con baja perdida de paquetes	24/32	16	20		
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 kbit/s para aplicaciones en circuitos digitales.	24/40	8	Muestreada	Obsoleta por G.726. Es totalmente diferente de G.723.1.	
G.723.1	ITU-T	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s	5.6/6.3	8	30	Parte de H.324 video conferencing. Codifica la señal usando linear predictive analysisby- synthesis coding. Para el codificador de high rate utiliza MP-MLQ y para el de low-rate usa ACELP.	3.8 - 3.9
G.726	ITU-T	40, 32, 24, 16 kbit/s adaptive differential pulse code modulation (ADPCM)	16/24/32/40	8	Muestreada	ADPCM; reemplaza a G.721 y G.723.	3.85
G.727	ITU-T	5-, 4-, 3- and 2-bit/sample embedded adaptive differential pulse code modulation (ADPCM)	var.		Muestreada	ADPCM. Relacionada con G.726.	
G.728	ITU-T	Coding of speech at 16 kbit/s using low-delay code excited linear prediction	16	8	2.5	CELP.	3.61
G.729 **	ITU-T	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code -excited linear-prediction (CS-ACELP)	8	8	10	Bajo retardo (15 ms)	3.92
GSM 06.10	ETSI	RegularPulse Excitation LongTerm Predictor (RPE-LTP)	13	8	22.5	Usado por la tecnología celular GSM	
LPC10	Gobierno de USA	Linear-predictive codec	2.4	8	22.5	10 coeficientes. La voz suena un poco "robotica"	
Speex			8, 16, 32	2.15-24.6 (NB) 4-44.2 (WB)	30(NB) 34 WB)		
iLBC			8	13.3	30		
DoD CELP	American Department of Defense)		4.8		30		
EVRC	3GPP2	Enhanced Variable Rate CODEC	9.6/4.8/1.2	8	20	Se usa en redes CDMA	
DVI	Interactive Multimedia Association (IMA)	DVI4 uses an adaptive delta pulse code modulation (ADPCM)	32	Variable	Muestreada		
L16		Uncompressed audio data samples	128	Variable	Muestreada		

Tabla 1.1 .- Codecs usados para Telefonía IP

1.4- SUITE H.323.

1.4.1- Familia de protocolos H.32x.

Para aplicaciones de multimedia, las primeras acciones se emprendieron con la definición de los protocolos RTP/RTCP (RFC-1889). La norma del ITU-T H.225 utiliza a RTP (está anexa enteramente de H.225). El ITU-T ha definido standard de cobertura para distintos servicios, inicialmente se presenta una descripción de la serie de standard H.32x.

a).- ITU-T H.320. Se ha diseñado para tecnologías referidas como velocidades Px64 kbps para video-teléfono. El estándar cubre desde 64 a 2048 kbps con un retardo inferior a 150 mseg. se señala un protocolo de conectividad internacional que permite la comunicación entre aparatos de distinta producción y compatible con ISDN. La norma H.320 involucra las funciones una familia de normas: H.261 para la señal de vídeo; G.721/722/728 para sonido; H.221 para el entramado de datos; H.230 para el control y H.242 para la señalización. Determinan los componentes del sistema de videoteléfono conectado a una central privada o desde un acceso ISDN a 2x64 kbps. El algoritmo de codificación de vídeo se indica el H.261; el algoritmo de audio en AV.250; el control de sistema en H.242 (señalización dentro de banda) y H.230 (intercambio de tramas de control); el multiplexor de las 3 señales anteriores en H.221 y el adaptador hacia la red en I.400.

b).- ITU-T H.323. Esta norma data de 1996 (versión 1) y 1998 (versión 2) y ha sido generada para sistemas de comunicación multimedia basado en paquetes (redes que pueden no garantizar correctamente la calidad de servicio QoS). Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de suma importancia ya que los primeros servicios de voz sobre protocolo Internet (VoIP) utilizan esta norma. En la versión 1 del protocolo H.323v1 se disponía de un servicio con calidad de servicio (QoS) no garantizada sobre redes LAN. En la versión 2 se definió la aplicación VoIP independiente de la multimedia. Una versión 3 posterior incluye el servicio de fax sobre IP (FoIP) y conexiones rápidas entre otros.

La versión H.323v2 introduce una serie de mejoras sobre la H.323v1. Algunas de ellas son:

- Permite la conexión rápida (elimina parte de tiempo de solicitud de conexión).

- Mediante H.235 introduce funciones de seguridad (autentificación, integridad, privacidad).

- Mediante H.450 introduce los servicios suplementarios.

- Soporta direcciones del tipo RFC-822 (e-mail) y del formato URL.

- Mediante la unidad MCU permite el control de llamadas multi-punto (conferencia).

- Permite la redundancia de gatekeeper.

- Soporta la codificación de vídeo en formato H.263.

- Admite el mensaje RIP (*Request in Progress*) para informar que la llamada no puede ser procesada por el momento.

- Provee la facilidad que el gateway informe al gatekeeper sobre la disponibilidad de enlaces para mejorar el enrutamiento de llamadas.

c) ITU-T H.324. Esta norma incluye la codificación H.263 para la señal de vídeo. El objetivo de ITU-T H.263 es mejorar la calidad de H.261. Esta norma es coherente con MPEG-4 desarrollado por la ISO. Formalmente utiliza las mismas técnicas de compresión de imagen con 5 a 15 imágenes/seg. H.324 permite la interactividad entre terminales PC-multimedia, módem de voz-datos, *Browsers* de web con vídeo en vivo, videoteléfonos, sistemas de seguridad, etc.

1.4.2- Protocolos de la Suite H.323.

a).- Tráfico. El tráfico de señal vocal se realiza sobre los protocolos UDP/IP. La codificación de audio puede ser de diferentes tipos. Con G.711 a velocidad es de 64 kbps. El ITU-T ratificó en 1995 a G.729 para las aplicaciones de VoIP. En tanto, el VoIP-Forum en 1997, liderado por Intel y Microsoft, seleccionó a G.723.1 con velocidad de 6,3 kbps para la aplicación VoIP. La codificación de vídeo se realiza de acuerdo con H.263. Ambos servicios se soportan en el protocolo de tiempo real RTP.

b).- Señalización. La señalización se transporta sobre los protocolos TCP/IP o UDP/IP. La familia de protocolos de señalización en H.323 incluye los siguientes protocolos (ver la Figura 1.6)

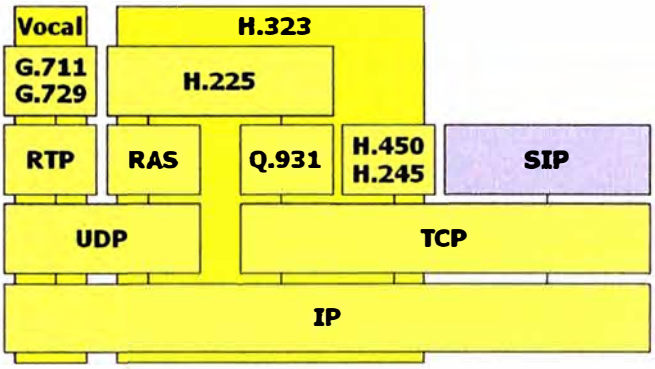


Figura 1.6. Familia de protocolos para H.323.

- H.225. Son los mensajes de control de señalización de llamada que permiten establecer la conexión y desconexión. Este protocolo describe como funciona el protocolo RAS y Q.931. El H.225 define como identificar cada tipo de codificador y discute algunos conflictos y redundancias entre RTCP y H.245.

-Q.931. Este protocolo es definido originalmente para señalización en accesos ISDN básico. Es equivalente al ISUP utilizado desde el GW hacia la red PSTN.

-RAS (*Registration, Admission and Status*) utiliza mensajes H.225 para la comunicación entre el GW y GK. Sirve para registración, control de admisión, control de ancho de banda, estado y desconexión.

-H.245. Este protocolo de señalización transporta la información no-telefónica durante la conexión. Es utilizado para comandos generales, indicaciones, control de flujo, gestión de canales lógicos, etc. Se usa en las interfaz GW-GW y GW-GK. El H.245 es una librería de mensajes con sintaxis del tipo ASN.1. En particular codifica los dígitos DTMF (*Dual-Tone MultiFrequency*) en el mensaje UserInputIndication.

-H.235. Provee una mejora sobre H.323 mediante el agregado de servicios de seguridad como autentificación y privacidad (criptografía). El H.235 trabaja soportado en H.245 como capa de transporte. Todos los mensajes son con sintaxis ASN.1.

c).-Calidad de servicio. Se transporta en protocolos UDP/IP. Se tienen los protocolos siguientes:

RTP (*Real-Time Transport Protocol*). Es usado con UDP/IP para identificación de carga útil, numeración secuencial, monitoreo, etc. Trabaja junto con RTCP (*RT Control Protocol*) para entregar un feedback sobre la calidad de la transmisión de datos. El encabezado de RTP puede ser comprimido para reducir el tamaño de archivos en la red.

RSVP. El protocolo de reservación de ancho de banda es usado para reservar un ancho de banda especificado dentro de la red IP. Téngase en cuenta que RSVP trabaja sobre PPP (o similar a HDLC) pero no trabaja bien sobre una LAN multiacceso.

PPP Interleaving se utiliza para enlaces inferiores a 2 Mb/s para fraccionar los paquetes de gran longitud y permitir el intercalado con paquetes de servicios en tiempo-real.

1.5.-Definición del Protocolo SIP.

El protocolo "Session Initiation Protocol" (SIP) es un estándar emergente para establecer, enrutar y modificar sesiones de comunicaciones a través de redes Internet Protocol (IP). Utiliza el modelo de Internet y lo convierte al mundo de las telecomunicaciones, utilizando protocolos Internet existentes tales como HTTP y SMTP (Simple Mail Transfer Protocol). También usa una estructura de dirección URL. Usa estas direcciones de tipo correo electrónico para identificar a los usuarios en lugar de los dispositivos que los utilizan. De esta forma SIP no depende del dispositivo y no hace distinción alguna entre voz y datos, teléfono u ordenador. Como se describe a continuación, SIP es usado mas para el manejo de servicios, mientras que H.323 se usa prácticamente para la conversión del número telefónico en paquetes IP.

1.5.1. Características Básicas del Protocolo SIP.

Se trata de un protocolo para el establecimiento de sesiones sobre una red IP. Una sesión que puede soportar desde una llamada telefónica hasta una multiconferencia multimedia con elementos de colaboración. Está siendo desarrollado por el SIPWG del IETF (RFC 2543, 2543bis), con la misma filosofía de sencillez y mínimo esfuerzo de siempre. SIP está

pensado como un mecanismo para el establecimiento, la terminación y la modificación de sesiones. Se trata de un protocolo basado en el paradigma de petición/respuesta (request-response), al igual que HTTP o SMTP.

SIP maneja mensajes de petición: [que se estructuran en tres bloques] Request Line + Cabecera + Cuerpo, y mensajes de respuesta: Status Line + Cabecera + Cuerpo. En ambos casos el cuerpo es independiente de SIP y puede contener cualquier cosa. A efectos de estandarización se definen métodos para describir las áreas de especificación; SIP define los siguientes métodos: invite, bye, options, ack, register, cancel, info (rfc 2976), comet, prack, subscribe/ notify/ message.

En la Figura 1.7 se ilustra un mensaje tipo, con los campos más importantes de la cabecera y el cuerpo rellenos de forma genérica.

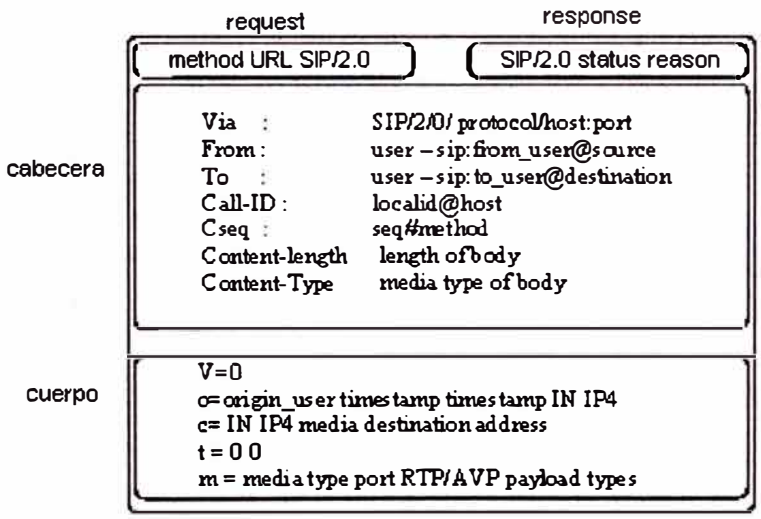


Figura 1.7 mensajes SIP

Las respuestas son del tipo HTTP:

1xx Informational (100 Trying, 180 Ringing, 181 Call is being forwarded)

2xx Successful (200 OK, 202 Accepted)

3xx Redirection (300 Multiple choices, 301 Moved Permanently, 302 Moved Temporarily)

4xx Client Error (400 Bad Request, 404 Not Found, 482 Loop Detected, 486 Busy here)

5xx Server Failure (500 Server Internal Error, 501 Not Implemented)

SIP se puede definir como un protocolo de control, pensado para la creación, modificación y terminación de sesiones, con uno o más participantes. Esas sesiones pueden comprender conferencias multimedia, llamadas telefónicas sobre Internet (o cualquier otra red IP), distribución de contenidos multimedia... Las sesiones pueden realizarse en multicast o en unicast; los participantes pueden negociar los contenidos y capacidades que van a utilizar; soporta movilidad de los usuarios, mediante utilización de proxies.

Las funcionalidades que se le exigen a un protocolo de estas características, son básicamente: La traducción de nombres y las ubicación de usuarios, la negociación de capacidades de cada usuario, la gestión de los usuarios que toman parte en una conferencia (sesión) y la gestión de los cambios en las capacidades de cada participante. SIP propone la utilización de un direccionamiento análogo al que se usa para el servicio de correo electrónico (e.g. sip:paco[arroba]bbva.com). Para la descripción_de contenidos, puede utilizar MIME, estándar de facto en Internet; aunque el IETF sugiere, para la descripción de la propia sesión, la utilización de SDP (Session Description Protocol), que no es un protocolo propiamente dicho, sino un formato para describir los flujos multimedia que se intercambian en una sesión.

Al igual que el servicio de correo, utiliza DNS para encontrar el servidor adecuado al que se le debe pasar una determinada petición. Está pensado para ser independiente de los niveles inferiores; sólo necesita un servicio de datagramas no fiable, con lo cual se puede montar sobre UDP o TCP. Sobre ese servicio no fiable se monta un transporte con RTP/RTCP. La Figura 1.8 pretende ponernos un poco en situación, representando los protocolos implicados en los aspectos de señalización (H.323, SIP, RTCP), provisión de calidad de servicio (RTCP, RSVP), transporte y encapsulación de contenidos multimedia y/o de medios múltiples (H.261, MPEG/RTP) que aparecen en escena cuando se aborda el problema del establecimiento, control y transporte de sesiones, que soportan comunicaciones multimedia entre varios participantes.

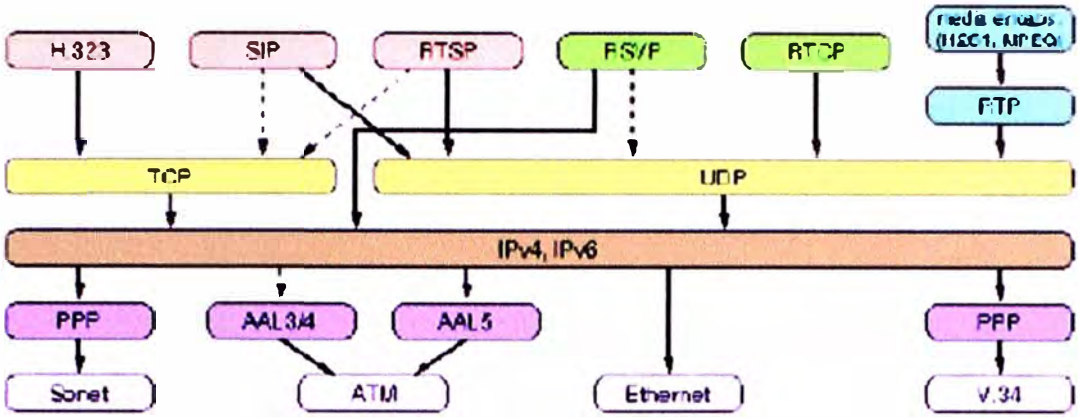


Figura 1.8 Suites de Protocolos de comunicación.

1.5.2. Arquitectura del Protocolo SIP.

SIP necesita dos componentes básicos: un agente de usuario (UA, User Agent) y un servidor (NS, Network Server). El agente de usuario, comprende un elemento cliente (UAC, User Agent Client) y un elemento servidor (UAS, User Agent Server). El cliente inicia las llamadas, y el servidor las responde: la idea es realizar llamadas (establecer sesiones 'peer-to-peer', P2P) con un protocolo Cliente/Servidor.

Las funciones principales de los servidores SIP son la resolución de nombres y la ubicación de usuarios. Se comunican con otros servidores pasándose mensajes en base a protocolos NHR. Los servidores pueden guardar o no información de estado, dando lugar a dos modos de funcionamiento ('statefull' o 'stateless' respectivamente para los anglosajones). Los servidores sin estado constituirían lo que se podría denominar el 'backbone' de una infraestructura SIP, mientras que los servidores con estado serían los dispositivos más cercanos a los agentes de usuario, que se encargarían del control de los dominios de usuarios.

Otras funcionalidades importantes de los servidores son la redirección (de una petición) y la "distribución" (pueden pasar una llamada a un grupo de usuarios, apropiándose de la sesión el primero que conteste).

Con esos componentes, UAC, UAS y NS, se puede montar una infraestructura básica de SIP; sobre la cual se pueden montar servidores de aplicaciones que podrían alojar módulos de servicio: de mensajería instantánea, de presencia, de control de llamada, perfiles de usuario. Al mismo nivel se supone que interaccionarían con otros servidores de contenidos en una arquitectura distribuida que integraría el balanceo de carga y soportaría la interfaz de gestión.

1.5.3 Mensajería Instantánea (IM) del SIP.

Es un medio de comunicación que resulta adecuado para el intercambio rápido de ideas entre pequeños equipos de trabajo distribuidos. El concepto de la "lista de amiguetes" ('buddy list') que ha surgido en entornos de IM como AOL o ICQ resulta interesante: es el hecho de poder disponer de una lista de usuarios de un servicio, con su disponibilidad online anunciada constantemente en la red. Es un servicio que se integra fácilmente, puesto que se trata de clientes muy ligeros.

Una sesión que se establece con SIP puede incluir cualquier medio de soporte, de manera que podemos pasar una comunicación vía IM a una conferencia telefónica, una pizarra compartida tipo NetMeeting o una videoconferencia. Podemos pensar en una especie de "telefonía instantánea" como evolución. En el mundillo de la telefonía móvil hay un claro precedente de la IM: el servicio de SMS. Tanto Yahoo como AOL han visto la potencialidad de este servicio y ya se están moviendo para alcanzar acuerdos con proveedores de servicios móviles.

Ese concepto de presencia asociado a las 'buddy lists' también está evolucionando; se habla de presencia no sólo a nivel del propio PC del puesto, sino asociado con cualquier tipo de dispositivo o aplicación independiente: es el caso de los 'bots' que IBM utiliza en su Lotus SameTime: son 'buddy lists' que representan realmente consultas a bases de datos o directorios corporativos. En principio se trata de la extensión del concepto de mensajería instantánea a un contexto mucho más amplio del que propició su origen: estamos hablando del intercambio de mensajes entre usuarios, que pueden ser personas (usuarios finales del servicio que tendrán uno u otro perfil asociado), máquinas (cualquier tipo de terminal

asociado a un usuario), o aplicaciones (que pueden incluir agentes inteligentes o servicios Web).

Todas las posibilidades que se han mencionado nos llevan a la integración de todo tipo de comunicación en el "escritorio" del puesto de cada empleado, posibilitando la gestión conjunta de todos los medios de comunicación a disposición de aquellos, con un 'repositorio' único de contactos a mantener. Este aspecto resulta de un interés indudable en el entorno empresarial, puesto que redunda de forma directa en el incremento de la productividad de los empleados, permitiendo el despliegue de servicios de valor añadido como cualquier otro servicio sobre una arquitectura SIP apoyada en una red IP multiservicio.

1.6.- Protocolo H.248 (MEGACO).

Este protocolo se define en la Recomendación H.248 de la ITU-T. El protocolo H.248 o Megaco permite la conmutación de llamadas de voz, fax y multimedia entre la red PSTN y las redes IP de siguiente generación. El protocolo Megaco, que tiene su origen en el protocolo MGCP (Media Gateway Control Protocol, Protocolo de control de puerta de enlace al medio), proporciona un control centralizado de las comunicaciones y servicios multimedia a través de redes basadas en IP. Megaco está adquiriendo solidez en el mercado porque permite una mayor escalabilidad que H.323, y da respuesta a las necesidades técnicas y a las funciones de conferencia multimedia que se pasaron por alto en el protocolo MGCP.

Funcionalmente, Megaco es un protocolo de señalización utilizado entre los elementos de una arquitectura distribuida que incluye media gateway y controladores de media gateway (conocidos a menudo como softswitches, gatekeeper o call server); H.248 es el resultado de la cooperación entre la ITU y el IETF. Antes de lograr esta cooperación existían varios protocolos similares compitiendo entre si, principalmente MGCP (la combinación de SGCP e IPDC) y MDCP. H.248 se considera un protocolo complementario a H.323 y SIP, ya que un Media Gateway Controller (MGC), controlará varios Media Gateways utilizando H.248, pero será capaz de comunicarse con otro MGC utilizando H.323 o SIP.

1.6.1.- MGCP.

El MGCP es, en esencia, un protocolo maestro/esclavo, donde se espera que los gateways ejecuten comandos enviados por el MGC. El Protocolo de Control de Media Gateway (MGCP) es usado para controlar los gateways de telefonía desde los elementos de control de llamadas externos llamados Media Gateways Controllers (MGC) o Gatekeepers.

Un gateway de telefonía es un elemento de red que provee conversión entre las señales de audio transportadas sobre los circuitos telefónicos y los paquetes de datos transportados sobre la internet o sobre otra red de paquetes.

MGCP asume una arquitectura de control de llamada, donde la inteligencia del control de la llamada está fuera de los gateways y manejada por un elemento de control de llamada externo. El MGCP asume que estos elementos de control de llamadas o MGC, se sincronizarán entre sí para enviar comandos coherentemente a los gateways que están bajo su control. Lo que se propuso con MGCP fue sacar el control de la señalización del propio gateway (GW), llevándolo a otro elemento, el 'media gateway controller' MGC (que se conoce como 'softswitch') que se encargará del control de los media gateways'(MGW).

A nivel de sistemas lo que se ha hecho es desagregar el gatekeeper (GK) en sus equivalentes en el mundo SS7. Esta iniciativa surgió de varios fabricantes con el nombre de IPDC (Cisco, Alcatel, 3Com et al.) por un lado y SGCP (Telcordia) por otro; un esfuerzo que el IETF aglutinó bajo la denominación de MGCP y asignada a la responsabilidad del grupo de trabajo Megaco. MGCP es en la fecha de redacción de este documento un documento de trabajo. Tanto IETF como la ITU-T trabajan para llegar a un estándar, el primero bajo la responsabilidad de Megaco y como H.248 para el segundo.

En MGCP se puede decir que se ha separado la "inteligencia" (las funciones de control) de los datos (los contenidos: 'the media'). Que se trata de un protoclo Maestro/Esclavo. El maestro es el MGC ('softswitch' o 'call agent') y el esclavo es el MGW (que puede ser un GW de VoIP, un DSLAM, un router MPLS, un teléfono IP,...). Esta es precisamente la característica que más choca con la filosofía (P2P) de SIP. Otra característica interesante es que intenta reproducir el modelo de la PSTN/IN sobre IP (en la Figura 1.9 se ilustra el escenario típico para un despliegue tipo 'Internet Telephony' que es la aplicación para la

que se pensó, al menos en principio esta solución), en contra del modelo distribuido que propone SIP.

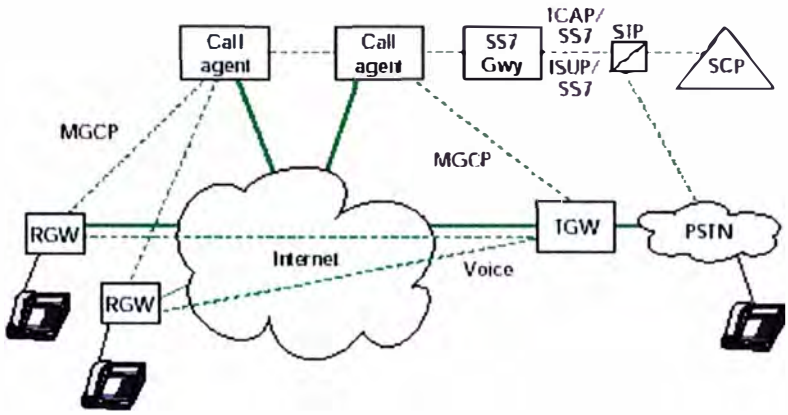


Figura 1.9 red basada en MGCP

El Megaco pretende dar una solución basada en una visión propia de las Telcos tradicionales, una oficina central (Central Office, CO, en este caso IPCO) y una red de sucursales (Branch Offices, BO). Tal y como se observa en la Figura 1.10, SIP puede complementar a MGCP en un escenario donde tengamos varios MGC.

Figura 1.10 Integración de redes MGCP

Un tema de debate importante es la utilización de MGCP para controlar los terminales (los teléfonos IP por ejemplo); el problema que surge es que sólo soporta servicios básicos de red inteligente. El tema es que si se quieren desplegar servicios avanzados necesitamos montar SIP tanto en los terminales como sobre la red de señalización, realizando las funciones de control asociadas al servicio.

Ya se ha comentado más arriba que la visión de los partidarios de MGCP es que la inteligencia del servicio esté pegada a los MGC (softswitch), y de hecho en el corto plazo

es un planteamiento adecuado puesto que el esfuerzo de convergencia se centrará en los puntos de interconexión entre la PSTN y la red IP, y pro tanto interesará que los servidores SIP estén junto a los MGC en la CO. Pero, según avancemos hacia un escenario más integrado, la atención se centrará en la infraestructura IP, con lo cual la función de los MGC se alejará de los puntos de interconexión. Finalmente, en un entorno IP puro, la función de creación de servicios se distribuirá por toda la red: se puede extender el modelo ASP para dar servicios de voz. Tanto los ASPs como los ISPs, o incluso los propios usuarios finales pueden crear sus propios servicios. Se puede pensar en un escenario basado en SIP, donde se utilice MGCP para controlar internamente un GW de Telefonía IP (TIP) y los servidores de aplicaciones SIP distribuirían servicios por la red a través de los servidores proxy SIP.

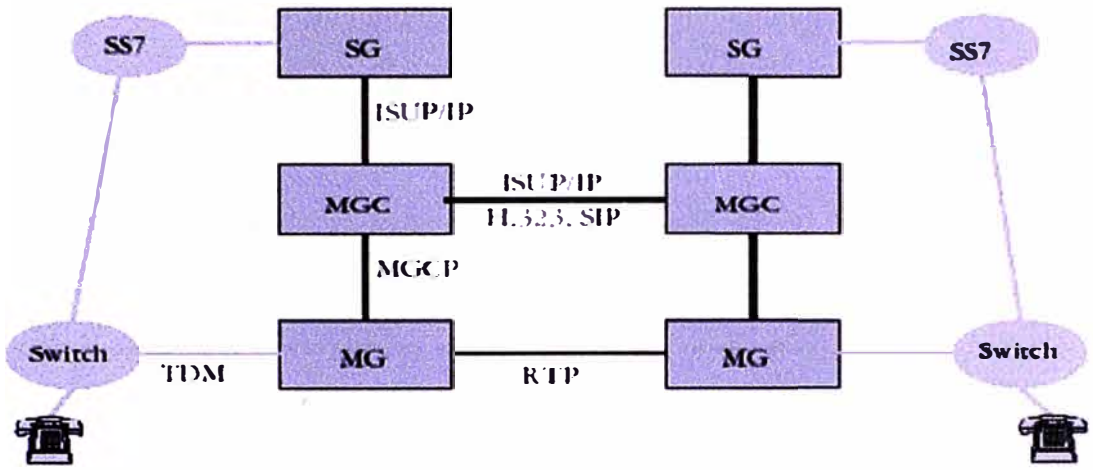


Figura 1.11 Descomposicion del Gateway e Interaccion del PSTN

Como conclusión debemos extraer el hecho de que MGCP no se puede considerar como un competidor de SIP, puesto que ambos resultan complementarios en ciertos aspectos, mientras que son mutuamente excluyentes en otros.

Esta idea de dividir el Gateway de voz en varias entidades funcionales se ha propuesto también desde iniciativas como TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) de la ETSI, con la intención de proporcionar una arquitectura "escalable" que soporte el servicio de Telefonía IP con la necesaria capacidad para convivir con las redes tradicionales de conmutación de circuitos (SCN, Switched Circuit Networks) como la PSTN. Esta división es la que se ilustra en la figura 1.11

1.7. - Protocolo IAX (Inter-Asterisk Exchange Protocol)

El protocolo IAX se corresponde con Inter-Asterisk exchange protocol. Como indica su nombre fue diseñado como un protocolo de conexiones VoIP entre servidores Asterisk aunque hoy en día también sirve para conexiones entre clientes y servidores que soporten el protocolo. La versión actual es IAX2 ya que la primera versión de IAX ha quedado obsoleta Es un protocolo diseñado y pensado para su uso en conexiones de VoIP aunque puede soportar otro tipo de conexiones (por ejemplo video).

Los objetivos de IAX son:
-Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIP.
-Evitar problemas de NAT (Network Address Translation).
-Soporte para transmitir planes de marcación.
Entre las medidas para reducir el ancho de banda cabe destacar que IAX o IAX2 es un protocolo binario en lugar de ser un protocolo de texto como SIP y que hace que los mensajes usen menos ancho de banda.

Para evitar los problemas de NAT el protocolo IAX o IAX2 usa como protocolo de transporte UDP, normalmente sobre el puerto 4569,(el IAX1 usaba el puerto 5036), y tanto la información de señalización como los datos viajan conjuntamente (a diferencia de SIP) y por tanto lo hace menos proclive a problemas de NAT y le permite pasar los routers y firewalls de manera más sencilla.

1.7.1 mensajes IAX2

Los mensajes o tramas que se envían en IAX2 son binarios y por tanto cada bit o conjunto de bits tiene un significado. Como hemos indicado anteriormente existen dos tipos de mensajes principalmente:

a).- Tramas F o Full Frames

La particularidad de las tramas o mensajes F es que deben ser respondidas explícitamente. Es decir cuando un usuario manda a otro una trama F (full frame) el receptor debe contestar confirmando que ha recibido ese mensaje. Estas tramas son las únicas que deben ser respondidas explícitamente.

Figura 1.12 Formato binario de una trama F o full frame de IAX2

El significado de cada uno de los campos es el siguiente:

- F : Un bit que indica si la trama es F (full frame) o no. Para que sea F o full frame debe estar puesta a 1.
- Source Call Number - Número de llamada de origen : 15 bits que identifican la conversación de origen ya que puede haber varias comunicaciones multiplexadas por la misma línea.
- R : Bit de retransmisión. Se pone a uno cuando la trama es retransmitida.
- Destination Call Number - Número de llamada destino : lo mismo que el de origen pero para identificar el destino.
- Timestamp o sello de tiempo - Para marcar el tiempo en cada paquete
- OSeqno - sec. de salida : Número de secuencia de salida con 8 bits. Comienza en 0 y se va incrementándose cada mensaje.
- ISeqno - sec. de entrada : Lo mismo para la entrada.
- Frame Type - tipo de trama :Indica la clase de trama de que se trata
- C: Puesto a 0 indica que el campo subclase debe tomarse como 7 bits (un solo mensaje): Puesto a 1 indica que el campo subclase se obtiene con 14 bits (dos mensajes consecutivos).
- Subclass - subclase - Subclase del mensaje.
- Data - Datos : datos que se envían en formato binario.

b).- Tramas M o Mini Frames

Las tramas M o mini frames para mandar la información con la menor información posible en la cabecera. Estas tramas no tienen porque ser respondidas y si alguna de ellas se pierde se descarta sin más. El formato binario de las tramas M o mini frames es el siguiente:

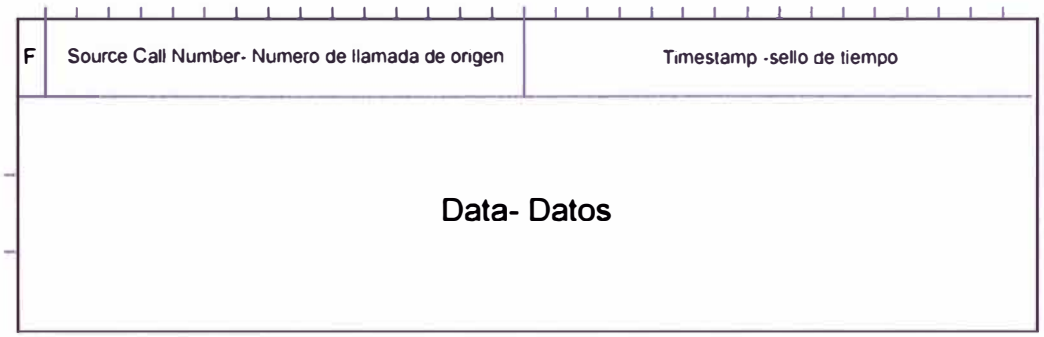


Figura 1.13.-formato binario de una trama M o mini frames

El significado de los campos es similar al de las tramas F o full frame. En este caso el bit F está puesto a 0 y el sello de tiempo o Timestamp está truncado y solo tiene 16 bits para aligerar la cabecera. Son los clientes los que deben encargarse de llevar un timestamp de 32 bits si lo desean y para sincronizarlo mandar una trama F.

C A P Í T U L O II

BASES PARA EL TRANSPORTE DE LA TELEFONIA IP

2.1.- MPLS (Multi-Protocol Label Switching)

Es una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM.

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red. Contamos con distintas soluciones, una completamente gestionada que incluye el suministro y la gestión de los equipos en sus instalaciones (CPE). O bien, que sea usted quien los gestione.

MPLS intenta conseguir las ventajas de ATM, pero sin sus inconvenientes; asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la de destino)

Las principales aplicaciones de MPLS son:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)

- Policy Routing

- Servicios de VPN .

- Servicios que requieren QoS

MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS). La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA. El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LANs.

Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.

2.1.1.-Conmutación MPLS

Conmutación de etiquetas en un LSR a la llegada de un paquete:

Examina la etiqueta del paquete entrante y la interfaz por donde llega

Consulta la tabla de etiquetas

Determina la nueva etiqueta y la interfaz de salida para el paquete

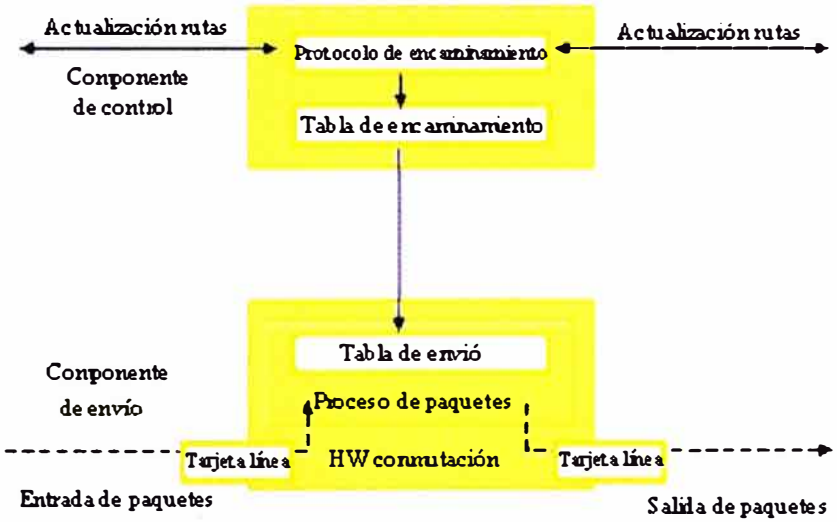


Figura 2.1 MPLS y pila de etiquetas

2.1.2.- Jerarquía MPLS

MPLS funciona sobre multitud de tecnologías de nivel de enlace. La etiqueta MPLS se coloca delante del paquete de red y detrás de la cabecera de nivel de enlace; las etiquetas pueden anidarse, formando una pila con funcionamiento LIFO (Last In, First Out). Esto permite ir agregando (o segregando) flujos. El mecanismo es escalable.

Cada nivel de la pila de etiquetas define un nivel de LSP → Túneles MPLS, así dentro de una red MPLS se establece una jerarquía de LSPs.

En ATM y Frame Relay la etiqueta MPLS ocupa el lugar del campo VPI/VCI o en el DLCI, para aprovechar el mecanismo de conmutación inherente

2.1.3- Etiquetas MPLS

Las etiquetas MPLS identifican a la FEC asociada a cada paquete

Etiqueta MPLS genérica:

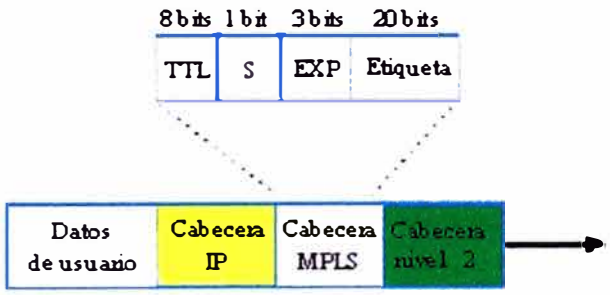
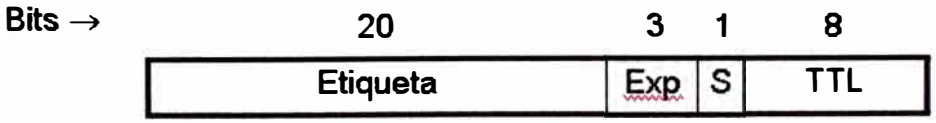


Figura 2.2- Formato de la etiqueta MPLS: 32 bits



Etiqueta: La etiqueta propiamente dicha que identifica una FEC (con significado local)

Exp: Bits para uso experimental; una propuesta es transmitir en ellos información de DiffServ

S: Vale 1 para la primera entrada en la pila (la más antigua), cero para el resto. Esta es la primera etiqueta introducida.

TTL: Contador del número de saltos. Este campo reemplaza al TTL de la cabecera IP durante el viaje del datagrama por la red MPLS.

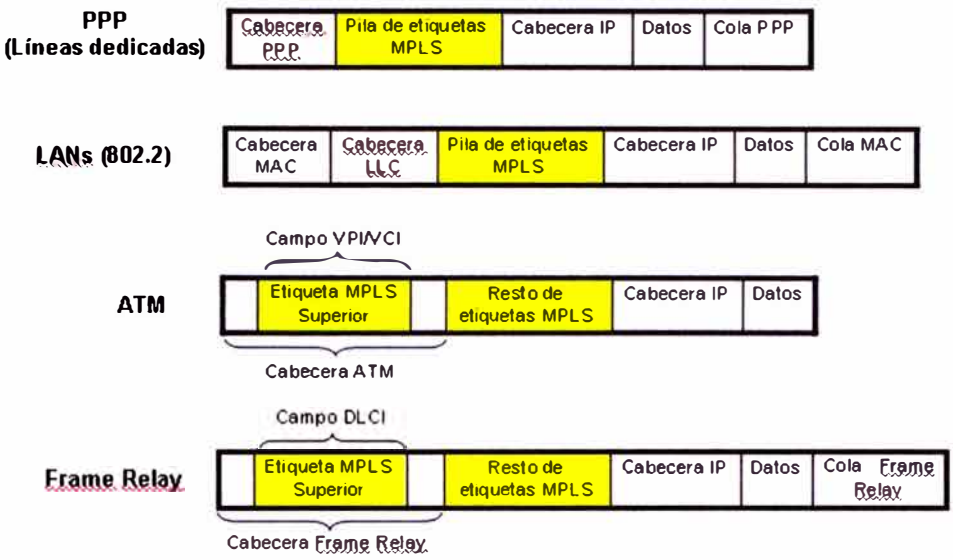


Figura 2.3 Situación de la etiqueta MPLS

2.1.4.- Routing MPLS

Los paquetes se envían en función de las etiquetas. No se examina la cabecera de red completa por lo cual el direccionamiento es más rápido.

Cada paquete es clasificado en unas clases de tráfico denominadas FEC *(Forwarding Equivalence Class)*. Los LSPs por tanto definen las asociaciones FEC-etiqueta.

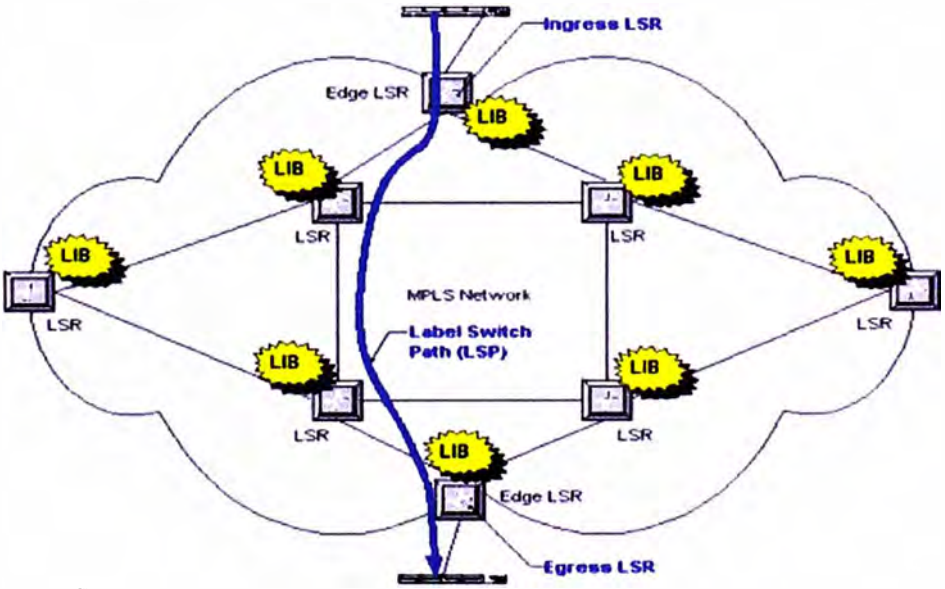


Figura 2.4. Esta es una red MPLS en la cual se ven todos sus componentes, la línea azul representa el LDP entre el LSR de entrada y el LSR de salida.

2.1.5.- Funcionamiento global MPLS

Una vez vistos todos los componentes funcionales, el esquema global de funcionamiento es el que se muestra en la figura, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de routers IP.

El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de routers). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP. Todo ello abre enormes posibilidades a la hora de mejorar el rendimiento de las redes y de soportar nuevas aplicaciones de usuario.

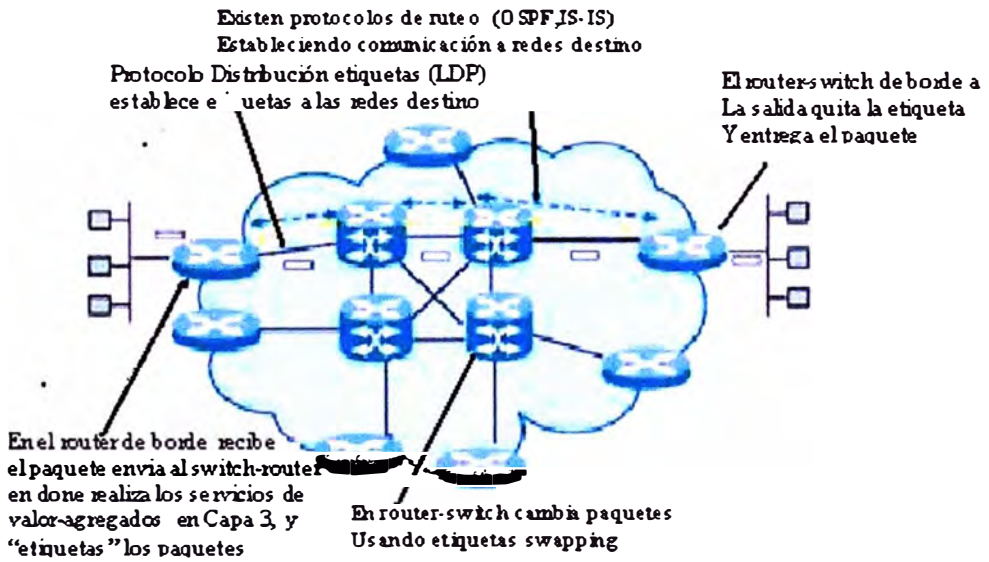


Figura 2.5. funcionamiento MPLS

2.1.6.- Aplicaciones de MPLS

Redes de alto rendimiento: las decisiones de encaminamiento que han de tomar los routers MPLS en base a la LIB son mucho más sencillas y rápidas que las que toma un router IP ordinario (la LIB es mucho más pequeña que una tabla de rutas normal). La anidación de etiquetas permite agregar flujos con mucha facilidad, por lo que el mecanismo es escalable.

Soporte multiprotocolo: los LSPs son válidos para múltiples protocolos, ya que el encaminamiento de los paquetes se realiza en base a la etiqueta MPLS estándar, no a la cabecera de nivel de red.

a)- Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén supra utilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. Antiguamente los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos). En el esquema de la figura se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

MPLS es una herramienta efectiva para esta aplicación en grandes backbones, ya que permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.

Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

Permite hacer "encaminamiento restringido" (Constraint-based Routing, CBR), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, etc.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

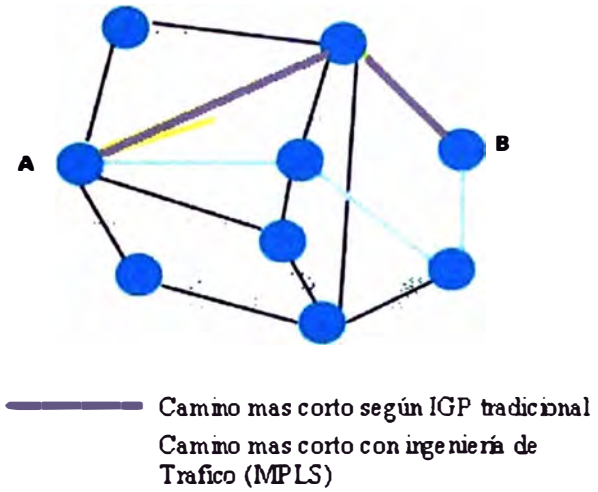


Figura 2.6. camino mas corto en redes MPLS

b).- Clases de servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de vídeo y voz interactiva. Para ello se emplea el campo ToS (Type of Service), rebautizado en DiffServ como el octeto DS. (Véase más información sobre el modelo DiffServ en las referencias correspondientes a QoS). Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De es te modo, una red MPLS puede transportar distintas clases de tráfico, ya que el tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP; entre cada par de LSR exteriores se puede provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort, tres niveles de servicio, primero, preferente y turista, que, lógicamente, tendrán distintos precios.

c).- Redes Privadas Virtuales (VPNs)

Una red privada virtual (VPN) se construye a base de conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se va a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos Frame Relay, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR). Algo similar se puede hacer con ATM, con diversas clases de garantías. Los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone

retocar todos los CPEs del cliente y restablecer todos los PVCs. Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan sólo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones. Se puede obtener más información sobre IP VPN con túneles en las referencias correspondientes a VPNs con MPLS.

Las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs)

- evita la complejidad de los túneles y PVCs

- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router

- tiene mayores opciones de crecimiento modular

- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación), lo que es necesario para un servicio completo VPN.

2.2 PROTOCOLOS DE TRANSPORTE EN VoIP

2.2.1- PROTOCOLO DE TRANSPORTE EN TIEMPO REAL (RTP).

Es un protocolo que como su nombre lo indica, está orientado a la transmisión de información en tiempo real, como la voz o el video. Este es un protocolo de las capas superiores de usuario que funciona sobre UDP (user datagram protocol) , como mecanismo de transporte porque posee un menor retardo que TCP, y además porque el trafico de voz en la actualidad, sin importar que sean datos o señalización, toleran menos niveles de perdida y no tienen la facilidad de retransmisión, en el UDP se cambia confiabilidad por velocidad, lo cual es básico para manejo de transmisiones en tiempo real como la VoIP.

El protocolo RTP tiene como objetivo asegurar una calidad de servicio QoS para servicios del tipo tiempo-real. Incluye: la identificación del payload, la numeración secuencial, la medición de tiempo y el reporte de la calidad (función del protocolo RTCP).El RTP trabaja en capa 4 y sobre UDP, de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertas (port UDP).Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x forma una familia del ITU-T de normas para videoconferencia).

El RTP funciona en conjunto con RSVP (capa 3) para la reservación de ancho de banda y asegurar de esta forma la QoS del tipo Garantizada. La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversos alternativas de prioridad para formar una cola de espera en routers. Un algoritmo particular de gestión de prioridad de tráfico es el WFQ (Weighted Fair Queuing) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes. Cada cliente ocupa un intervalo de tiempo en un Round-Robin.

El RTP además provee transporte para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo IGMP para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el

encabeza del RTP y ocupa el campo de carga útil. No es lo suficientemente confiable por si solo, este proporciona "ganchos" con protocolos y aplicaciones de capas inferiores y recursos proporcionados por los switches y enrutador para garantizar confiabilidad.

Los paquetes RTP no contienen campo de longitud, ya que al funcionar sobre UDP, este protocolo es quien encapsula la voz comprimida en datagramas. Para la compresión RTP usa una aplicación llamada "vocoder" pudiendo reducir de 64 kbps hasta a 8 kbps el ratio para digitalización y compresión de voz produciendo un desmejoramiento en la calidad de la voz poco perceptible, además de esto usa h.323 g.729 y otros protocolos más para transmisiones en tiempo real. RTP es capaz de correr sobre protocolos WAN de alta velocidad como ATM sin ningún problema, también en redes asimétricas como ADSL, cable-modem o por enlace satelital pero cumpliendo con ciertas características de ancho de banda para ambas direcciones y uso exclusivo para la aplicación RTP. Las herramientas de las que se vale RTP para lograr transmisiones en tiempo real son el RTCP, que proporciona un feedback a cerca de la calidad de distribución y la congestión, con esto, la empresa que ofrece el servicio puede monitorear la calidad y puede diagnosticar los problemas que pueda presentar la red.

2.2.2.-Características Generales del Protocolo RTP

Fiabilidad	* No es fiable si se utiliza junto con UDP o IP que as u vez no son fiables. * Puede apoyarse en el servicio prestado por las capas inferiores de las redes que funcionan en modo conectado (por ejemplo capas ATM, AAL3/4 o AAL5).
Control de congestión	* No tiene un mecanismo de control de congestión incorporado como TCP.
Estabilidad de trenes	* No garantiza el control de los tiempos de transmisión o la continuidad de flujo en tiempo real.
Recursos	* No reserva ningún recurso y no repercute directamente en el comportamiento de la red.
Información y herramientas para el destinatario	* El encabezamiento RTP contiene varios ítem de información para la sincronización y restitución de la señal en el receptor, a saber,: indicación de tiempo, índices de tren y secuencias, fuentes que contribuyen, etc
Información para el remitente	* No proporciona, por si mismo, ninguna información útil al remitente. Se utiliza por lo general con el protocolo RTCP, que ofrece al remitente una información muy completa acerca de la calidad de transmisión: pérdida de paquetes, retardos, etc. Permite al remitente modular su velocidad de salida según los recursos disponibles.

Tabla 2.1 Características del protocolo RTP

2.2.3.- Funciones del Protocolo RTP

Entre sus funciones se encuentran: la memorización de datos, la simulación de distribución interactivo, el control y mediciones de aplicaciones.

La funcionalidad ToS (Tipo de Servicio) en IP puede determinar un ancho de banda específico para el cliente. Un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección de origen y destino IP, tipo de protocolo y número de socket para asignar una ponderación. En redes que disponen de switch de capa 2 se requiere extender la gestión de la calidad de servicio a dicha capa. Para ello la IEEE ha determinado el ToS sobre IEEE-802.

2.2.4 Diagrama del Paquete de Transporte RTP.

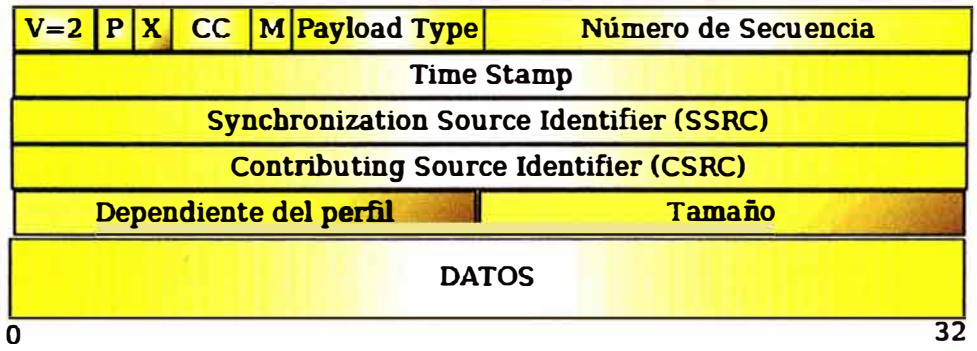


Figura 2.7 paquete RTP

P = Padding , X = Extenciones tras CSRC(0), CC = CSRC Count(0)

M = Marcador (SID Support), Nª Sec = Comienza en nª aleatorios

Timestamp = Tick count tras la emisiòn del 1er paquete. 1tick =1/8000

SSRC = Origen del medio. Mismo origen, mismo tiempo y nuecero de secuencias.

2.2.5. Protocolo RTCP (REAL-TIME CONTROL PROTOCOL).

Se basa en la periódica transmisión de los paquetes de control a todos los participantes en sesión, utilizando el mismo mecanismo de distribución como dato paquete. El protocolo subyacente debe proveer de la multiplexación de los datos y de los paquetes del control.

Es una herramientas de las que se vale RTP para lograr transmisiones en tiempo real, que proporciona un feedback a cerca de la calidad de distribución y la congestión.

RTCP sincroniza el audio y el video, conoce el número de usuarios presentes en una conferencia y con esto calcula la rata a la cual deben ser enviados los paquetes.

Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo de RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (UDP Port) como mecanismo de identificación de protocolos.

La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio. Se relaciona con el control de congestión y flujo de datos. El RTCP involucra varios tipos de mensajes, por ejemplo:

-Send report para emisión y recepción de estadísticas (en tiempo random) desde emisores activos. es uno de los más interesantes, disponen de 3 secciones bien diferenciadas:

1. Los primeros 8 Bytes se refieren a un encabezado común.

2. La segunda parte de 20 Bytes permite la evaluación de diferentes parámetros (retardo, jitter, eficiencia de datos, etc).

3. La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado. Incluye los siguientes reportes: cantidad total de paquetes RTP perdidos y a la proporción de los mismos; la cantidad de paquetes recibidos y el jitter entre paquetes; el horario del último paquete recibido y el retardo de transmisión del mismo.

-Receiver Report para recepción estadísticas desde emisores no activos.

-Source Description para un identificador de nivel de transporte denominado CNAME (Canonical Name).

-Bye para indicar el final de la participación en la conexión.

-Application para aplicaciones específicas.

2.2.6. Diagrama del Paquete de Transporte RTCP

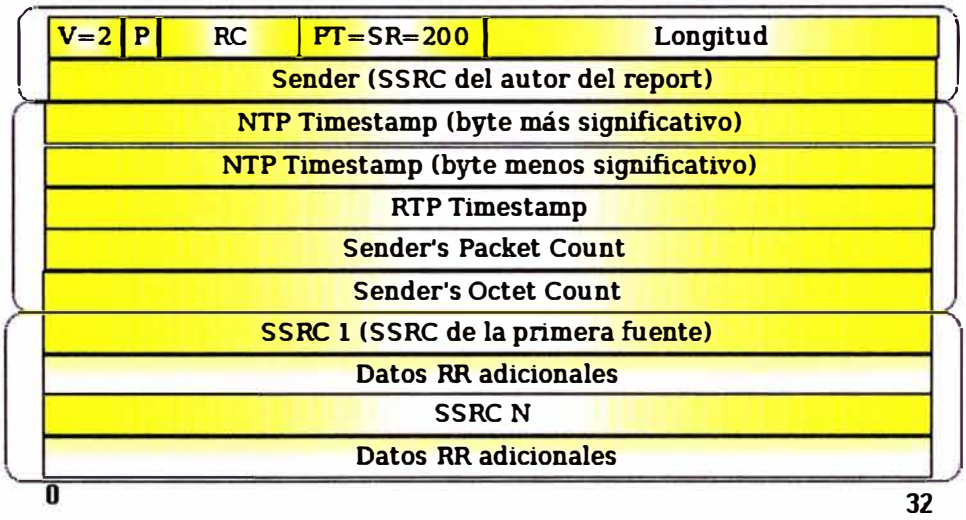


Figura 2.8 paquete RTCP

SR (Informe de emisor)	Conjunto de estadísticas de transmisión y recepción que proviene de participantes que son emisores activos.
RR (Informe del receptor)	Conjunto de estadísticas que proviene de participantes que sólo son receptores.
SDES (Descripción de fuente)	Los paquetes de descripción de fuente están compuestos de varios elementos, incluido el CNAME. Constituyen la «tarjeta de visita» de la fuente.
BYE (Mensaje de fin)	Indica que se termina una sesión.
APP	Funciones específicas de una determinada aplicación.

Tipos de paquetes RTCP

Figura 2.9 Tipos de paquetes RTCP

- PIMER CUERPO:

RC = Report Count PT: Carga util = 200 para SR. Longitud del reporte SSRC: que lo origina.

-SEGUNDO CUERPO:

NTP timestamp: segundos desde el 1/1/1900. entero y decimal.

Instante de tiempo en que se envia el reporte (32 +32).

RTP timestamp: el mismo enstante en ticks de RTP (equivalencia.

Paquetes y octetos enviados desde el inicio de la sesiòn por (SSRC).

-TERCER CUERPO:

Conjunto de RR, uno por cada fuente escuchada.

2.2.7. Diagrama del paquete completo de Transporte.

Los destinatarios de los paquetes RTP devuelven información sobre de la calidad de recepción, utilizando diferentes formas de paquetes RTCP, según si ellos mismos son emisores de contenido o no. Los dos tipos, SR y RR, contienen ninguno, uno o varios bloques de informe de receptor, previstos para la sincronización de las fuentes de las cuales el receptor ha recibido un paquete de contenido RTP desde el último informe. La evaluación de la calidad de recepción no es sólo útil para el emisor, sino también para el receptor y cualquier supervisor de red que pudiera existir. El emisor puede modificar su transmisión de acuerdo con la información recibida; el receptor puede inferir si las dificultades de recepción que observa son de origen local, regional o más amplio.

El supervisor recibirá solamente los paquetes RTCP, con lo cual podrá evaluar la calidad de funcionamiento de la red.

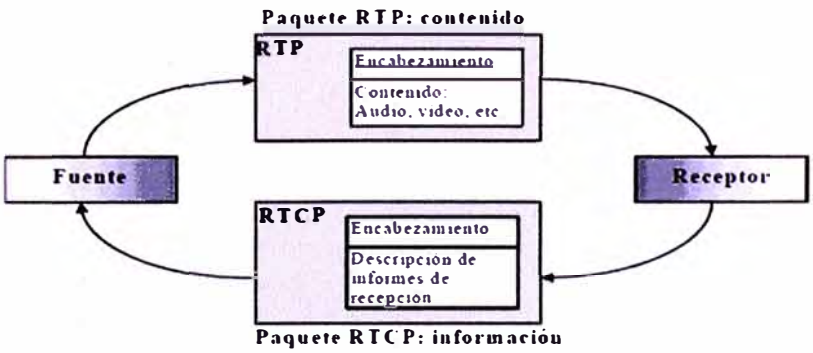


Figura 2.9 diagrama de paquetes RTP

2.3. SIGTRAN.

2.3.1 ¿Qué es el SIGTRAN ?

SIGTRAN (de signalling transport) es el nombre del grupo de trabajo del IETF encargado de definir una arquitectura para el transporte de señalización en tiempo real sobre redes IP. A raíz de ello, no sólo se creó una arquitectura, sino que se definió un conjunto de protocolos de comunicaciones para transportar mensajes SS7 sobre IP.

2.3.2 Arquitectura de los Protocolos SIGTRAN.

La arquitectura definida por el Sigtran [RFC2719] consta de tres componentes:

• IP estándar como protocolo de red.

• Un protocolo común de transporte de señalización. Los protocolos definidos por el Sigtran se basan en un nuevo protocolo de transporte sobre IP, llamado SCTP (Stream Control Transmission Protocol).

• Capas de adaptación específicas para cada capa de la torre SS7 que se necesite transportar. El IETF ha definido las siguientes: M2PA, M2UA, M3UA, SUA, TUA e IUA. IP SCTP Capa de adaptación S7UP/S7AP

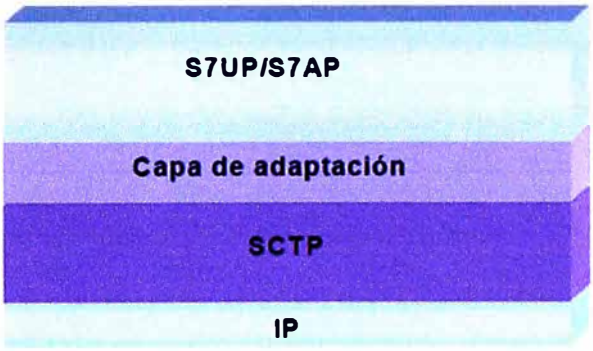


Figura 2.10 Arquitectura protocolos SIGRAN

a).- M2UA [RFC 3331].

M2UA son las siglas de MTP2 User Adaptation. El protocolo M2UA, al igual que M2PA, adapta MTP3 a SCTP, e igualmente gestiona asociaciones SCTP en lugar de enlaces MTP3. M2UA permite el intercambio de mensajes MTP3 entre dos puntos de señalización IP o entre un punto de señalización IP y una pasarela IP-SS7.

M2UA es un protocolo entre pares en caso de que la comunicación comience y termine en dos puntos de señalización IP, sin SGWs intermedios, tal como muestra la Figura 2.11.

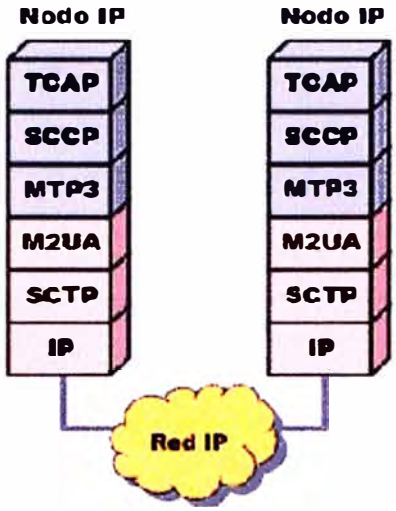


Figura 2.11. Transporte de MTP3 entre 2 puntos de señalización IP, mediante M2UA

Sin embargo, M2UA no es un protocolo entre pares si se implementa en una pasarela de señalización. En ese caso, M2UA no procesa las órdenes (primitivas del protocolo) que le llegan desde la capa superior (MTP3), sino que las envía tal cual hacia un nodo remoto, mediante SCTP. Como M2UA no procesa las primitivas de MTP3, sino que las reenvía, en caso de que se utilice un SGW se debe entender este protocolo como un medio que comunica la capa MTP3 de un nodo IP con la capa MTP2 de un SGW, como a Figura 2.12.

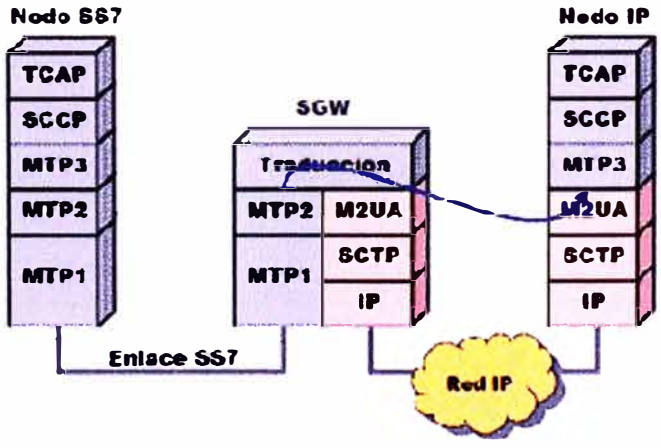


Figura 2.12. Transporte de primitiva MTP3 hacia una capa MTP2 remota, mediante M2UA

De esta forma, varios puntos de señalización IP con MTP3 sobre M2UA pueden acceder a la red SS7 tradicional a través de los mismos enlaces MTP2 físicos.

Es importante tener en cuenta que, debido a la propia naturaleza del protocolo, sólo puede existir un SGW M2UA en una misma comunicación MTP3, por lo que no se puede utilizar para transportar mensajes MTP3 entre dos nodos SS7 puros a través de una red IP. Si se utiliza M2UA, alguno de los extremos es un punto de señalización IP.

b).- M3UA [RFC 3332].

M3UA son las siglas de MTP3-User Adaptation. M3UA es un protocolo que

transporta mensajes procedentes de un usuario de MTP3 (ISUP, TUP o SCCP) a través de una red SCTP/IP hasta un nodo remoto.

De forma similar a M2UA, M3UA simplemente transporta los mensajes hasta el destino, pero no realiza por sí mismo las funciones de la capa MTP3. Esto significa que M3UA no dispone de tablas de encaminamiento basadas en puntos de señalización, ni realiza ninguna otra función propia de MTP3.

En general, M3UA se utilizará como medio de transporte de primitivas entre la capa usuaria de MTP-3 (SCCP o ISUP) de un punto de señalización IP y la capa MTP3 de un SGW remoto, tal como muestra la Figura 2.13.

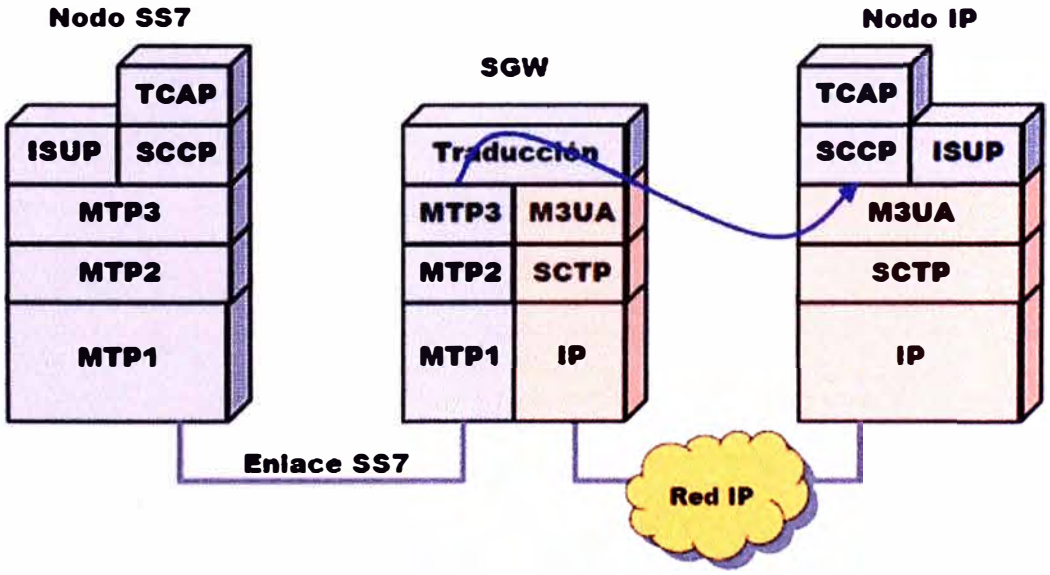


Figura 2.13. transporte entre SGW remotos.

Utilización de M3UA.

Como se ha visto, dado que M3UA transporta primitivas desde la capa ISUP o SCCP de un nodo hasta la capa MTP3 de otro (típicamente un SGW), este protocolo sólo puede utilizarse para conectar nodos con señalización IP a una red SS7. Por tanto, no se puede utilizar M3UA para descargar tráfico SS7 entre dos nodos TDM a través de red IP, a no ser que se utilicen SGWs con SCCP. Pero para esta aplicación es mucho más adecuado utilizar SGWs con M2PA, por los motivos indicados en el apartado 3.3.

2.3.3.- Características principales del SIGTRAN.

Debido a los inconvenientes mencionados de TCP y UDP, el SIGTRAN definió del protocolo SCTP, cuyas principales características son las siguientes:

• Es un protocolo punto a punto. Se establece intercambio de datos entre dos extremos conocidos.

• Define tiempos de reintento (time-outs) mucho menores que los de TCP.

• Proporciona transporte fiable de datos de usuario, detectando y reparando los datos erróneos o fuera de secuencia. • Se adapta a la tasa de transferencia, disminuyendo la velocidad de envío de datos en caso de congestión en la red.

• Permite definir en un mismo extremo SCTP en varios servidores físicos (multihoming). Un único extremo SCTP se puede definir en varias direcciones IP.Hacia cada una de ellas se encaminan los mensajes de forma independiente, de manera que si uno de los nodos físicos queda fuera de servicio, el resto de comunicaciones no se ven afectadas.

2.3.4. Funciones de SCTP

Una asociación SCTP es una relación de comunicación de mensajes entre dos entidades SCTP (comunicación orientada a conexión). Las asociaciones SCTP se establecen a petición del usuario de nivel superior de este protocolo. Para proporcionar protección frente a ataques de denegación de servicio, se emplea un protocolo de establecimiento de asociaciones en cuatro pasos, basado en cookies [RFC2522].

Dentro del protocolo SCTP, se utiliza el término stream para referirse a una secuencia de mensajes de usuario que debe entregarse al nivel superior de forma ordenada. El número de streams que se enviarán a través de una asociación se define en el establecimiento de la misma, de forma negociada entre ambos extremos de la comunicación. Los streams son unidireccionales, de forma que para una comunicación bidireccional se deberán definir al menos dos streams en una asociación SCTP.

Los mensajes de usuario se asocian a streams determinados, de forma que el extremo receptor SCTP entrega al nivel superior todos los mensajes de un mismostream en el mismo orden en que se enviaron. Sin embargo, no existen restricciones de entrega ordenada entre mensajes de distintos streams de la misma asociación. De esta forma, los mensajes de un stream se pueden seguir entregando aunque otro esté bloqueado esperando el siguiente mensaje. Adicionalmente, SCTP proporciona un mecanismo para no utilizar el servicio de entrega ordenada de mensajes, de forma que los mensajes enviados mediante dicho mecanismo se entregan al nivel superior del destino SCTP tan pronto como se reciben.

2.3.5.- Formatos de Paquetes SCTP.

Un paquete SCTP se compone de una cabecera de 24 octetos y una serie de unidades de información, denominadas chunks. Estas unidades de información pueden contener datos de usuario, o instrucciones de control del propio protocolo SCTP (establecimiento y liberación de asociaciones, control de flujo, retransmisiones, etc). Los chunks tienen estructura propia, y presentan una serie de campos, dependiendo del tipo de chunk que sean.

En el ámbito de la planificación de una red SS7 sobre IP, el dato más relevante es el tamaño de las cabeceras de los datos de usuario. La cabecera de un chunk de datos de usuario mide 16 octetos, y pueden contener hasta 65520 octetos de información del nivel superior. Esto significa que, en principio, cualquier mensaje de cualquier operación MAP, ISUP o CAMEL cabe en un chunk de datos SCTP, incluyendo las cabeceras de los protocolos de adaptación intermedios.

Además, SCTP permite transportar varios mensajes de usuario en un único mensaje SCTP, mediante el uso de distintos chunks de datos dentro del mismo mensaje.

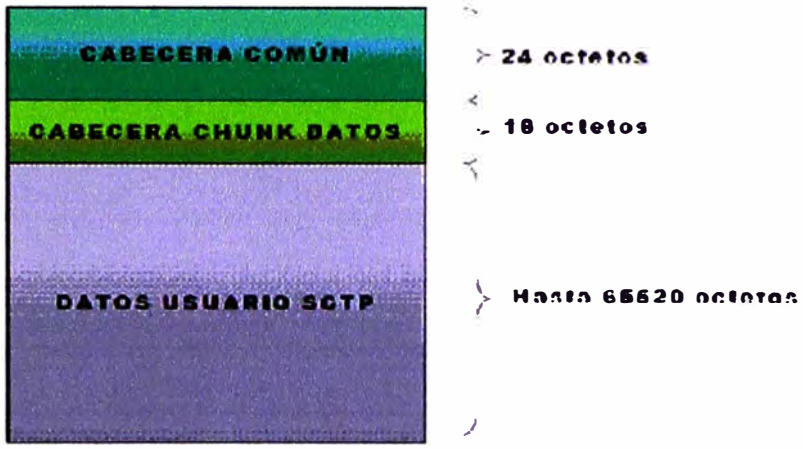


Figura 2.14. Formato Paquetes SCTP con datos de usuario

2.3.6. Validación de Paquetes.

Dentro de la cabecera común de SCTP se incluye un campo de verificación obligatorio, aparte de otro campo de 32 bits con una suma de comprobación (checksum) frente a errores. El valor del campo de verificación obligatorio lo decide el extremo de la comunicación SCTP en el establecimiento de la asociación. De esta forma se consigue más protección frente a comunicaciones con suplantación de identidad. La suma de comprobación se calcula a partir de los datos de la propia cabecera SCTP y la protege frente a errores en la comunicación.

a).- Gestión de conexiones

El usuario del nivel SCTP puede manipular el conjunto de direcciones de transporte destino de los mensajes. La función de gestión de conexiones de SCTP escoge la dirección de transporte destino para cada paquete SCTP que se envía, basándose en las instrucciones del usuario de SCTP y en las direcciones disponibles alcanzables para ese destino SCTP.

En periodos de inactividad, la función de gestión de conexiones monitoriza la disponibilidad de los extremos de la comunicación mediante mensajes de comprobación (heartbeats). Si SCTP percibe algún extremo como inalcanzable informa a su usuario de

nivel superior. En el establecimiento de la asociación, se define un camino primario para cada extremo SCTP, que es el que se usa en el envío normal de paquetes.

En el extremo receptor, la gestión de conexiones se encarga de comprobar la existencia de una asociación SCTP válida a la que pertenece cada paquete SCTP recibido.

b).-. Fragmentación de los datos del usuario

SCTP posee mecanismos de fragmentación y re-ensamblado de mensajes de usuario para adecuarlos al tamaño requerido por el nivel inferior (IP en el caso de SS7 sobre IP).

c).- Control de entrega de mensajes.

SCTP asigna un número de secuencia de transmisión (TSN) a cada mensaje de datos de usuario, fragmentado o no. El TSN es independiente del stream por el que se envía el mensaje. El extremo receptor envía acuses de recibo (ACK) de todos los TSNs recibidos, aunque no lleguen de forma ordenada. De esta forma, la fiabilidad en la entrega de los mensajes se mantiene funcionalmente separada de la entrega ordenada dentro del stream.

CAPITULO III

COMPONENTES DE UNA CENTRAL IP Y ESTABLECIMIENTO DE LLAMADAS

3.1.- Componentes central IP

Este estándar define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define los siguientes componente más relevantes como se muestra en la siguiente figura:

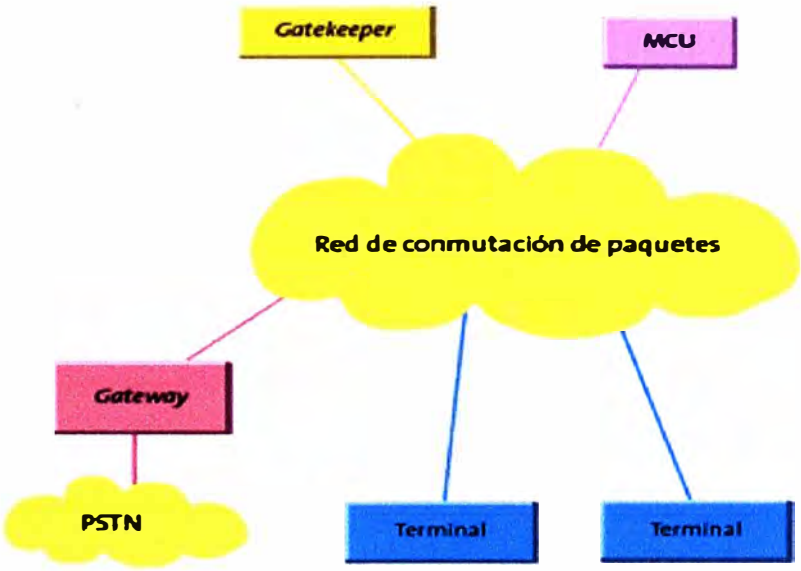


Figura 3.1 componentes H323

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.

Terminal:

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Las funciones de control que realizan los terminales son las siguientes:

H.245 para negociación del canal.

H.225.0 (Q.931) para señalización y control de llamada.

H.225.0 (RAS) para comunicación con el gatekeeper.

También implementan los protocolos RTP/RTCP para el manejo de los flujos de audio y video.

3.1.1.- Gatekeeper:

El gatekeeper (GK) 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. El Gatekeeper 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 que debe desarrollar un gatekeeper son las siguientes:

- Control de la señalización.
- Control de acceso y administración de recursos, autorización de llamadas.
- Traducción de direcciones de transporte entre direcciones IP y alias.
- gestión del ancho de banda.
- gestión de llamadas(concesión de permisos...)
- gestión del ancho de banda.

Para desarrollar estas funciones , entre el gatekeeper y el endpoint se emplea el protocolo RAS (Registration /Admission /Status) sobre UDP.

Un gatekeeper y sus endpoints definen una zona H.323, de manera que en entornos LAN's es suficiente un gatekeeper, pero en entornos como Internet, son necesarios varios de ellos, cada uno definiendo una zona H.323.

Lógicamente, entre gatekeepers se requerirá comunicación, por lo que actúa como el punto central para todas las llamadas en una zona, comportándose como un conmutador virtual.

Si bien el gatekeeper no es obligatorio, su empleo en un entorno H.323 sí posibilita emplear más eficientemente la plataforma, por ejemplo mediante el enrutamiento de llamadas a su través.

Los gatekeepers son entidades funcionales separadas de los endpoints H.323, pero es posible incluir funcionalidades gatekeepers en los gateways y las MCU's.

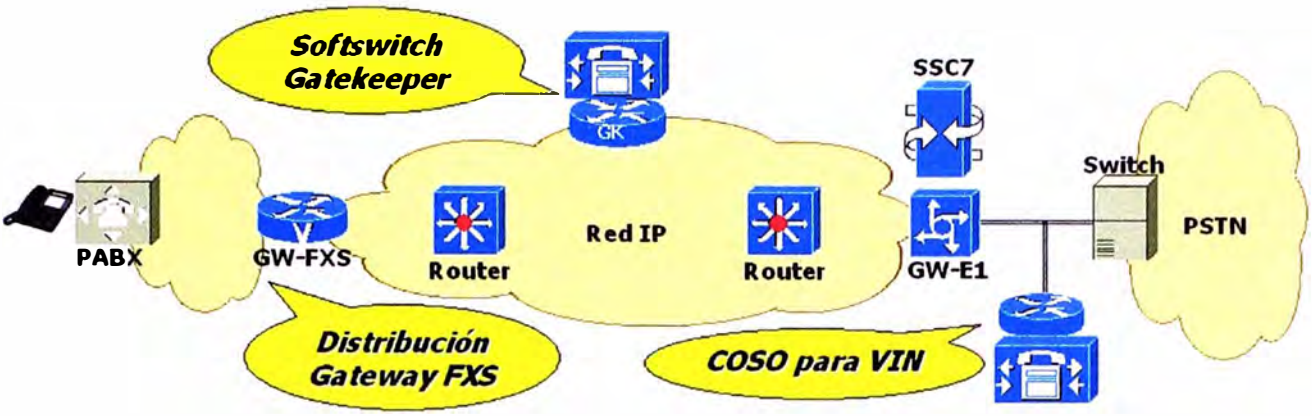


Figura 3.2. Componentes en una red de Telefonía-IP.

b).-Gateway:

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. 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. los gateways, son los sistemas encargados de permitir que los equipos H.323 puedan operar con otras redes.

Desarrollan la traducción de la señalización, información de control e información de usuario, posibilitando así interoperabilidad entre redes, terminales y servicios, haciendo viable la integración de servicios aún con plataformas dispares, llámese PSTN y redes IP.

Una diferencia respecto a los gatekeepers, es que los gateways sí cursan información de usuario, soportada en RTP/UDP/IP.

Funciones de los gateways:

transcodificación de audio y vídeo.

traducción de procedimientos de comunicación.

traducción de formatos de transmisión.

Evidentemente, dada su funcionalidad, los gateways son elementos opcionales en entornos H.323, y sólo son necesarios cuando se requiere una interconexión entre entornos H.323 y entornos no H.323:

c).- MCU (Multipoint Control Units):

La Unidad de Control Multipunto 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.

Dado el jitter, que sufren los paquetes IP en la red, y las consecuencias negativas de esto para el tráfico de audio y vídeo, en el terminal H.323 se requiere un buffer de recepción para absorber, en la medida de lo posible, estas fluctuaciones en la demora de los paquetes IP, anulando o reduciendo el efecto negativo que el jitter puede producir en flujos de información de usuario con requerimientos de tiempo real.

Los protocolos de control comprendidos en H.323, unos se encapsulan en UDP (protocolos H.225.0 (RAS, Registration Admisión Status), que se desarrolla entre el gatekeeper y los endpoints) y otros en TCP (H.225.0 (Q.931), para el control de la llamada y H.245 para el control del canal.

3.2.- Procedimiento de Comunicación H.323.

El procedimiento de funcionamiento de los protocolos de la suite H.323 se describe con detalle a continuación. En H.323 se encuentran 3 tipos de mensajes de señalización diferentes:

-H.245: se describen estos mensajes en forma de texto concatenado en letras tipo bold (por ejemplo se menciona el mensaje: maximumDelayJitter).

-RAS: se representa mediante 3 letras (por ejemplo ARQ).

-H.225/Q.931: representado en una o dos palabras con la primer letra en mayúsculas (ejemplo: Call Proceeding). Es usado para encapsular los mensajes H.245 de señalización entre terminales y originalmente fue diseñado como protocolo DSS1 en capa 3/7 para los accesos ISDN.

3.2.1- Fase de Mantenimiento de la Registración.

Contiene un intercambio de mensajes para mantener activa la conexión entre los Gateways GW y el Gatekeeper GK. Ver la Figura 3 para el intercambio de mensajes de RAS.

- Discovery. Este primer paso es el proceso por el cual el GW determina cual es el GK que atiende a la red en ese momento. El mensaje desde el GW es del tipo multicast y se denomina GRQ (*Gatekeeper Request*). El GK responde con la aceptación GCF (*GK Confirmation*) o rechazo GRJ (*GK Reject*). El GK puede indicar un GK alternativo mediante mensajes alternateGatekeeper. Si no se está en condiciones de procesar el request, se puede enviar un mensaje RIP (*Requst in Progress*) para indicar que se está procesando el request; esto resetea el timeout de la conexión.

- Registration. El GW informa de sus direcciones de transporte y alias mediante RRQ (*Registration Request*) y el GK responde con RCF (*Registration Confirmation*) o RRJ (*Registration Reject*). El RRQ se emite en forma periódica. La registración tiene un tiempo de duración (expresado en segundos) para lo cual se utiliza el mensaje timeToLive. El terminal o el GK puede cancelar la registración mediante el mensaje URQ (*Unregister Request*) al cual le corresponde la confirmación URF (*Unregister Confirmation*).

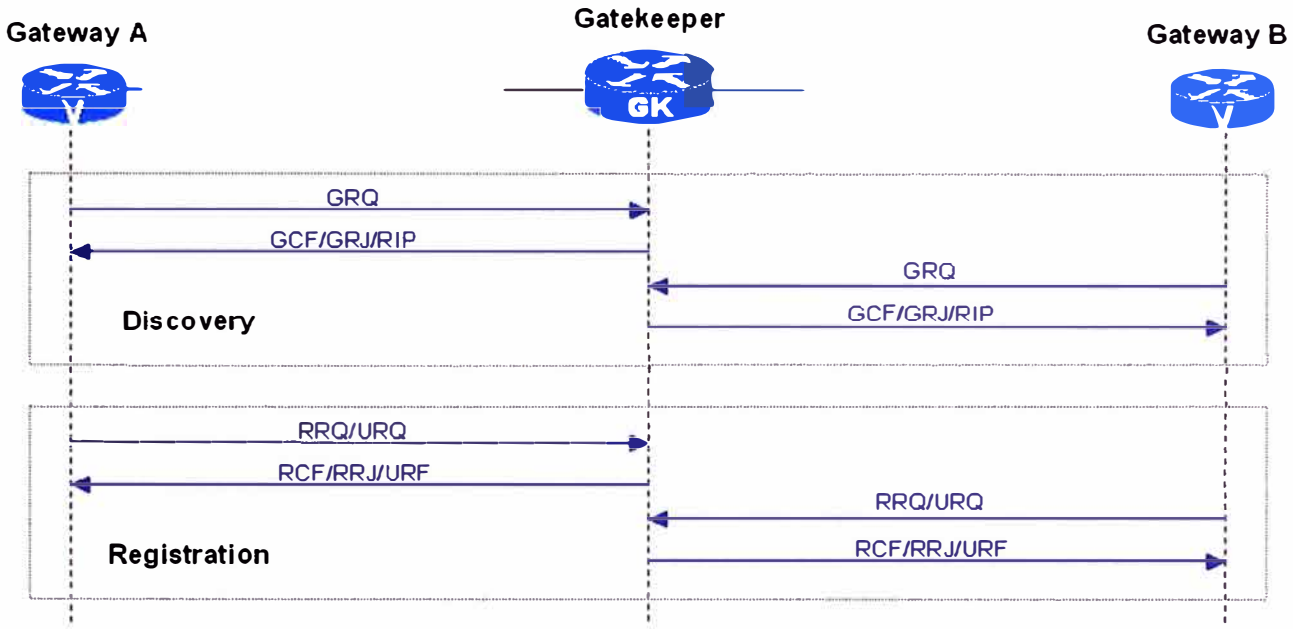


Figura 3.3. Fase de mantenimiento de la registración entre GW y GK.

- Location. Un GW o GK que tiene un alias para un GW y quiere determinar su información de contacto, puede emitir el mensaje de requerimiento de localización LRQ (*Location Request*). Al cual le corresponde la confirmación LCF (*Location Confirmation*) con la información requerida. La dirección puede ser del tipo E.164 si se trata de un GK fuera de la red.

De existir varios GK se disponen de mensajes para intercomunicación, por ejemplo, LRQ para *Locate Request* y LCF para *Locate Confirm*.

- Status. Se trata de un mensaje periódico (mayor a 10 segundos) que emite el GK al terminal para determinar el estado y requerir un diagnóstico. Se trata de los mensajes IRQ (*Information Request*) y IRR (*Information Response*). La habilitación se realiza mediante willRespondToIRR enviado en el mensaje RCF o ACF.

3.2.2- Fase de Conexión de la llamada.

Representa las distintas etapas para establecer una llamada.

- Admission. En la Figura 4, el proceso se inicia cuando desde la PSTN se recibe un mensaje de Setup para inicio de una llamada entrante en protocolo ISUP (de la suite de protocolos de señalización telefónica SS7). El GW responde a la PSTN mediante el mensaje Call Proceesing, para mantener la conexión en espera.

El GW requiere iniciar una llamada mediante el pedido de admisión desde GW al GK. Este mensaje es ARQ (*Admissions Request*) y contiene un requerimiento Call Bandwidth (en formato Q.931). El GK puede reducir las características de la solicitud en el mensaje de confirmación ACF (*Admissions Confirm*).

En el mismo mensaje ARQ se dispone de la funcionalidad TransportQOS para habilitar la funcionalidad de reservación de ancho de banda RSVP, para servicios unidireccionales (orientado-al-receptor).

a)- Setup Modo No-Ruteado. Una vez admitido el GW-B por el GK el procedimiento se bifurca en el modo ruteado y no-ruteado. En el modo de operación no-ruteado, el GK informa al GW-B cual es la dirección IP del GW-A al cual va dirigida la llamada, de acuerdo con la dirección E.164 recibida en el mensaje ARQ. Ahora, el GW-B se comunica con el GW-A que fue indicado por el GK y le envía el mensaje Setup. Este mensaje (en protocolo Q.931) es respondido mediante el mensaje Call Proceesing.

El GW-A se ocupa de registrarse mediante ARQ y recibe desde el GK el mensaje ACF. Con estas acciones cumplidas, el GW-A se ocupa de informar al usuario de la llamada entrante (corriente de llamada al teléfono) y hacia el GW-B le envía el mensaje de Alerting en Q.931 para indicar el estado de llamada. El GW-B envía el mensaje de Alerting a la PSTN, ahora en formato de protocolo ISUP.

b)- Setup Modo Ruteado. Para el caso de trabajar con Modo Ruteado, el mensaje de Setup entre GW pasa por el GK. En el caso No-Ruteado anterior, el GK se desentiende de

la conexión y solo se ocupa de la traslación entre direcciones E.164 y IP. En el modo ruteado el GK seguirá toda la conexión, de forma que haciendo uso de las funcionalidades de Softswitch se podrán ofrecer servicios de valor agregado.

- Conect. Cuando el usuario en el GW-A responde se genera el mensaje Q.931 de Connect. Este mensaje se emite hacia el GK (Modo Ruteado), quien hace lo mismo hacia el GW-B y este lo imita hacia la PSTN pero en protocolo ISUP. Ver la Figura 5.

El paso siguiente es establecer las capacidades de los terminales utilizando el protocolo H.245 entre GWs. Se trata del mensaje TerminalCapabilitySet de solicitud y el TerminalCapabilityAck de respuesta, que permite determinar capacidad del terminal, tipo de codificador, canal lógico, etc. Finalmente, se envía el mensaje OpenLogical Channel para abrir un canal lógico.

- Canal Vocal. El canal vocal se transporta sobre los protocolos RTP de la suite IP.

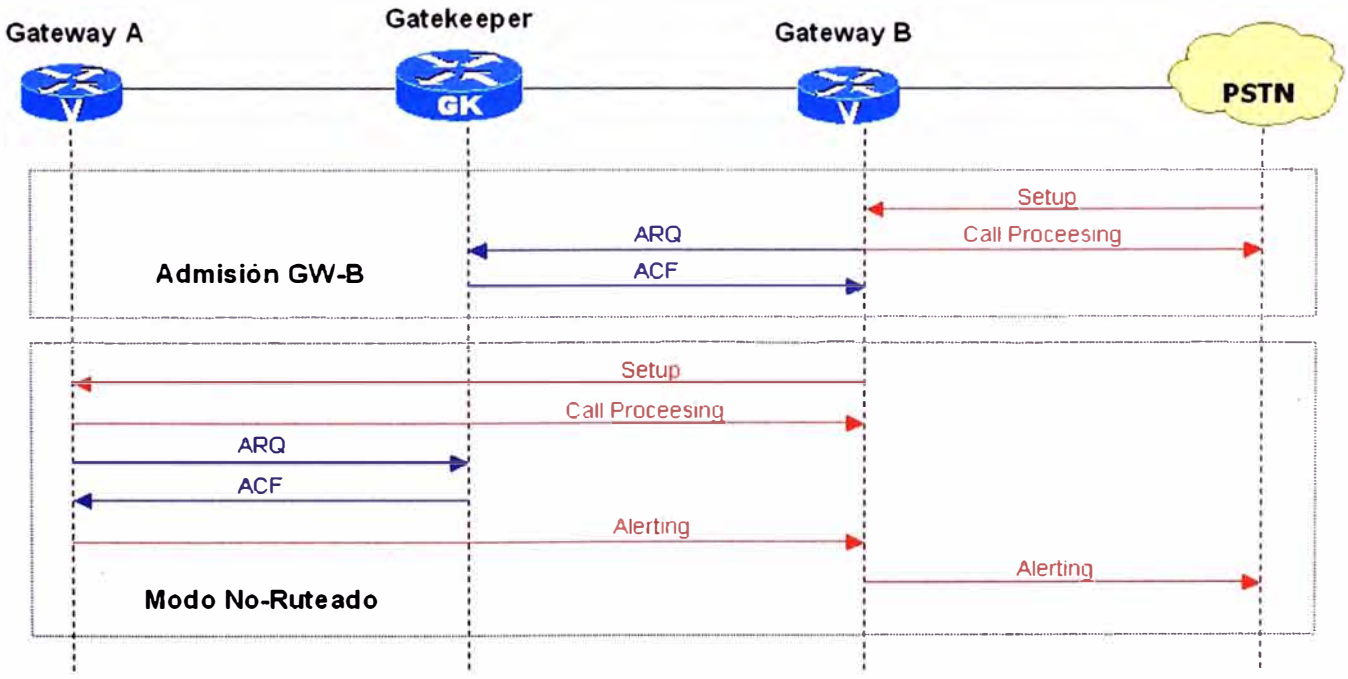


Figura 3.4 Operación de Conexión mediante el Modo No-Ruteado

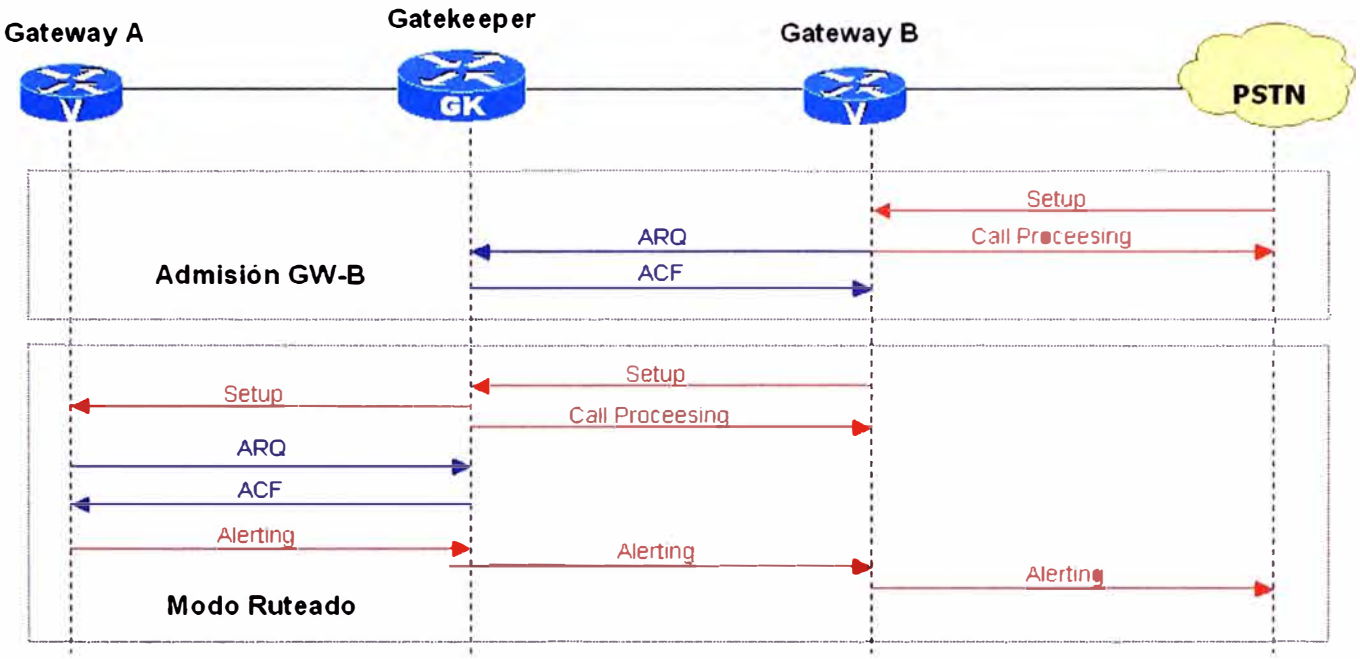


Figura 3.5 Operación de Conexión mediante el Modo No-Ruteado

- Bandwidth. Durante una conexión el terminal o el GK pueden requerir el cambio de ancho de banda del canal mediante el mensaje BCR (*Bandwidth Change Request*).

3.2.3.- Fase de desconexión de la llamada.

En la Figura 3.6 se indica la fase de desconexión de la llamada. La misma se realiza con mensajes Release Complete de Q.931 y DRQ (*Delete Request*) y DCF (*Delete Confirm*) de RAS.

Sobre el paquete Q.931 (H.225) se disponen de distintos tipos de mensajes:

-Mensajes para establecimiento de llamada: Alerting, Call Proceeding, Connect, Setup, Progress, etc.

-Mensajes para la fase de información de llamada: Resume, Suspend, User Information, etc.

-Mensajes para el cierre de la llamada: Disconnect, Release, Restart, etc.

-Mensajes misceláneos: Segment, Congestion Control, Information, Notify, Status, Status Enquiry, etc.

Los mensajes manejados en el ámbito de H.245 (durante la fase de comunicación telefónica) son:

-multimediaSystemControl para efectuar el control del sistema; las variantes del mensaje son request, response, command and indication.

-otros mensajes de interés son: masterSlaveDetermination, terminalCapability, MaintenanceLoop, communication Mode, communicationMode, conferenceRequest and Response, terminal-ID.

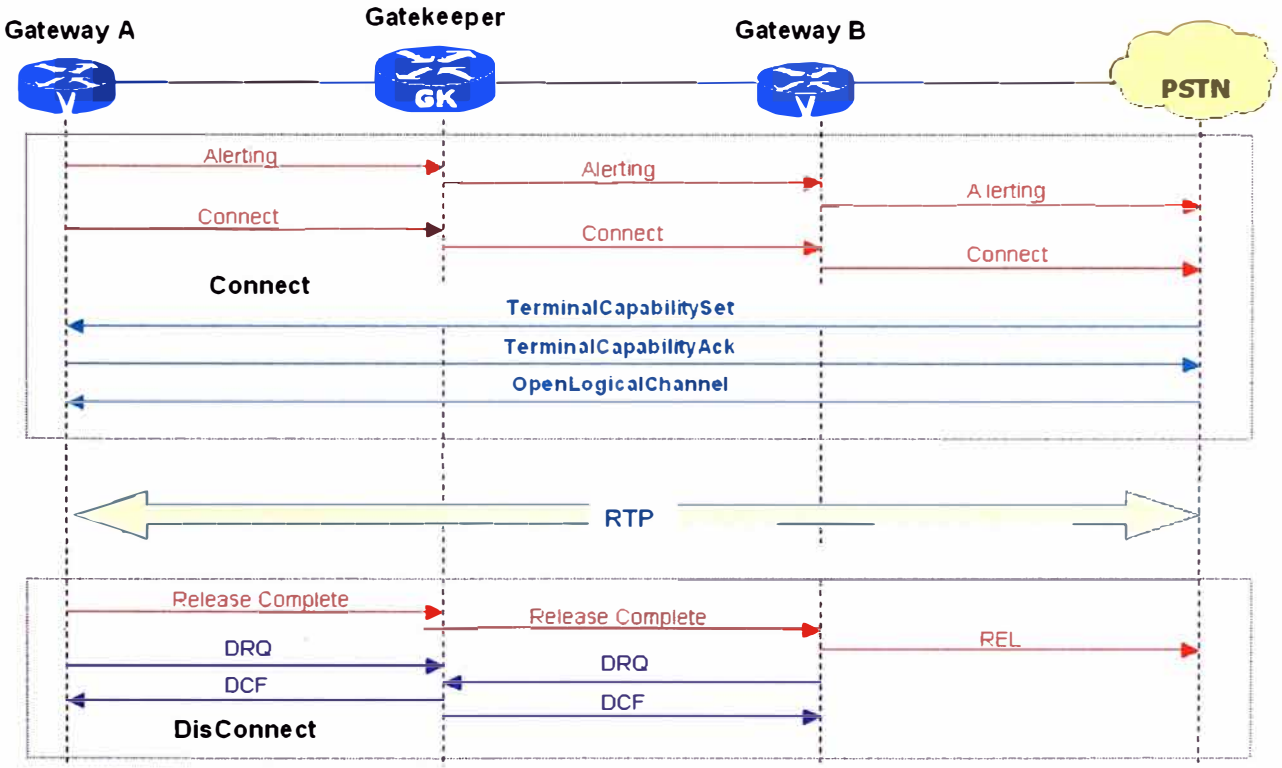


Figura 3.6. Conexión final de la llamada y desconexión de la misma en Modo Ruteado.

3.3 Establecimiento de una llamada básica de SIP

En la figura 3.7 se observa la manera de establecimiento de una llamada, el usuario paco[arroba]bbva.com quiere hablar con emilio[arroba]bbva.com es decir con un usuario que habitualmente está en su mismo dominio; pero por algún motivo, que desconocemos, hoy no está en bbva.com, sino en bbv.es aunque paco no lo sabe: tal es así que manda una invitación (invocará un método INVITE) para el usuario emilio[arroba]bbva.com al servidor responsable de su dominio (en este caso es un servidor proxy con estado, 'Stateful Proxy 1').

El servidor enviará la invitación a un servidor para de redirección para tratar de averigüar la localización actual de emilio. Es este servidor de redirección el que determina que el usuario emilio está en el dominio bbv.es y le contesta al proxy con un 302 MOVED TEMPORARILY que incluye la nueva dirección de emilio(sip:emilio[arroba]bbv.es). El proxy responde con un 302 ACK, puesto que aquí termina la secuencia de la invitación inicial (INVITE(1) de la figura).

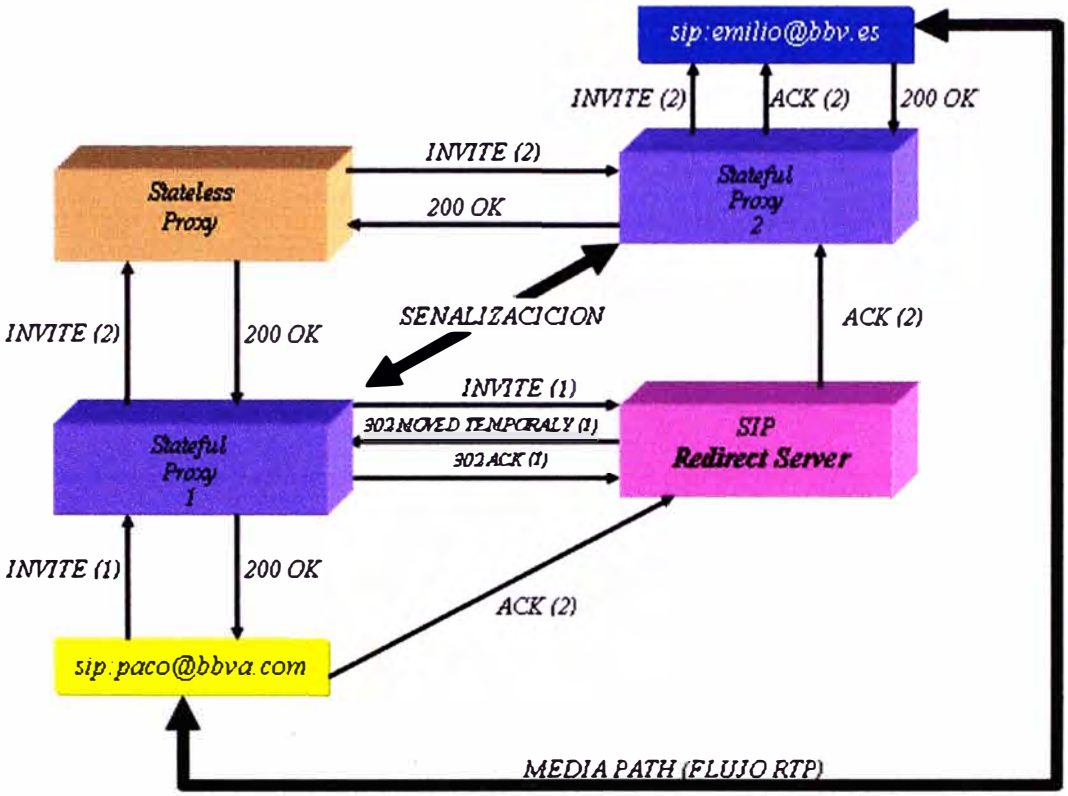


Figura 3.7 Establecimiento de una llamada SIP

A partir de esta situación, el Proxy 1 [con estado] (Stateful Proxy 1) podría mandarle la dirección de emilio a paco para que él tratara de comunicarse con ´directamente con sip:emilio[arroba]bbv.es. En el ejemplo, lo que hace el proxy 1 es modificar la invitación y tratar de encontrar a sip:emilio[arroba]bbv.es. Como no conoce a ningún otro servidor con estado que se responsabilice del dominio bbv.es, pasará la invitación a un servidor sin estado ('Stateless proxy') que conocerá el siguiente salto que debe seguir para llegar hasta sip:emilio[arroba]bbv.es.

Para simplificar el ejemplo hemos querido que ese primer proxy sin estado conozca a un servidor proxy que controla el dominio bbv.es ('Stateful Proxy 2'). Ese segundo proxy completa la entrega de la invitación para sip:emilio[arroba]bbv.es; momento en el cual emilio acepta la llamada enviando un mensaje de respuesta (200 OK), que recorre el mismo camino de vuelta de la invitación hasta llegar a sip:paco[arroba]bbva.com. Ahora paco debería mandarle un ACK de esta respuesta a emilio; y aunque en principio podría hacerlo directamente, en nuestro ejemplo hemos decidido que toda la señalización pase por los proxies de cada dominio (se supone que así lo habrán indicado en los mensajes de invitación que se han cruzado).

SIP sigue el modelo Cliente/Servidor: los proveedores de servicio [de acceso troncal] podrían ofrecer esa infraestructura SIP como un servicio IP más a otros proveedores de servicio, que a su vez podrían montar sobre ella sus propios servicios SIP que comercializarían en modo ISP/ASP.

SIP proporciona los mecanismos necesarios para ofrecer una serie de servicios:

Usuarios:

Localización.

Disponibilidad y capacidades (servicio de presencia y terminal asociado).

Perfil.

Llamadas

Establecimiento.

Mantenimiento.

Desvíos.

Traducción de direcciones.

Entrega de los números llamado y llamante.

Movilidad: direccionamiento único independiente de la ubicación del usuario.

Negociación del tipo de terminal

Negociación de las capacidades del terminal.

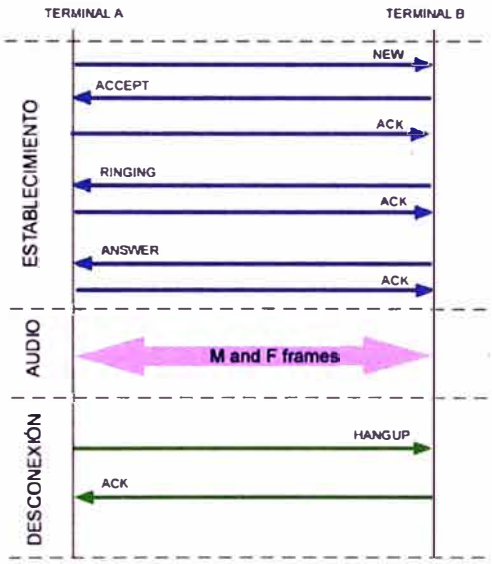
Autenticación de usuarios llamado y llamante.

Transferencias ciegas y supervisadas.

Incorporación a conferencias multicast.

3.4.- Establecimiento de llamada en IAX

Para poder entender el protocolo IAX vamos a ver un grafico del flujo de datos de una comunicación IAX2:



Una llamada IAX o IAX2 tiene tres fases:

a) Establecimiento de la llamada

El terminal A inicia una conexión y manda un mensaje "new". El terminal llamado responde con un "accept" y el llamante le responde con un "Ack". A continuación el terminal llamado da las señales de "ringing" y el llamante contesta con un "ack" para confirmar la recepción del mensaje. Por último, el llamado acepta la llamada con un "answer" y el llamante confirma ese mensaje.

b Flujo de datos o flujo de audio

Se mandan los frames M y F en ambos sentidos con la información vocal. Los frames M son mini-frames que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Los frames F son frames completos que incluyen información de sincronización.

Es importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.

c) Liberación de la llamada o desconexión

La liberación de la conexión es tan sencillo como enviar un mensaje de "hangup" y confirmar dicho mensaje.

3.5- Protocolo MGCP.

El MGCP es un protocolo que soporta un control de señalización de llamada escalable. El control de calidad de servicio QoS se integra en el gateway GW o en el controlador de llamadas MGC. Este protocolo tiene su origen en el SGCP (de Cisco y Bellcore) e IPDC. Bellcore y Level3 plantearon el MGCP a varios organismos.

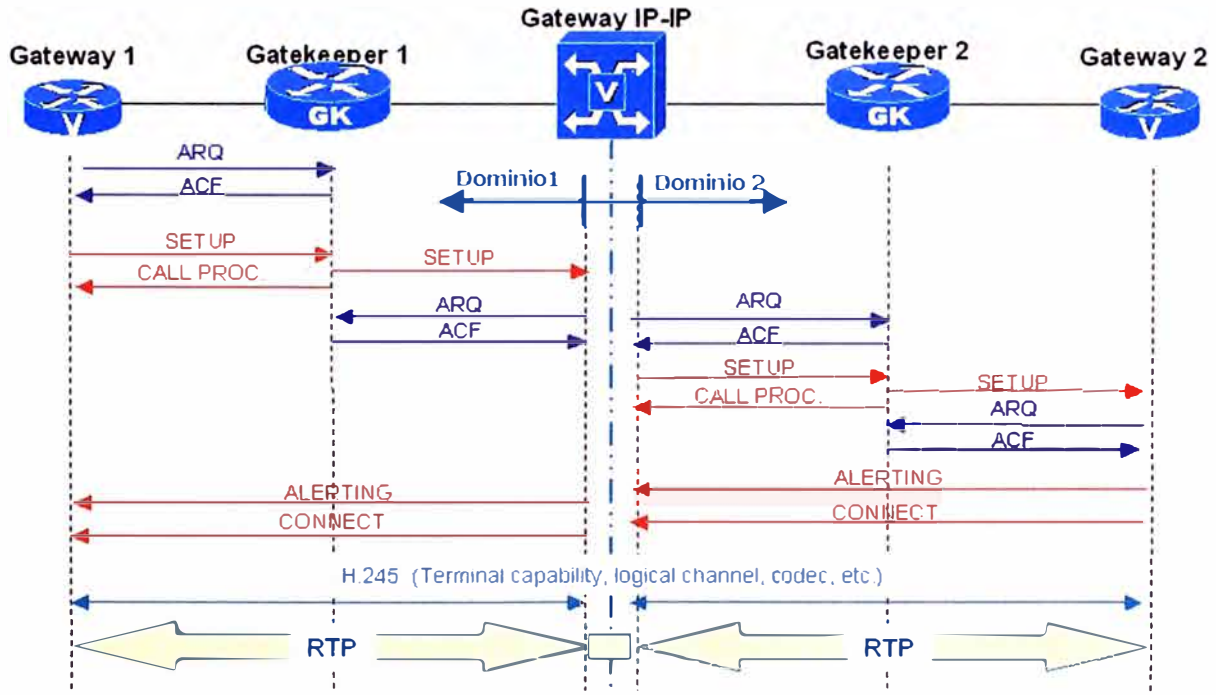


Figura 3.9. Proceso de comunicación entre dominios con el GW IP-IP.

El protocolo SIP se aplica para sesiones punto-a-punto unicast. Puede ser usado para enviar una invitación a participar en una conferencia multicast. Utiliza el modelo cliente-servidor y se adapta para las aplicaciones de Telefonía-IP. El server puede actuar en modo proxy o redirect (se direcciona el requerimiento de llamada a un server apropiado).

El MGCP es un protocolo que permite comunicar al controlador de gateway MGC (también conocido como *Call Agent*) con las gateway GW de telefonía (hacia la PABX o PSTN). La primera versión 1.0 es de octubre-1999 (RFC-2705). Se trata de un protocolo de tipo master-slave donde el MGC informa las acciones a seguir al GW. Los mensajes MGCP viajan sobre UDP/IP, por la misma red de transporte IP con seguridad IPsec.

El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El GW solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto. El protocolo MGCP entrega al GW la dirección IP, el port de UDP y los perfiles de RPT.

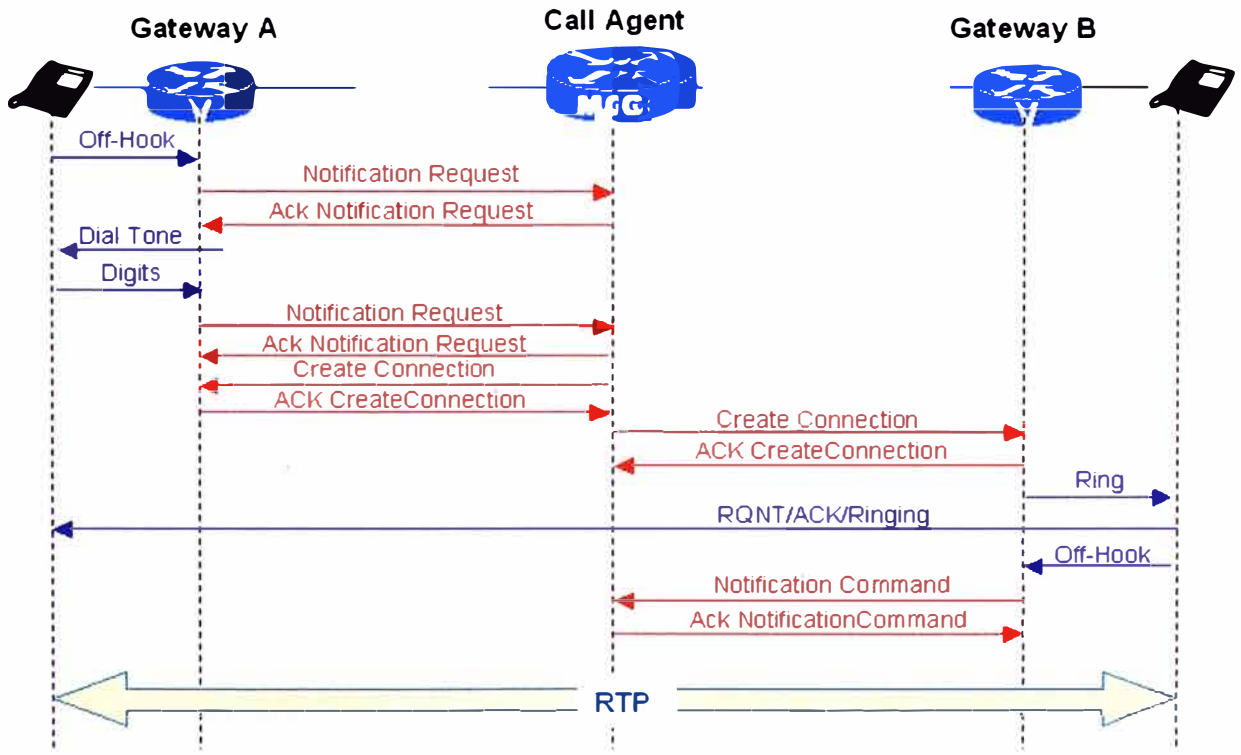


Figura3.10 Proceso de comunicación con protocolo MGCP.

En la Figura 3.10 se muestra el intercambio de mensajes en el establecimiento de una comunicación con protocolo MGCP. Los mensajes o comandos disponibles en MGCP son los siguientes:

Comando *NotificationsRequest*. Este primer mensaje se genera ante el requerimiento de conexión de un teléfono. El GW-A indica al MGC el requerimiento del usuario A. Como

respuesta se recibe un *Ack-NotificationRequest.* El mismo comando transfiere los dígitos discados cuando el usuario termina la marcación correspondiente.

Mensaje *CreateConnection,*. Es utilizado para crear una conexión que se inicia en el GW. Se envía a ambos GW y se recibe el comando de confirmación *Ack-CreateConnection.* El comando *ModifyConnection*, puede ser usado para cambiar los parámetros de la conexión existente. El comando *DeleteConnection* es usado en cambio para cancelar la conexión existente al final de la llamada. Otro comando, *AuditConnection*, es usado para requerir el estado de la conexión.

Con ambos extremos conectados, se entrega la señal de llamada al extremo del GW-B y finalmente se establece la conexión entre extremos.

Comando *DeleteConnection.* Utilizado para el cierre de la llamada. Como respuesta el GW envía una serie de informaciones obtenidas desde el protocolo RTP número de paquetes y de Bytes emitidos; número de paquetes y Bytes recibidos; número de paquetes perdidos; jitter promedio en mseg, retardo de la transmisión, etc.

Comando *AuditEndpoint*. Es usado para requerir el estado del extremo al GW. Los comandos *AuditEndpoint* y *AuditConnection* permiten obtener información que posteriormente forman parte de la MIB y pueden consultadas mediante el protocolo SNMP por el sistema de Management. Por ejemplo, se obtienen los siguientes mensajes de respuesta: *RequestedEvents, DigitMap, SignalRequests, RequestIdentifier, NotifiedEntity, ConnectionIdentifiers, DetectEvents, ObservedEvents, EventStates, Restart-Reason, RestartDelay, ReasonCode, and Capabilities.*

Existen otros comandos de interés. Por ejemplo, *RestartInProgress* es usado por el GW para notificar que un grupo de conexiones se encuentran en falla o reinicio. El *EndpointConfiguration* es usado para indicar al GW las características de codificación esperadas en el extremo final.

CAPITULO IV

CENTRALES TELEFÓNICAS DE ÚLTIMA GENERACIÓN

4.1.- Arquitectura de comunicaciones de Avaya – Descripción general

La arquitectura de comunicaciones de Avaya es un marco que permite la evolución hacia las comunicaciones inteligentes. Este marco soporta funcionalidades de acceso multimodal (voz, video y datos) a una infraestructura que proporciona una variedad completa de comunicaciones. La arquitectura de comunicaciones de Avaya se fundamenta en el concepto dual de aplicaciones de comunicaciones y servicios de comunicación. Las aplicaciones de comunicaciones de Avaya se pueden integrar en las operaciones y procesos de la empresa. Los servicios de comunicación de Avaya proporcionan una mayor granularidad, semejante a la de un bloque funcional de aplicaciones que se puede acoplar a las aplicaciones empresariales y a los flujos de procesos. Cuando se combinan, cumplen la promesa de las comunicaciones inteligentes.

Al adoptar esta estructura e implementar sus recursos de comunicación de maneras creativas, los planificadores empresariales pueden lograr una infraestructura de red y aplicaciones con la suficiente flexibilidad para adaptarse a los cambios que su negocio requiera. Al mismo tiempo, sacarán el máximo provecho a sus recursos existentes de comunicaciones e información. En opinión de Avaya, la arquitectura de comunicaciones, que se muestra en la siguiente figura y que es la usada por Avaya, constituye la base para la integración de las comunicaciones en la empresa con acceso, aplicaciones y servicios multimedia unificados.

La estructura en la siguiente ilustración separa los recursos de comunicación de la empresa en capas de comunicaciones y del negocio. Estas capas se muestran horizontalmente y también como dos elementos verticales: desarrollo y gestión de aplicaciones. La capacidad de servicio es el respaldo tras la tecnología y las aplicaciones de hoy en día, pues mantiene y garantiza las comunicaciones.

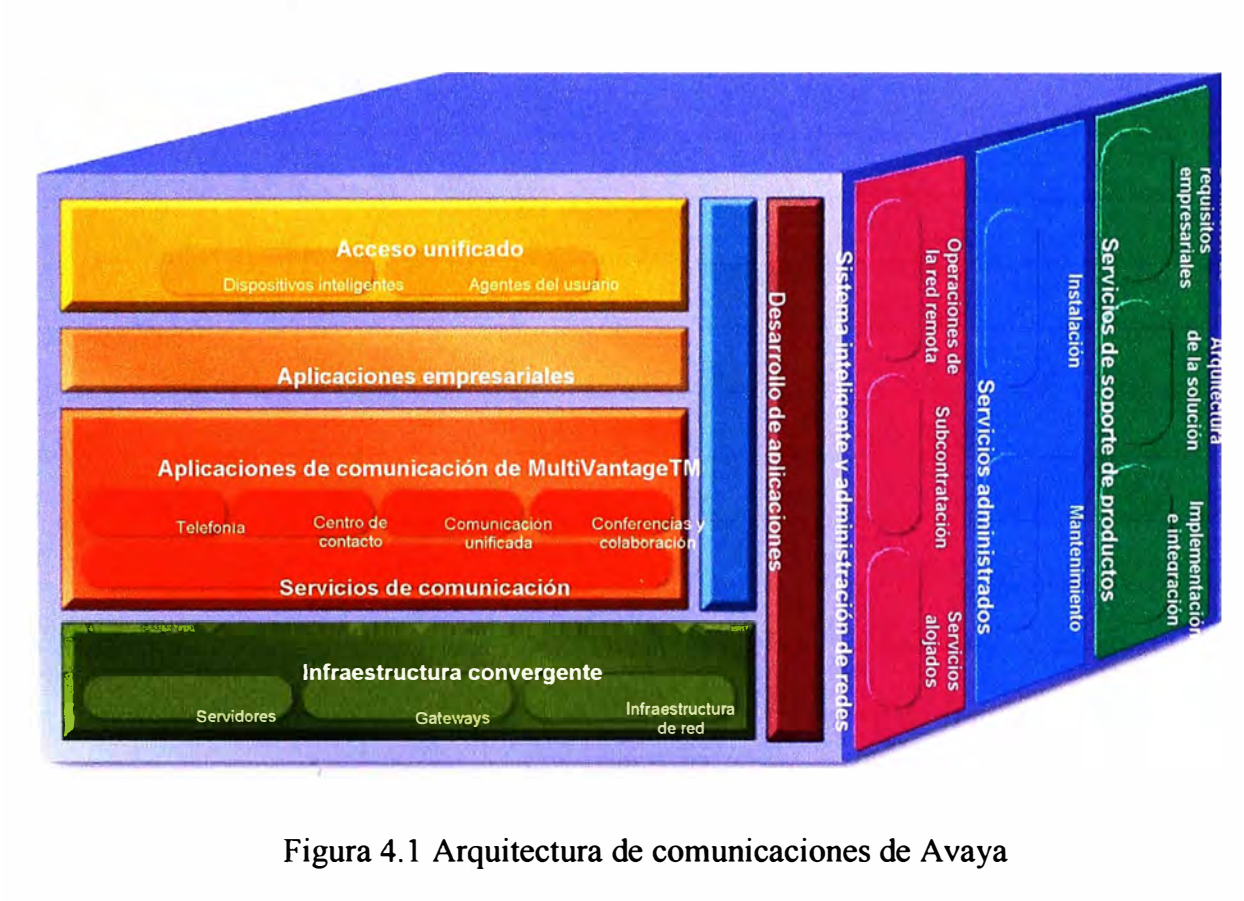


Figura 4.1 Arquitectura de comunicaciones de Avaya

La estructura tiene tres capas principales: acceso unificado, aplicaciones e infraestructura convergente. Las aplicaciones de negocios y las de comunicación se encuentran dentro de la capa de aplicaciones. Los servicios de comunicación enlazan las comunicaciones con los procesos de la empresa a través de la infraestructura de software de IT convergente para integrar las comunicaciones en las aplicaciones de empresariales y la infraestructura convergente subyacente, proporcionando capacidades de comunicación. La estructura es abierta, usa los estándares de la industria cuando es posible y como tal, permite que los productos y soluciones de Avaya se puedan integrar fácilmente en un entorno de distintos vendedores. El elemento de desarrollo de aplicaciones establece un entorno en el que los integradores de sistemas y los desarrolladores pueden crear nuevas aplicaciones de

negocios y flujos de procesos empresariales habilitados por comunicaciones a través de kits de desarrollo de software de servicios de comunicaciones. El elemento de administración del sistema y de la red permite controlar de manera unificada todas las capas.

4.1.1.- Avaya Communication Manager, versión 3.1

El Avaya Communication Manager es el facilitador de las comunicaciones inteligentes y forma parte de la siguiente generación de software de procesamiento de llamadas de Avaya. Designado como una solución de telefonía abierta, escalable y altamente confiable, el Communication Manager se puede ampliar de menos de 100 usuarios hasta un máximo de 36,000 en un solo sistema y a más de un millón de usuarios en una sola red. El Communication Manager es la base para la creación de redes completas de comunicaciones empresariales, ya que puede soportar los protocolos: sistema de comunicaciones distribuidas (DCS) y Q-Signaling (QSIG) sobre redes TDM, ATM o IP y proveer servicios de correo de voz centralizados, operaciones por medio de operadora y capacidades de gestión de relaciones con el cliente, en varios sitios.

El Communication Manager ofrece todos los beneficios del IP, ya que la confiabilidad y la funcionalidad de la convergencia no se ven afectadas. Este sistema ha sido diseñado para ejecutarse en una variedad de servidores de medios, pero el control de las llamadas se realiza desde un sitio centralizado formando una red flexible y distribuida de gateways de medios y una amplia gama de dispositivos de comunicación analógicos, digitales y basados en IP. Considerado el software de telefonía central de las aplicaciones de comunicaciones MultiVantage™ de Avaya, brinda la flexibilidad necesaria para introducir soluciones de telefonía IP avanzadas, según se requiera, sin desaprovechar las inversiones en infraestructura ya realizadas.

Las funcionalidades del Communication Manager de Avaya operan sobre IP. El software se puede administrar usando las herramientas del servidor para la administración de sistemas, lo cual resulta más sencillo para las empresas que tienen múltiples ubicaciones, pues pueden aprovechar las capacidades del Communication Manager como el

enrutamiento de llamadas, contabilización de los costos, autodiagnósticos, seguridad, protección contra llamadas de larga distancia no autorizadas y aplicaciones de acceso remoto.

El Communication Manager es capaz de centralizar el procesamiento y la administración de llamadas en poderosos servidores, y al mismo tiempo, extender la gran variedad de aplicaciones hacia los gateways con funciones de supervivencia que se encuentran en otras ubicaciones. Entre los beneficios de que pueden gozar las universidades y las oficinas con múltiples sucursales podemos mencionar la habilidad para crear redes de comunicaciones flexibles que se pueden administrar de manera centralizada.

Aplicaciones como IP Softphone e IP Agent se usan para crear un centro de llamadas distribuido y poner a disposición de todos los usuarios la gran capacidad del Communication Manager, sin importar si se encuentran en la oficina o trabajando en otro sitio. A través de la conmutación distribuida y las capacidades de procesamiento de llamadas del Communication Manager en todos los niveles de la red se puede ejecutar la conmutación. El Communication Manager soporta estándares abiertos como el H.323 Call Control, SIP y H.248 Media Gateway Control.

4.1.2.- S8720 Media Server de Avaya (PBX)

Diseñado para cubrir las necesidades de los entornos más exigentes del cliente, el S8720 Media Server, junto con el Communication Manager, versión 3.1 de Avaya, cuentan con la opción de duplicación de software, un procesador más poderoso y mayor espacio de almacenamiento, aunque se ha conservado el diseño vertical de 2 unidades de las plataformas de la serie S8700. El resultado es un S8720 Media Server con duplicación de hardware cuyo procesamiento de BHCC (terminación de llamada durante las horas de más tráfico) es un 50% más eficiente que el del S8710 Media Server con una configuración similar. Este servidor también soporta la funcionalidad de *duplicación de software*, cuenta con mayor capacidad de almacenamiento y con una interfaz USB 2.0 adicional. El S8720 se basa en un poderoso procesador AMD Opteron y se ejecuta en el sistema operativo Red Hat Enterprise Linux 4.0.

El S8720 Media Server, refleja nuestra principal estrategia de servidores de medios, la cual promete una relación precio/ rendimiento similar a la arquitectura de comunicaciones de Avaya, mediante actualizaciones regulares de nuestras plataformas de servidores de medios para aprovechar las nuevas tecnologías y las mejoras en el terreno del rendimiento. Al igual que otros servidores de esta serie, el S8720 Media Server siempre se entrega con dos procesadores para garantizar un nivel de fiabilidad máximo.

El S8720 Media Server está disponible en dos configuraciones: con duplicación de hardware (se requieren dos tarjetas de duplicación DAL1) o con duplicación de software (no se requieren tarjetas DAL1). Con la duplicación de hardware, los S8720 Media Servers se pueden colocar a una distancia máxima de 10 kilómetros (6.3 millas) uno del otro para asegurar la continuidad de las operaciones. Si se usa la duplicación de software se requiere un enlace completo de un Gigabyte. La distancia de separación respecto al servidor la determina la calidad del enlace de duplicación.

El S8720 Media Server, con la duplicación de hardware, puede procesar hasta 600,000 terminaciones de llamadas durante las horas de mayor tráfico (BHCC), manejando distintos tipos de llamadas. El índice de BHCC para el S8720 con duplicación de software es de aproximadamente 250,000 con distintos tipos de llamadas. Además, el S8720 puede soportar 36,000 estaciones y 44,000 puertos; hasta 12,000 terminales IP (que es la suma total de enlaces troncales IP, estaciones IP y enlaces troncales SIP) y 8,000 enlaces troncales, lo que le permite brindar soporte a las operaciones de grandes compañías multinacionales y centros de contacto.

4.1.3.- Servidores duplicados

Los S8720 Media Servers se instalan en pares, en configuraciones de par a par. Uno de ellos se ejecuta en el modo activo y el otro en el modo de reserva. El S8720 Media Server en modo activo tiene un elemento de procesamiento de conmutación (SPE) que controla activamente y da servicio a todas las entidades del sistema (redes de puertos, gateways, dispositivos adjuntos, teléfonos IP, etc.). Además, constantemente se monitorea a sí mismo para determinar su condición. El S8720 Media Server que se ejecuta en modo de reserva,

también ejecuta el SPE, pero no controla ninguna entidad. Se encarga de monitorear la condición del servidor y está listo para hacerse cargo del sistema (tomar el lugar del servidor activo) cuando es necesario.

En versiones anteriores del Communication Manager de Avaya, los Media Servers serie S8700 sólo estaban disponibles con duplicación de hardware. Con este tipo de duplicación, la tarjeta de duplicación DAL1 procesa los datos de la memoria volátil (conversiones) del servidor de medios activos y los transmite a la tarjeta de duplicación DAL1 del servidor de reserva sobre el cable de fibra óptica. Los datos de la memoria no volátil se pueden transmitir sobre un enlace Ethernet dedicado o no dedicado.

La solidez fundamental de la arquitectura del S8720 Media Server de Avaya reside en el hecho de que *todo el complejo del servidor está duplicado*. Al usar servidores duplicados, uno activo y otro de reserva, se eliminan todos los puntos de falla. Uno de los principales diferenciadores de Avaya en el mercado es el uso de un servidor de reserva activo.

El S8720 consiste en un par de servidores que usan los poderosos procesadores AMD Opteron y ejecutan el sistema operativo Red Hat Enterprise Linux, versión 4. Además, debido a que ejecuta el Communication Manager de Avaya, soporta la mayoría de las interfaces de programación de aplicaciones de estándar industrial y protocolos como TAPI, TSAPI, JTAPI, DAPI, ASAI, LDAP, H.323, QSIG, H.450 y H.248.

Con el S8720 Media Server de Avaya el control de llamadas y el tráfico de portadora se manejan por separado. Para el control de llamadas se utilizan redes Ethernet, mientras que el tráfico de portadora entre armarios puede viajar sobre un medio separado (red IP, fibra óptica, ATM o DS-1). El servidor de medios controla la matriz de conmutación mediante una red Ethernet privada. La red de control puede estar dedicada (sobre una red privada) o no dedicada (sobre la red corporativa de la empresa).

La red de portadora de voz está disponible en varias configuraciones:

Portadora de voz sobre IP (conexión IP): Configuración totalmente IP.

Portadora de voz sobre ATM (modo asíncrono de transferencia) o Center Stage Switch (CSS) (conexiones múltiples): En esta configuración los trayectos de portadora y de control están separados. La información de control para las redes de puertos viaja sobre una red de control dedicada, a través de la Ethernet, conmutador (LAN privada) o una red de control no dedicada (sobre la LAN del cliente) y termina en el S8700 Series Media Server, en uno de los extremos, y en una tarjeta de circuito impreso de interfaz del servidor IP (IPSI) en el otro.

Adicionalmente, el Communication Manager permite configuraciones de redes de puertos mixtas en las que las redes de puertos (PN) con conexión de IP se pueden introducir en un Center Stage Switch (CSS) existente, ATM-PNC, y también permite configuraciones de redes de puertos conectadas directamente. Una configuración puede contener una combinación de los siguientes métodos de conectividad de redes de puertos (PNC):

Conexión IP y directa.

Conexión IP y Center Stage Switch (CSS).

Conexión IP y ATM-PNC.

Figura 4.2. S8720 Media Server de Avaya

4.1.4.- Equipo de Supervivencia S8500

Dentro de la versión de Avaya Communication Manager, ofrece soluciones para mejorar la capacidad de supervivencia de grandes localidades de la manera más efectiva. Trabajando junto con el Communication Manager, el Servidor de Medios S8500 de Avaya ahora puede actuar con un procesador local con capacidad de supervivencia, asegurando que las localidades de negocios de hasta 2,400 personas tengan comunicaciones IP continuas en caso de interrupciones o fallas de red. Esto es un incremento sobre el soporte anterior que cubría a 450 personas. Otra nueva capacidad, la Duplicación de Recursos de Medios IP, incrementa la capacidad de supervivencia al asegurar que las llamadas de telefonía IP permanezcan trabajando con completa funcionalidad (por ejemplo, transferencia, llamada conferencia) durante caídas de red o hardware. Los beneficios añadidos de supervivencia incluyen la capacidad única para centros de contacto para que, durante caídas de red, se continúe recolectando información de clientes y que se pueda reconsolidar después de la recuperación para ayudar a asegurar que los reportes de clientes sean veraces.

Las capacidades de SIP y SOA de Avaya aprovechan el potencial completo de las comunicaciones abiertas. El Servidor de Comunicaciones Convergentes de Avaya incluye los Servicios de Habilitación de SIP de Avaya que permiten que las empresas integren funcionalidad abierta y presencial de SIP para comunicaciones en tiempo real. El Servidor de Comunicaciones Convergentes también incluye los Servicios de Habilitación de Aplicaciones de Avaya, las cuales integran interfases de programación de aplicación (APIs, por sus siglas en inglés) y servicios de Web del Communication Manager para ayudar a los desarrolladores a diseñar nuevas aplicaciones para Service Oriented Architecture o arquitectura orientada al servicio (SOA, por sus siglas en inglés).

Los Servicios de Habilitación de Aplicaciones de Avaya incrementan la seguridad y capacidad de supervivencia para dar a los desarrolladores de aplicaciones un ambiente más confiable y con mayor capacidad de supervivencia para desarrollar aplicaciones de servicios de Web. Las mejoras incluyen una seguridad ampliada para aplicaciones y encripción mejorada, así como un incremento en la flexibilidad del vínculo de transporte para que las aplicaciones puedan preservarse y mantenerse ininterrumpidas durante caídas de red de hasta 30 segundos.

4.1.5.- Tarjeta de circuito impreso de la interfaz de servidor IP (IPSI) (TN2312BP)

El Media Server serie S8700 controla los gateways de medios usando trayectos separados de portadora y de control. La señalización de control de llamadas se establece desde el Media Server serie S8700 sobre una conexión Ethernet a una interfaz de servidor IP TN2312 (IPSI) en el gateway de medios.

La IPSI tiene las siguientes características:

Siempre reside en la ranura de tono / reloj.

Incluye una interfaz 10/100BaseT para conectarse al servidor.

Incluye un jack RJ45 en la placa frontal 10/100BaseT para conectar una computadora portátil de servicios.

Realiza la generación y sincronización de reloj con el gateway de medios.

Genera los tonos del gateway de medios.

Clasifica las llamadas globales.

Incluye una interfaz de paquetes del gateway de medios.

Soporta la descarga del firmware de IPSI.

Gateway de medios.

Realiza la interfaz con la tarjeta de mantenimiento TN775D del gateway de medios. La interfaz de servidor IP (IPSI) TN2312BP realiza el mantenimiento del entorno y es la interfaz del servidor IP soportada en el G650. La IPSI TN2312BP es compatible con versiones anteriores de gateways de medios, pero realiza el mantenimiento del entorno sólo cuando se usa en un G650. La IPSI TN2312BP siempre realiza las funciones de detección de tonos, clasificación de llamadas, generación de tonos y de reloj. Cuando la IPSI TN2312BP se usa en el MCC1 o SCC1 de Avaya, un TN755D realiza el mantenimiento del entorno.

La IPSI TN2312BP cuenta con funciones de mantenimiento para el G650. Entre ellas se incluyen:

Mantenimiento del suministro de alimentación, armario y generador de señal de llamada.

Detección de alarmas de dispositivos externos.

Control de transferencia en caso de emergencia.

Control de dispositivos de alarmas.

En las configuraciones en las que la portadora de voz está sobre CSS o ATM, por lo general cada IPSI controla cinco redes de puertos mediante la tunelización de los mensajes de control sobre la red de portadora a las PN que no tienen IPSI; para las configuraciones en las que la portadora de voz opera sobre IP, debe haber una IPSI en cada PN. Una configuración de conexión directa sólo soporta una PN con conexión de IPSI.

4.1.6.- Media Gateways de Avaya

Los Media Gateways de Avaya son elementos de hardware apilables y modulares que ofrecen aplicaciones con capacidades de voz, datos, fax, video y mensajería para su red. Los Media Gateways de Avaya soportan tráfico de portadora y de señalización que se enruta entre las redes de conmutación de paquetes y de circuitos. Estas gateways han sido optimizadas para la telefonía de clase empresarial.

Los Media Gateways de Avaya ofrecen una variedad de opciones de implementación flexibles, incluyendo los ambientes 100% IP y los ambientes mixtos como IP y TDM.

Cuando se monta en un armazón, el G650 está limitado a un máximo de cinco (5) gateways en una sola red de puertos. Si una red de puertos G650 contiene más de una (1) portadora, cada portadora dentro de la red de puertos debe estar alineada verticalmente con todas las demás portadoras en dicha red, de tal forma que los paneles frontales de todas las portadoras queden en el mismo plano vertical.

Los Media Gateways de Avaya tienen las siguientes funcionalidades y beneficios:

- Pueden interoperar con redes de datos basadas en los estándares.
- Son soluciones con componentes apilables, modulares y configurables.
- Ofrecen capacidades redundantes.
- Operan en redes distribuidas.
- Son compatibles con los armarios de los sistemas tradicionales de Avaya.

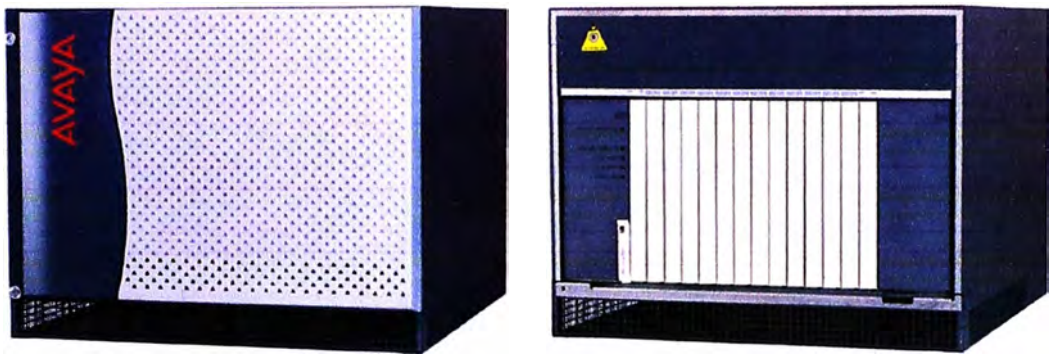


Figura 4.3. G650 Media Gateway de Avaya

4.2.- Softswitch

Softswitch: El un dispositivo quc provcc Control dc llamada y scrvicios intcligcntcs para redes de conmutación de paquetes. Un Softswitch sirve como plataforma de integración para aplicaciones e intercambio de servicios. Son capaces de transportar tráfico de voz, datos y vídeo de una manera más eficientes que los equipos existentes, habilita al proveedor de servicio para soporte de nuevas aplicaciones multimedia integrando las existentes con las redes inalámbricas avanzadas para servicios de voz y Datos.

La interconexión de las redes de circuitos y las redes conmutadas está provocando la evolución de los centros de conmutación actuales mediante la tecnología de softswitch, la cual se basa en una combinación de software y hardware que se encarga de enlazar las redes de paquetes (ATM o IP) y las redes tradicionales, las cuales desempeñan funciones de control de llamadas tales como conversión de protocolos, autorización, contabilidad y

administración de operaciones. Esto significa que los softswitches buscan imitar las funciones de una red de conmutación de circuitos para conectar abonados (clase 5), interconectar múltiples centrales telefónicas (clase 4 o tandem) y ofrecer servicios de larga distancia (clase 3), de la misma manera como lo hacen las centrales telefónicas actuales. Además, según los fabricantes –como Nortel, Lucent, Cisco y HP– el uso de esta tecnología ayudará a los operadores a suministrar servicios nuevos y tradicionales a menor costo.

Softswitch es la pieza central en la red de telefonía IP , puede manejar inteligentemente las llamadas en la plataforma de servicio de los ISP. Softswitch Es un conjunto de productos, protocolos y aplicaciones capaz de permitir que cualquier dispositivo accese los servicios.

Además los conmutadores por software permiten ofrecer servicios de voz avanzados así como nuevas aplicaciones multimedia, las cuales se caracteriza por:

Su inteligencia, la cual les permite controlar los servicios de conexión asociados a las pasarelas multimedia (Media Gateways) y los puntos terminales que utilizan IP como protocolo nativo. La posibilidad de seleccionar los procesos. Los cuales se pueden aplicar a cada llamada.

El enrutamiento de las llamadas en función de la señalización y de la información almacenada en la base de datos de los clientes.

La capacidad para transferir el control de una llamada a otro elemento de red.

Interfaces con funciones de gestión como los sistemas de facturación y provisión.

Puede existir con las redes tradicionales de redes conmutadas así como puede proveer los servicios de la tecnología de conmutación de paquetes; los servicios que pueden soportar incluye Voz, Fax, vídeo, datos y nuevos servicios que serán ofrecidos en el futuro , los dispositivos finales incluyen teléfonos tradicionales, teléfonos IP, computadores, beepers, terminales de videos conferencia y más.

4.2.1.- Beneficios de Softswitch.

Los beneficios que Softswitch ofrece son:

Bajo Costo de desarrollo.

Fácil integración de redes diversas .

Mejora los servicios para el cliente lo cual reduce el tiempo para mercadear.

Mensajes unificados.

Flexibilidad al soportar el desarrollo de equipos de telefonía de gran nivel.

Mejores ingresos para los proveedores de servicios y operadores.

Esta tecnología permite una transición pacífica de circuitos a paquetes, con servicios diferenciados e interoperabilidad a través de redes heterogéneas.

4.2.2.- Arquitectura de Servicios del softswitch

Un softswitch puede consistir en uno o más componentes, sus funciones pueden residir en un sistema o expandirse a través de varios sistemas. A continuación se mencionan los componentes mas comunes en un softswitch.

a).- Gateway Controller : Es la unidad funcional del softswitch. Mantiene las normas para el procesamiento de llamadas, por medio del Media gateway y el Signalling Gateway los cuales ayudan a mejorar su operatividad. El responsable para ejecutar el establecimiento y desconexión de la llamada es Signalling Gateway.

Frecuentemente esta unidad es referida como Call Agent o Media Gateway Controller. Algunas veces el Call Agent es referido como el centro operativo del Softswitch. Este componente se comunica con las otras partes del Softswitch y componentes externos usando diferentes protocolos.

b) Signalling Gateway : Sirve como puente entre la red de señalización SS7 y los nodos manejados por el Softswitch en la red IP.

c).- Media Gateway: Actualmente soporta TDM para transporte de paquetes de voz al switch TELCO. Las aplicaciones de Codificación de voz, Decodificación y compresión son soportadas, así como las interfaces PSTN y los protocolos CAS y ISDN. Se lleva a cabo investigaciones para el en el para el soporte en el futuro de los paquetes de vídeo.

d).- Media Server: Mejora las características funcionales del Softswitch si es requerido soporta Digital Signal Processing (DSP) así como las funcionalidad de IVR.

e).- Feature Server: Controla los datos para la generación de la facturación, usa los recursos y los servicios localizados en los componentes del softswitch.

Un Gateway Controller combinado con el Media Gateway y el Signalling Gateway representan la mínima configuración de un Softswitch. El elemento controlador es frecuentemente conocido como Media Gateway Controller MGC.

4.2.3.- Requerimientos Funcionales del Gateway Controller.

El Gateway Controller debe soportar las siguientes funciones:

Control de llamada

Protocolos de establecimiento de llamadas: H.323, SIP

Protocolos de Control de Media: MGCP, MEGACO H.248

Control sobre la Calidad y Clase de Servicio.

Protocolo de Control SS7: SIGTRAN (SS7 sobre IP).

Procesamiento SS7 cuando usa SigTran.

El enrutamiento incluye:

Componentes de enrutamiento: Plan de marcado local.

Translación digital soportado para IP,FR,ATM y otras redes.

Detalle de las llamadas para facturación.

Control de manejo del Ancho de Banda.

Provee para el Media Gateways:

Asignación y tiempo de configuración de los recursos DSP.

Asignación de Canal DS0.

Transmisión de Voz (Codificación, Compresión y paquetización).

Provee para el Signaling Gateways:

Cronometro de procesos

Variantes SS7

Registro de Gatekeeper.

Las Características del Sistema que tienen que tenerse en consideración son:

CPU de altas capacidades con multiprocesador.

Disco de Almacenamiento usado como bitácora

Requiere soportar una amplia variedad de protocolos.

Capacidad de redundancia para la conectividad a la red.

4.2.4.- Signaling Gateway

Crea un puente entre la red SS7 y la red IP bajo el control del Gateway Controller. El Signaling Gateway hace aparecer al Softswitch como un nodo en la red SS7. El Signaling Gateway únicamente maneja señalización SS7, Media Gateway maneja los circuitos de voz establecidos por el mecanismo de señalización.

El Protocolo SIGTRAN es definido como un grupo de protocolos y capas de adaptación para transportar la información de señalización sobre las redes IP. SigTran es usado como protocolo entre el Gateway Controller y el Signaling Controller entonces MTP1, MTP2 y SigTran residen en el Signaling Gateway. En este caso MTP3 y los protocolos de alto nivel residen en el Gateway Controller.

El Signaling Gateway soporta las siguientes capas:

SCTP, la cual es responsable de la confiabilidad de la señalización de transporte, evitar la congestión y proporciona control.

M3UA, la cual soporta el transporte de ISUP, SCCP y los mensajes TUP sobre IP.

M2UA, la cual soporta la congestión y el transporte de los mensajes MTP3.

IUA, soporta las interfaces Q.931/Q.921

M2Peer, soporta las interfaces MTP3 a MTP2.

Un Signaling Gateway establece el protocolo, tiempo y requerimiento de las redes SS7, también como las equivalentes funcionalidades de la red IP.

a).-Requerimientos Funcionales de Signaling Gateway

Debe soportar las siguientes funciones:

Proveer conectividad física para la red SS7 vía T1/E1 o T1/V.35.

Capaz de Transportar información SS7 entre el Gateway Controller y el Signaling Gateway vía red IP.

Proveer una ruta de transmisión para la voz y opcionalmente para la data.

Proveer alta disponibilidad de operación para servicios de telecomunicaciones.

Las Características del Sistema que tienen que tenerse en consideración son:

Memoria disponible para mantener la información, configuración y rutas alternativas.

Disco de almacenamiento para llevar una Bitácora.

La Interface Ethernet puede requerir redundancia.

El rendimiento y la flexibilidad pueden ser incrementados usando H.110 o H.100 bus.

Alta disponibilidad.

4.2.5.- Media Gateway

El media gateway proporciona el transporte de voz, datos , fax y vídeo entre la Red IP y la red PSTN. En este tipo de arquitectura de red la carga útil se transporta sobre un canal llamado DS0, El componente mas básico que posee el media gateway es el DSP (digital signal processors). Típicamente el DSP se encarga de las funciones de conversión de analógico a digital, los códigos de compresión de audio/video, cancelación del eco, detección del silencio, la señal de salida de DTMF, y su función más importante es la translación de la voz en paquetes para poder ser comprendidos por la red IP.

a).- Requerimientos funcionales del Media Gateway

Un Media Gateway debe soportar lo siguiente:

Transmisión de los paquetes de voz usando RTP como protocolo de transmisión.

Los recursos del DSP y las ranuras de tiempo del T1 son controladas por el Gateway controller.

Soporte para cada uno de estos protocolos loop-strap, ground-star, E&M, CAS, QSIG y ISDN sobre un T1.

Habilidad para escalar en puertos, tarjetas, nodos externos y otros componentes del softswitch.

Las Características del Sistema que tienen que tenerse en consideración son:

Posee un entrada y salida de datos alta la cual puede aumentar a medida que la red aumente su tamaño, por lo tanto debe posee la característica de ser escalable.

Tiene una Interface Ethernet y algunos poseen redundancia.

Posee un Interface para redes TDM y algunos necesitan interfaces T1/E1

Un bus H.110 puede ofrecer mas flexibilidad al sistema

Densidad de 120 puertos (DS0s) es normal, típicamente estas interfaces se incorporan en una tarjeta DSPs.

4.2.6.- Media Server

Un media server usualmente se clasifica de manera separada del Feature Server porque contiene las aplicaciones de procesamiento del medio, esto significa que el media server soporta un alto funcionamiento del hardware del DSP.

Un media server no es estrictamente requerido como parte de las funciones del switch. En el contexto ASP este se puede incorporar en la tecnología de switch y proporciona la oportunidad de integrar la voz y los datos en la solución. También es usado para explotar las capacidades del Standard H.110.

a).- Requerimientos funcionales del Media Server

Funcionalidad básica de voicemail, integran fax y mail box, notificando por e-mail o pregrabación de los mensajes. Capacidad de videoconferencia, utilizando como medio de transmisión H323 o SIP. Speech-to-text , el cual se basa en el envío de texto a las cuentas de e-mail de las personas o a los beeper usando entradas de voz. Speech-to-Web, es una aplicación que transforma palabras claves en códigos de texto los cuales pueden ser usados en el acceso a la Web.

Unificación de los mensaje de lectura para voice, fax y e-mail por una interfase Ethernet.

Fax-over-IP usando el protocolo Standard T.38. IVR/VRU es un dispositivo que tiene como interfase hacia el usuario un script de voz, y recibe comandos a través de tonos DTMF.

4.2.7.- Feature Server

Se define como una aplicación al nivel de servidor que hospeda un conjunto de servicios. Estos servicios de valor agregado pueden ser parte de CALL AGENT o pueden ser desarrollados separadamente. Las aplicaciones se comunican con el CALL AGENT a través de los protocolos SIP, H.323 y otros, estas aplicaciones son usualmente hardware independiente pero requieren un acceso ilimitado a las base de datos.

Las Características del Sistema que tienen que tenerse en consideración son:

- Requiere de un CPU de Moderada Capacidad.
- Amplia Memoria para evitar el retardo.
- Diversidad de Base de datos localizadas en el Feature Server.
- Interface Ethernet con redundancia dual.
- Adecuado disco de almacenamiento.

4.2.8.- Tipos de arquitecturas de Softswitch

En la construcción de un Softswitch las alternativas de implementación deben basarse en las consideraciones de la Arquitectura y los cinco componentes del Softswitch.

Los factores para considerar incluyen: Escalabilidad, Confiabilidad del Hardware, disponibilidad de requerimientos, requerimientos de funcionamiento, Habilidad para lograr la interconexión con múltiples protocolos y el retorno de la Inversión.

GATEWAY CONTROLLER	MEDIA GATEWAY	SIGNALING GATEWAY	MEDIA SERVER	FEATURE SERVER
Capacidades de procesamiento elevadas, escalabilidad y soporte de un amplio rango de protocolos.	Tiempo real de respuesta y disponibilidad remota.	Escalabilidad IP,T1/E1, SS7.Acceso remoto	Alto tráfico IP, tiempo real de respuesta, alta disponibilidad, escalable según demanda.	Capacidad alta de procesamiento, mayormente de tráfico IP
SOLARIS OS	SOLARIS OS	SOLARIS OS	SOLARIS OS	SOLARIS OS
PLATAFORMA NETRA	PLATAFORMA NETRA	PLATAFORMA NETRA	PLATAFORMA NETRA	PLATAFORMA NETRA

Tabla 4.1. Requerimientos para los cinco componentes del SOFTSWITCH.

La mayoría de las compañías de Telecomunicaciones han seleccionado el Sistema Operativo SOLARIS como sistema operativo debido su confiabilidad, tiempo de respuesta menor a una décima de milisegundo, flexibilidad, Excelente soporte para el ambiente de red y seguridad.

C A P Í T U L O V

CONSIDERACIONES DE CALIDAD DE SERVICIO

5.1.- CALIDAD DE SERVICIO (QOS).

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final. En esto influyen dos factores fundamentales:

La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red. La demora extremo a extremo, debido a las sucesivos procesos de codificación, decodificación, paquetización y "encolados". Afecta la interactividad en la conversación y por tanto a la QoS.

Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, jitter y pérdida de paquetes. La preparación de los medios en los terminales para ser enviados y transferidos por la red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica demora de procesamiento y demora de empaquetado:

• Demora de procesamiento: demora producida por la ejecución del algoritmo de codificación, que entrega un stream de bytes listos para ser empaquetados.

• Demora de paquetización: es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados. Debe señalarse que el resultado de esta codificación –

paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa el retardo y la distorsión de la señales de voz.

Lo contrario ocurre al aumentar la velocidad de codificación. Otro aspecto a considerar es el compromiso entre el retardo de paquetización y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de paquetización para cierto estándar de codificación. Claro está, según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50 %, con un crecimiento de la demora en forma exponencial en el caso de los codecs de baja velocidad como el G.723.1. La demora de paquetización también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP.

A las demoras de procesamiento y empaquetado se suma también la demora que introduce el proceso de buffering en los terminales, y la demora de "encolado" en la red. Todo esto da una demora extremo a extremo que percibe el usuario final en mayor o menor medida. A continuación se resumen los aspectos que afectan la QoS en las redes de VoIP.

5.1.1.-Retardo.

Se refiere sobre todo al tiempo de tránsito total, incluido el tiempo necesario para reconstituir el orden de los paquetes cuando se reciben y para compensar las fluctuaciones de los tiempos de tránsito (este tiempo de tránsito total debe ser inferior a 400 ms si se han de respetar las limitaciones de la conversación interactivo). Los excesivos retardos punto a punto hacen conversaciones difíciles y poco naturales. Cada componente en el camino de transmisión – emisor, red y receptor añaden retardo. ITU-TG.114 (tiempo de transmisión en un solo sentido) recomienda 150 mseg. como el máximo retardo deseado en un sentido para lograr alta calidad de la voz.

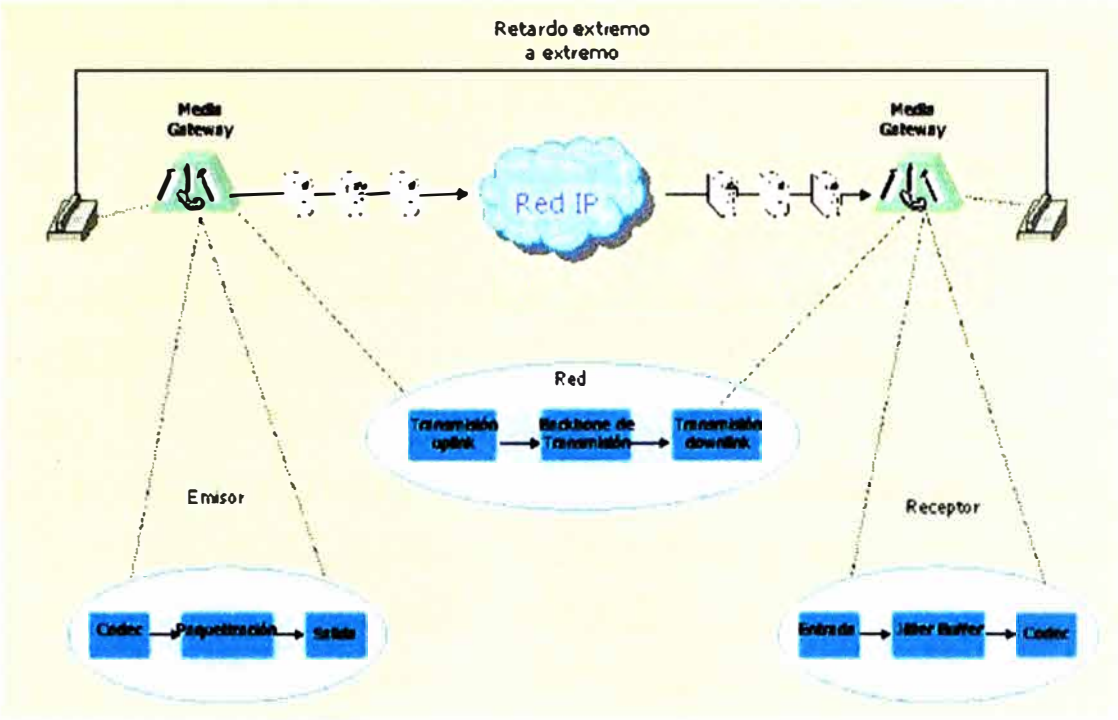


Figura 5.1 Retardo extremo a extremo

El retardo causa dos problemas: eco y traslape del habla. El eco es causado por las señales reflejadas por el equipo telefónico del extremo distante que regresan al oído del hablante. El eco llega a ser un problema significativo cuando el retardo del viaje redondo llega a ser mas de 50 milisegundos. A medida que el eco se incremente, los sistemas de paquetes se ven en la necesidad de utilizar controles como la cancelación de eco.

El traslape del habla (cuando dos personas hablan casi al mismo tiempo) es significativo si el retardo en una sola vía es mayor de 250 milisegundos. Por lo tanto el retardo completo llega a ser mayor. Algunas de las fuentes de retardo en una sola vía para una llamada hecha con paquetes de voz se describen a continuación

5.1.2.- Retardo Acumulado (Retardo algorítmico).

Es causado por la necesidad de recolectar un marco de muestras de voz para que sean procesados por el codificador de voz. Esto está relacionado con el tipo de codificador usado y varia de una sola muestra en el tiempo (.125 msg) a muchos milisegundos.

Codificadores de voz y sus tiempos:

G.726 modulación adaptativa diferencial de pulsos codificados (ADPCM), 16, 24, 32, 40 Kbps = 0.125 msg.

G.728 predicción lineal de excitación de código LD (CELP), 16 Kbps = 2.5 msg

G.729 CS-ACELP 8Kbps = 10 msg

G.723.1 codificador multitasa, 5.3, 6.3 Kbps = 30 msg.

5.1.3.-Retardo de Procesamiento.

Es causado por el procesamiento de codificación y recolección de las muestras codificadas en paquetes para la transmisión sobre una red de paquetes. El retardo de codificación es una función del tiempo de ejecución del procesador y el tipo de algoritmo usado. A menudo se recolectan múltiples marcos de codificación de voz en un solo paquete para reducir la cabecera del paquete. Por ejemplo, 3 marcos de palabras codificadas en G.729 (equivalente a 30 milisegundos de habla) se recolectan y empacan en un solo paquete.

5.1.4.- Retardo de red.

Es causado por el medio físico y los protocolos usados para transmitir los datos de voz y por los buffers usados para remover el jitter en el lado receptor. El retardo de red es una función de la capacidad de los enlaces en la red y del procesamiento que ocurre a medida que los paquetes transitan por esta. Los buffer para jitter agregan retardo, que es utilizado para remover la variación de retardo a la que están sujetos los paquetes a medida que transitan en una red de paquetes.

5.1.5.- Colas.

S e definen como las que manejan el trafico mediante la asignación de distintas cantidades de espacio en la cola a las diversas clases de paquetes y a continuación dan servicio a las colas en la modalidad de ordenamiento cíclico. Aunque se puede asignar un mayor espacio en la cola a un protocolo, usuario o aplicación particular, ninguno de ellos podrá monopolizar nunca toda la anchura de la banda.

5.1.6.- Eco.

El eco es el tiempo que transcurre entre la transmisión de una señal y su regreso al transmisor. Por lo general, este problema aparece en el contexto de las comunicaciones de PC a teléfono, de teléfono a PC o de teléfono a teléfono, y es causado por los componentes electrónicos de las partes analógicas del sistema que reflejan una parte de la señal procesada. Un eco menor que 50 milisegundos es imperceptible. Por encima de este valor, el hablante oirá su propia voz después de haber hablado. Si se desea ofrecer un servicio de telefonía IP, las pasarelas tendrán que procesar el eco generado por la transferencia de dos a cuatro hilos, de lo contrario, no será posible utilizar el servicio con equipos analógicos clásicos. Como solución, se están instalando compensadores de eco de alta calidad en la pasarela de la red. A medida que el eco se incremente, los sistemas de paquetes se ven en la necesidad de utilizar controles como la cancelación de eco.

a).- Compensación de Eco.

El eco en una red telefónica, es causado por las reflexiones de señales generadas por un circuito híbrido que convierte de 4 hilos (un par para transmisión y uno para recepción) a 2 hilos (un solo hilo para transmisión y uno para recepción). Estas reflexiones de la voz del hablante son escuchadas por el oyente. El eco se presenta aún en las redes de conmutación de circuitos, sin embarco acá es aceptable ya que los retardos completos a través de la red son menores que 50 msg. Y el eco es enmascarado por el tono lateral que todo teléfono genera.

Existen dos (2) tipos de eco. Uno tiene alto nivel y poco retardo y se produce en el circuito híbrido de 2 a 4 hilos local; mientras que otro es de bajo nivel y gran retardo y se produce en el circuito separador híbrido remoto.

El eco es problema en una red de paquetes de voz cuando el retardo completo en la red es mayor que 50 msg, entonces se deben aplicar técnicas de cancelación de eco.El estándar G.165 de la UIT define el desempeño de los canceladores de eco, en la recomendación G.IEC se encuentran mas características.

El cancelador de eco compara los datos de voz recibidos de la red de paquetes con los datos de voz que están siendo transmitidos por la red de paquetes. Se construye mediante la técnica de ecualización transversal autoadaptativa. Consiste en usar una parte de la señal de transmisión para cancelar el eco producido por la desadaptación de impedancias en el circuito híbrido que convierte de 4 a 2 hilos.El eco del híbrido de la red de paquetes se remueve con un filtro digital en el camino de transmisión hacia la red de paquetes.

5.1.7.-. JITTER.

Cuantifica el efecto del retardo total en la red ocasionado por los paquetes que llegan al receptor. Los paquetes transmitidos a intervalos iguales desde el gateway de la izquierda llegan al gateway de la derecha a intervalos irregulares. El excesivo jitter hace que la voz sea entrecortada y con dificultades para entenderse. El jitter es calculado basado, en las horas de llegada entre paquete y paquete de los paquetes exitosos. Para una alta calidad de voz, el promedio de las horas de llegada entre los paquetes en el receptor debería ser casi igual a la diferencia entre los paquetes en el transmisor y el estándar de desviación debería ser bajo. El jitter buffer (el buffer mantiene paquetes entrantes por una determinada cantidad de tiempo) es usado para neutralizar los efectos de las fluctuaciones de la red y crear un fácil flujo de paquetes en la recepción.

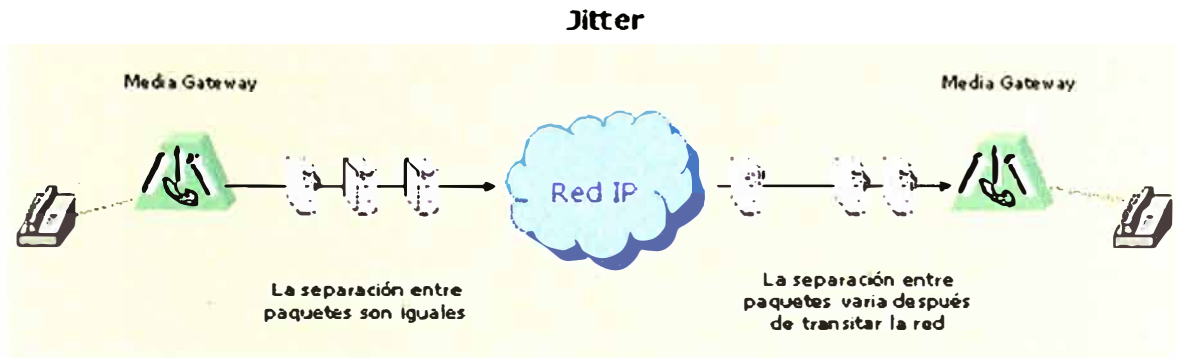


Figura 5.2 jitter sobre la red

Es también, la variación de tiempo entre los paquetes causada por la red. Remover el jitter requiere la recolección de paquetes y retención de estos el tiempo suficiente para que el paquete mas lento llegue a tiempo para ser interpretado en la secuencia correcta.

El conflicto que se produce al querer mezclar el retardo con la supresión del jitter, ha generado varios esquemas para adaptar el tamaño del buffer de jitter a los requerimientos de variaciones de tiempo de la red. Esta adaptación tiene la meta explícita de minimizar el tamaño y retardo del buffer de jitter mientras que al mismo tiempo previene el sobre flujo del buffer causado por el jitter. Se han hecho dos aproximaciones para adaptar el tamaño del buffer, la selección de la aproximación depende del tipo de red de paquetes usada.

La primera aproximación es medir la variación del nivel de paquetes en el buffer de jitter en un periodo de tiempo e incrementalmente adaptar el tamaño del buffer para que coincida con el jitter calculado. Esto funciona mejor con redes que tienen jitter constante en un periodo de tiempo, como las redes ATM

La segunda aproximación es contar el número de paquetes que llegan tarde y crear una relación de estos paquetes al numero de paquetes que son procesados exitosamente. Esta relación es usada para ajustar el buffer de jitter a una relación permisible de paquetes tardíos predeterminada. Esto funciona mejor con redes que tengan intervalos de arribo de paquetes altamente variable, como las redes IP.Además de estas técnicas, la red debe estar configurada y gestionada para que tenga retardos y jitter mínimos, permitiendo así un alto QoS.

C A P Í T U L O VI

APLICACIONES SOBRE CENTRALES TELEFONICAS

6.1.- Interconexión entre Centrales Telefónicas Remotas

Una de las aplicaciones mas importantes usadas en la red de datos son las aplicaciones de voz; es posible por el mismo medio el viaje tanto de paquetes de voz como de otras aplicaciones que los usuarios finales necesiten usar.

Analizaremos diferentes escenarios presentados para la interconexión entre distintas centrales telefónicas; propondremos soluciones para una empresa que tiene una centralita interna para recibir y establecer llamadas en forma local, además desea realizar llamadas a sus clientes para verificar su estado de facturación, y del mismo modo los usuarios finales necesitan comunicarse a la empresa solicitante para que le brinden información de sus estados de cuenta, etc; dentro de las necesidades esta el poder comunicarse con los anexos internos de la empresa a través de la llamada ingresante que realiza los usuarios externas de dicha empresa, además de la posibilidad de que un agente le brinde información sobre su facturación.

Por lo cual la empresa realiza hacerlo a través de una empresa Call Center que le brinde las facilidades requeridas de ingreso de llamadas que sean atendidas por agentes que pueden ser remotas que no se encuentren en su local de atención o agentes locales que se encuentran en el mismo edificio de la empresa; además que dicho call center le brinde el desarrollo de un IVR automático para que emita información en línea de montos

presentados por lo cual necesitan estar remotamente conectados a la base de datos de la empresa para brindar la información online.

Además se han hecho los cálculos respectivos para que la atención de llamadas que van ha realizar entre ambos locales es aproximadamente de 10 canales de voz los cuales al utilizar una compresión de voz de G729 lo realizaran usando un ancho de banda de 100Kbps.
Presentaremos diferentes soluciones e indicaremos las ventajas presentadas para los distintos casos como también los costos que toma implementar la solución presentada a la empresa

6.1.1- ESCENARIO 1 (OUT-HOUSE):

En esta primera solución el grupo de agentes que reciben las llamadas desde la PSTN se encontraran físicamente en el local del Call Center , ellos serán capaces de atender y recibir las llamadas a través de la central del Callcenter.

Como el enlace de voz y datos a utilizarse para la comunicación se aproxima que el enlace a usarse es un enlace MPLS de 512 kbps con calidad de Plata, se tendrá que utilizar para comunicación de datos y voz, de los cuales se usaran para la utilización de 10 Canales de Voz hacia la central de la empresa remota

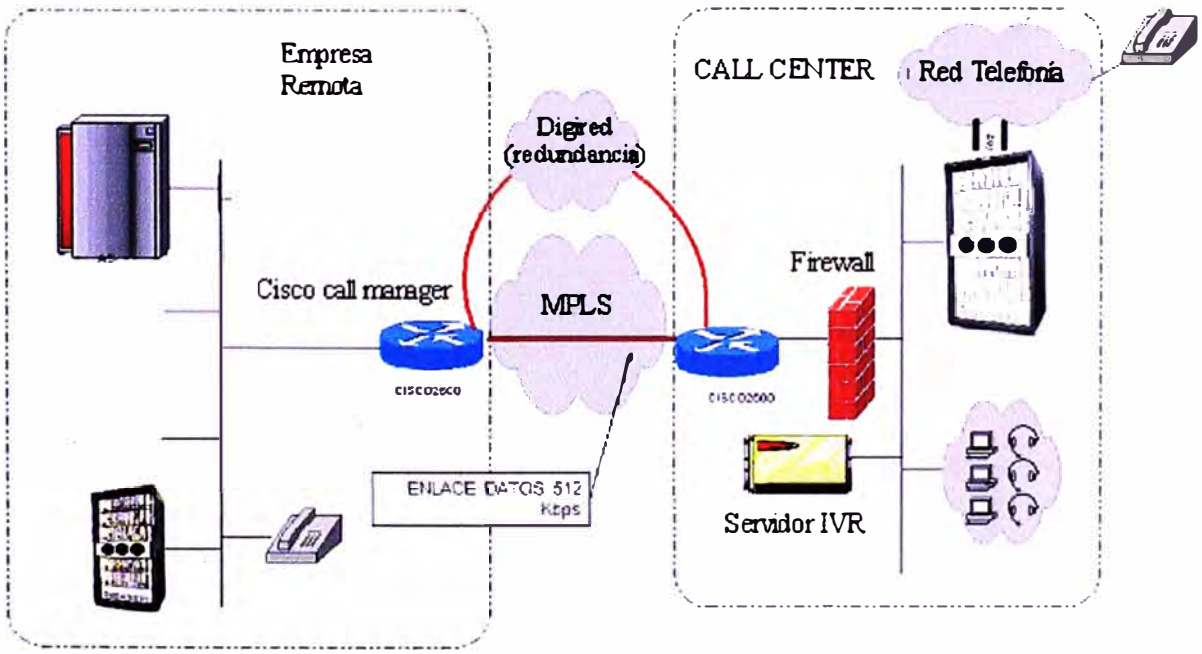


Figura 6.1 Solución out-house

a).- Descripción de la Solución:

- Como los agentes estarán en local del Callcenter ellos realizaran llamadas de salida a través de los enlaces de voz que tienen instalados en el Call center.
- La capacidad de uso de 10 canales de comunicación de Voz de la empresa remota se utilizara para la interconexión directa con los anexos de dicha empresa debido a que las llamadas dentro del menú de opciones pueden ser derivadas hacia los anexos de dicho local remoto para la atención especial, por lo cual se ha tenido que levantar una troncal H323 entre la Plataforma del Call center hacia el gateway de voz (Cisco Call Manager) que se tiene en el local remoto y poder atender las llamadas que se intercambiaran entre ambos locales, vemos pues que la conexión de datos nos permite levantar una troncal de voz para la atención respectiva.
- El ancho de banda para la comunicación de datos es de 512 kBps. Se utilizara dicho enlace para la comunicación tanto de los aplicativos como para poder brindar información on-line del IVR, además para pasar voz.
- El sistema redundante a implementarse en caso de contingencia es mediante una conexión DIGIRED de 128 Kbps o algún otro del proponente.
- Los sistemas de comunicación se configuraran de manera redundante y con balanceo de carga.
- Se aplican políticas de Calidad de Servicio QoS para discriminar el tráfico de voz a la de datos ya que por el mismo medio van ambos servicios realizando la priorización de los paquetes para que la calidad de voz no se vea degradada.

b).- Ventajas :

- Esta solución es más integral debido a la operatividad de los sistemas de voz y datos es mediante el mismo enlace de datos, debido a que nos permite levantar la troncal de voz a través de dicho enlace.
- El sistema redundante que se sugiere es mediante un enlace DIGIRED de 128kbps para poder tener en forma permanente el servicio que se activara en caso falle el enlace principal.

- Garantiza mayor escalabilidad para aumentar recursos de interconexión entre amas centrales ya que al tener mayor trafico a demanda se podrá realizar otro estudio de factibilidad .

c).-Costos de la Solución:

Mostramos en la tabla 6.1 los costos que implica esta solución

Costo de Comunicaciones	Costo Unitario			Costos Totales	
Descripción	Única Vez	Mensual	Cant	Única Vez	Mensual
Comunicaciones 512Kbps -Plata	950	940	1	950	940
Comunicaciones DIGIRED 128 Kbps	750	885	1	750	885
TOTAL COMUNICACIONES				1,700.00	1,825.00

Costo de Equipamiento				
Descripción	Unitario			Total
Alquiler Equipo CISCO 2600	500		2	1,000.00
TOTAL EQUIPAMIENTO				2,700.00

Tabla 6.1 costos solución out-house

Los costos son referenciales y están expresados en Dólares Americanos (US$)

6.1.2.- ESCENARIO 2

En esta segunda solución el grupo de agentes que reciben las llamadas desde la PSTN se encontraran físicamente en el local del Call center , ellos serán capaces de atender y recibir las llamadas a través de la central del Callcenter.

En esta solución se independizan el método de interconexión entre diferentes servicios.

a).- Descripción de la Solución:

- Como los agentes estarán en local del Callcenter ellos realizaran llamadas de salida a través de los enlaces de voz que tienen instalados en el Call center

- La comunicación de Voz de la empresa remota se utilizara para la interconexión directa con los anexos de dicha empresa ya que permite que las llamadas dentro del menú de opciones pueden ser derivadas hacia los anexos de dicho local remoto para lo cual se ha tenido que contratar un E1 de voz para la interconexión de voz, para poder levantar dicho enlace es necesario tener en cada uno de las centrales tarjetas adiciones para poder habilitar dicho E1 de voz, por esa razón en cada central es necesario una tarjeta de primarios para los distintas plataformas.
- Para la solicitud presentada por ser un E1 de voz este tiene capacidad para 30 canales, si se tenia proyectado usar 10 canales, la empresa contratante determinara en que usar dichos recursos.

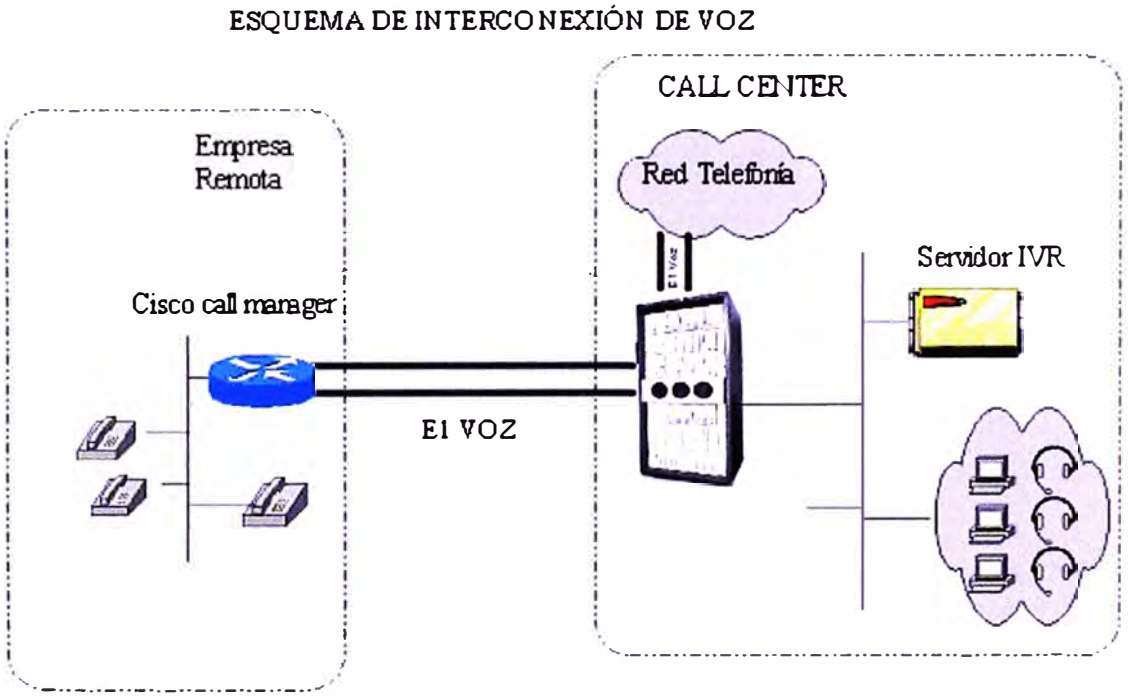


Figura 6.2: esquema de interconexión de voz

- El ancho de banda requerido para la comunicación de datos es de 256 kbps. Se utilizará dicho enlace para la comunicación de los aplicativos con los servidores de la empresa remota, así como para dar información on-line del IVR que solicito para la atención de llamadas.

- El sistema redundante a nivel de datos sería mediante un acceso básico (ISDN BRI). El sistema de comunicación redundante se activará a demanda a la caída del sistema principal.

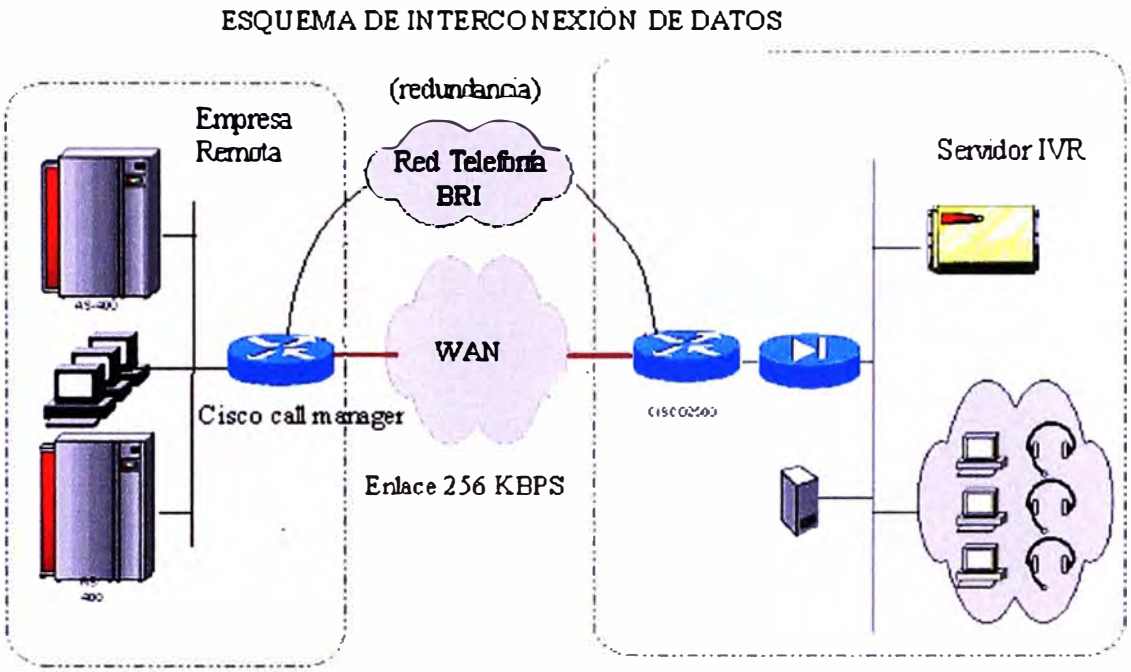


Figura 6.3: esquema de interconexión de datos.

b). Ventajas :

- Esta solución es altamente confiable debido a que la red de datos está separada de la red de voz, por lo cual en caso de alguna caída de red las llamadas tramitaran en forma normal sin que afecte la operatividad del servicio solicitado
- La calidad de audio es un poco mas limpia a comparación del modo de encapsulación que se utilice para la transmisión de voz, al tener un sistema redundante de datos es capaz de soportar la emisión de datos en forma continua esperando que los datos transmitidos sean los necesarios.

c).- Costos de la Solución:

Costo de Comunicaciones	Costo Unitario			Costos Totales	
Descripción	Única Vez	Mensual	Cant	Única Vez	Mensual
Comunicaciones 256Kbps -Plata	700	681	1	700	681
Comunicaciones BRI ISDN			1		97.84
Conexión a la RTB PRI E1			1		1,467.60
TOTAL COMUNICACIONES				700	2,246.44

Costo de Equipamiento				
Descripción	Unitario			Total
Tarjetas Primario central	1200		1	1,200.00
Alquiler Equipo CISCO 2600	500		2	1,000.00
Tarjeta FXO CISCO	1000		1	1,000.00
TOTAL EQUIPAMIENTO				3,200.00

Tabla 6.2 costos solución independientes

Los costos son referenciales y están expresados en Dólares Americanos (US$)

6.1.3. ESCENARIO 3 (IN-HOUSE)

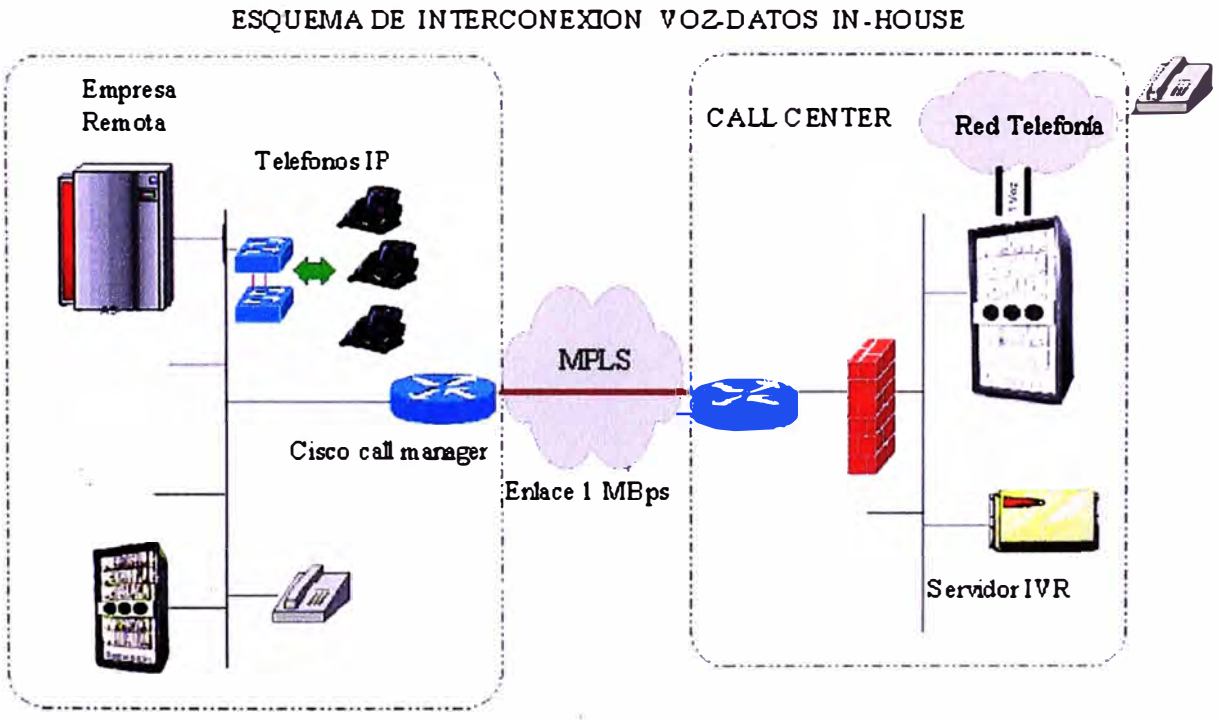
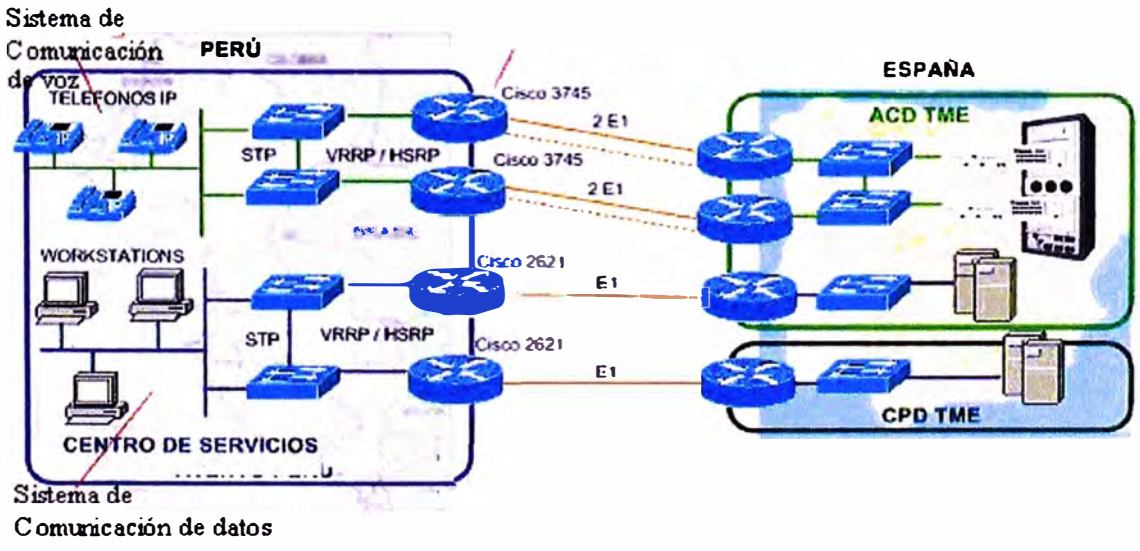


Figura 6.4: solución in-house.

a).- Descripción de la Solución:

- Esta solución está pensada para que en el local del cliente exista la infraestructura tecnológica para la atención en puestos IP, dependientes de la central del Callcenter. El Callcenter pondría brindar las facilidades de equipamiento tecnológico a ser usado para la atención de llamadas en el local del cliente, y los servidores de Telefonía estarán en el Callcenter que harán que los puestos de atención que se encuentra en el local remoto trabaje en forma normal como si estuviese en el local del Callcenter.
- Para esta solución, es necesario que el enlace de datos sea mayor a la considerada en forma inicial, que podrá variar en función de la cantidad final de teléfonos que se usarán en el local del cliente.
- Debido a que la infraestructura utilizada es similar a la planteada a la primera solución, ya que dicha solución es escalable, los costos variaran de acuerdo a los brindados en forma anterior.

Este tipo de soluciones esta siendo muy difundida hoy en día en donde por lo cual en diferentes puntos del planeta que necesitan atender diferente trafico telefónico para poder atender la demanda de sus clientes finales y necesitan que la atención de llamadas sea mas eficiente por lo cual tercerizan la atención de llamadas con



otros call center en diferentes puntos del planeta, como para poder levantar los canales de voz necesarios es mediante la utilización de los enlaces de datos para tener habilitados las troncales ips y solamente con gateways remotos en diferentes países derivan trafico de llamadas hacia distintos puntos del planeta en los call center que están colaborando, este tipo de servicio se puede brindar gracias a la Telefonía IP debido a que a comparación de una llamada mediante Telefonía IP es de menor costo que una llamada internacional, debido a que la inversión que se realiza para poder habilitar es considerable menor que tener siempre activo un enlace internacional que se este pagando mensualmente.

CONCLUSIONES

La telefonía IP ha revolucionado en la mayoría de carriers ya que brinda las facilidades de la red de datos debido a que por un mismo medio de comunicación es capaz de brindar la solución para distintos servicios no necesariamente de datos, sino también de voz y video.

Hoy en día existen diferentes formas para poder establecer llamadas telefónicas para diferentes plataformas como el software de pc que te permite realizar llamadas a través de una simple conexión de internet hasta centrales telefónicas preparadas para Telefonía IP, cualquiera sea el caso hay que determinar que hay ciertas consideraciones que tomar al momento de poner en funcionamiento una central IP, verificar equipos, codecs a usar para los distintas plataformas para determinar que sean compatible.

Hay que tener mucho cuidado al momento de implementar una central netamente IP puesto al no tener en consideración un sistema redundante de datos este seria muy riesgoso para la empresa pues las centrales netamente IP al caer dicho enlace de datos se vuelve muy vulnerable, puesto que las comunicaciones de voz también se verían perjudicadas ya que las troncales telefónicas dejarían de funcionar, perdiendo comunicación con el mundo exterior.

En cambio una ventaja que tiene la telefonía tradicional a través de TDM , al tener la plataforma de voz separada a la de datos estos son independientes; ante alguna caída de los enlaces principales de datos están centrales telefónicas seguirían funcionando sin problemas, por lo cual en el caso de centrales telefónicas es mas considerable tener una central híbrida que soporte tanto troncales analógicos como centrales IP, haciendo la atención de canales de voz sea permanente y de calidad.

Cabe resaltar también que una buena calidad de voz dependerá mucho del ancho de banda que se utilice para la transmisión de voz, cuando se estima cierta cantidad de ancho de banda para ciertos canales de voz, hay que utilizar solamente los canales de voz para lo cual se realizo el estudio inicial, debido a que un aumento de canales en forma considerable haría que la calidad de voz pueda disminuirse o el establecimiento de llamadas fallen en algún momento, por lo cual al haber un aumento de canales de voz siempre hay que evaluar si es necesario que también se aumenten el ancho de banda para la priorización de los paquetes de voz sobre los de datos que es realizado por las distintos medios de transporte como MPLS y los protocolos usados para dichos fines.

Otro factor importante es que estas centrales IP son de costo un poco mas considerable a las enlaces de voz tradicionales (E1's) y de las soluciones antes descritas en el capitulo anterior indican que el costo de inversión es menor para las soluciones Ip sobre las de TDM, por lo cual muchos optan por esta solución eficaz y de considerable calidad.

Antes de decidir invertir en una central IP, es necesario realizar un trabajo de análisis de las funcionalidades solicitadas. lo realmente relevante es conocer el negocio y el flujo de atención que se quiere proporcionar. Hay que analizar los canales que se abrirán con el público y los diversos tipos de respuesta que se quieren brindar. Por ejemplo, llamadas telefónicas, e-mails, chat, collaboration, SMS, de modo de seleccionar correctamente la arquitectura a utilizar y basarse en una red IP con capacidad de transporte de flujos diferenciados por calidad.

A la hora de realizar una migración hacia una central IP, muchas organizaciones están considerando la deslocalización de los call centers de sus sedes de origen. Generalmente ésta suele ser una de las causas de la migración, que repercute de manera positiva para aquellas compañías que no sólo estaban atentas a los cambios del mercado sino fundamentalmente para aquellas que supieron detectar que en la red estaba el negocio del cambio en los últimos tiempos, tal puede ser el caso de una compañía eléctrica, de gas o de telefonía donde su Contact Center opera las 24 horas del día distribuido en distintos sitios, sin riesgo de estar fuera de servicio y con todas sus aplicaciones distribuidas y redundantes

en su red".

Por lo cual algunos países en la actualidad se han convertido en un centro atrayente de inversiones dedicadas al outsourcing. Y justamente la evolución del mercado de los Contact Centers a nivel global continuará creciendo a nivel nacional y regional debido a tres datos fundamentales: el outsourcing and offshore (alta densidad), upgrades de tecnologías, e inversiones en nuevas soluciones (de mediana y baja densidad) que son los mayores consumidores en Tecnología de centrales IP.

Las aplicaciones distribuidas en la red tales como ASR, TTS, CTI, remotización de agentes, disponibilidad para que un usuario de call center pueda ver al agente que lo está atendiendo a través de la pantalla de su teléfono móvil son los nuevos retos que se estan presentando. La red será capaz de soportar una infinidad de aplicaciones sobre los Contact Centers. Además, un dato interesante: para los clientes que disponen de los beneficios de tener instalada telefonía IP, la migración a un call center IP es mucho más natural y escalable.

BIBLIOGRAFÍA

1. BLACK, U. (1999). Voice over IP. New Jersey: Prentice Hall PTR.

2. CUERVO, F., GREENE, N., HUITEMA, C., RAYHAN, A., ROSEN, B. y SEGERS, J. (2000). Megaco Protocol versión 0.8. RFC 2885, Agosto 2000.

3. DOUSKALIS, B. (2000). IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR

4. GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol Architecture and Requeriments. RFC 2805, Abril 2000.

5. HAMDI, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P. (Mayo, 1999).Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999, pags. 104-111.

6. HERSENT,O., GURLE, D. y PETIT, J.P. (2000). IP telephony: packet – based multimedia communication systems. Great Britain: Addison – Wesley.

7. ITU-T Study Group 16 (1998). Recommendation H.246. Enero 1998.

8. ITU-T Study Group 16 (2000). Recommendation H.323v4 (draft). Noviembre 2000.

9. MINOLI, D. y MINOLI, E. (1998). Delivering Voice over IP Networks. New York: John Wiley & Sons, Inc.

10.http://www.aui.es/biblio/libros/mi99/19voz_ip.htm

11.http://www.avaya.com

12.http://www.recursosvoip.com/protocolos/megaco.php

13.http://www.commworks.com/Spanish/Softswitch/Softswitch_Components/Session Agents/H.323_SIP/

14. http://neutron.ing.ucv.ve/revista/e/No7/Russomanno%5Cvoz%20sobre%20IP.html

15.http://www.protocols.com/pbook/VoIP.htm#MGCP

16. http://www.monografias.com/trabajos11/descripip/descripip.shtml

17. http://www.protocols.com/voip/testing.htm

18.http://www.aui.es/biblio/libros/mi99/19voz_ip.htm

19.http://www.gbm.net/bluetech/Edicion14.4/telefoniaip

20.REDES DE COMPUTADORAS, Andrew S. Tanenbaum. Prentice Hall.

21. COMUNICACIONES Y TECNOLOGIAS DE INTERCONECTIVIDAD DE REDES, Cisco Systems. Prentice Hall.

22.THE SOFTSWITCH CONSORTIUM. www.softswitch.org .

23.COMMUNICATIONS MAGAZINE. IEEE. www.comsoc.org , www.ieee.org .

24.SUN www.sun.com

25.CommWorks www.commWorks.com