UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

MIGRACIÓN DE UN CENTRO DE CONMUTACIÓN DE CIRCUITOS A UN CENTRO DE CONMUTACIÓN DE PAQUETES PARA UNA EMPRESA OPERADORA DE TELECOMUNICACIONES

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JIMMY HERBERTH GODOY VEGA

PROMOCIÓN
2006 - I

LIMA – PERÚ
2013

MIGRACIÓN DE UN CENTRO DE CONMUTACIÓN DE CIRCUITOS A UN CENTRO DE CONMUTACIÓN DE PAQUETES PARA UNA EMPRESA OPERADORA DE TELECOMUNICACIONES

SUMARIO

El presente trabajo consiste en mostrar las consideraciones y pasos a seguir para realizar la migración de una central telefónica que trabaja mediante la conmutación de circuitos hacia otra central que trabaja mediante la conmutación de paquetes. Se explica los conceptos básicos a tener en cuenta para realizar el análisis de trafico y entender los tipos de interconexiones usadas y las que se utilizaran para llevar a cabo el cambio de central, se realiza un análisis cuantitativo y cualitativo de las posibles soluciones a implementar teniendo en consideración atender los nuevos requerimientos de los clientes en cuanto a servicios de voz, datos, video y generar reducción de costos, traduciéndose en mejores tarifas para el cliente final, manteniendo o mejorando la calidad de servicio que se presta. A su vez con la actualización y la reducción de tarifas se busca proveer de la mejor y más actual tecnología a clientes actuales, futuros y a los sectores más desfavorecidos. Para la realización de este trabajo, primero se estudiará la plataforma de red actual de la Empresa y se realizará un levantamiento de información, acompañado con el desarrollo de un protocolo de pruebas necesario para cumplir con las exigencias de la Empresa y recomendaciones internacionales referentes a servicios de voz sobre redes de próxima generación (NGN). Finalmente, se procederá a desarrollar un modelo de Ingeniería conveniente para la futura inserción del Softswitch, utilizando los protocolos de control y transporte apropiados, incluyendo una metodología técnica necesaria para la migración de las rutas LDI TDM-S y LDN TDM-S a rutas IP a través del Softswitch.

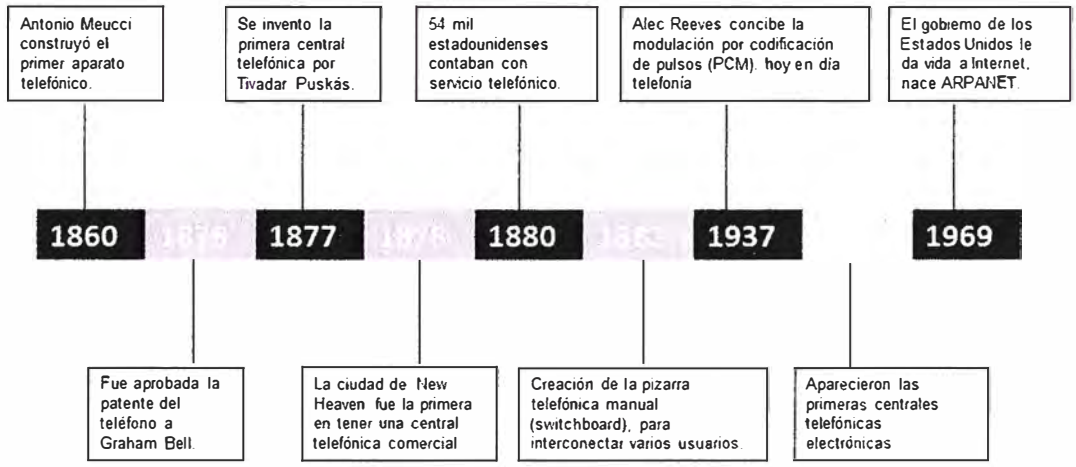
A mi familia

... Cecilia Vega y Diomedes Godoy, mis padres, por haberme apoyado en todo momento, por sus consejos, sus valores que me ha permitido ser una persona de bien, a mi hermana Jessica por ser el ejemplo de una hermana mayor y de la cual aprendí mucho, a Stephanny y Dayanna mis hermanas menores por motivarme a ser un ejemplo para ellas y por su amor.

ÍNDICE

INTRODUCCIÓN

La imprescindible necesidad de comunicación que ha tenido el ser humano desde hace más de un siglo hizo que científicos de la época desarrollaran sistemas que pudieran dar solución a esas necesidades. En 1847 Alexander Graham Bell concluyo teóricamente que se podía transmitir el habla a través de un alambre, haciendo variar una corriente eléctrica de la misma forma que lo hace el aire al variar su densidad dada la producción de sonidos. Entre 1854 y 1860 Antonio Meucci diseño y construyó el primer aparato telefónico. En 1876 fue aprobada la patente del teléfono eléctrico a Graham Bell; tres días después se llevó a cabo la primera conversación a través de un sistema telefónico. En Junio de 2.002 el Congreso de los Estados Unidos aprobó la resolución 269 donde se reconoce a Antonio Meucci como el inventor del teléfono.



Fuente: Elaboración propia, http://timerime.com/es.

En 1878, la ciudad de New Heaven en Connecticut fue la primera en tener una central telefónica comercial y contaba con 20 abonados, cuyo par de hilos de transmisión terminaban en un conector que era manejado por un operador de la central, el cual realizaba la conmutación de manera manual introduciendo una clavija en el puerto del abonado llamante para preguntar el número destino donde quería conectarse, hecho esto, insertaba la clavija en el puerto del destinatario y se establecía la conexión. Ya en 1880, 54 mil estadounidenses contaban con servicio telefónico. Por otro lado, los primeros sistemas de conmutación automáticos se denominaron "de paso" o "paso a paso". En estos sistemas

electromecánicos, la mayoría de los equipos de conmutación tienen sus propios circuitos de control, los cuales están bajo el control del abonado que llama, posteriormente un conmutador localiza la línea y la conecta a otro conmutador selector, que a su vez localiza la línea destino y establece la conexión de la llamada.

Poco a poco las centrales telefónicas fueron evolucionando de manera conjunta con la evolución de la electrónica, hasta llegar a las actuales centrales digitales que son administradas por medio de computadoras; dichas centrales permiten ofrecer servicios complementarios a los habituales en estas redes. Cabe destacar que estas redes telefónicas tradicionales estaban basadas en conmutación de circuitos; para que exista conmutación de circuitos, se requiere una conexión física para el establecimiento del enlace y durante todo el tiempo que este perdure, esto conlleva a cierta ineficiencia dado a que este circuito no puede ser utilizado mientras se mantenga la conexión.

Dado al amplio crecimiento en los suscriptores de dichas redes, la distribución de los recursos se hace cada vez mas critica. Debido a esto y gracias a la evolución de tecnologías y protocolos como el IP (Internet Protocol), basado en conmutación de paquetes, se ha logrado un mejor rendimiento de dichos recursos a un costo mas bajo.

La tendencia actual en las telecomunicaciones, basadas en protocolos IP, se inclina hacia la integración de todo tipo de servicios en una sola infraestructura de red basada en conmutación de paquetes. Estas redes deben ofrecer un nivel de calidad de servicio, capacidad, fiabilidad y seguridad equivalente al de las tradicionales redes telefónicas públicas conmutadas.

CAPÍTULO I.
PLANTEAMIENTO DEL PROBLEMA

1.1 Descripción del Problema.

En telecomunicaciones, la conmutación tuvo su origen en las redes telefónicas que empezaron a constituirse casi inmediatamente después de la invención del teléfono. Inicialmente, la función de conmutación se efectuaba en forma manual en las posiciones de operadora de las centrales telefónicas, como se observa en la figura 1.1.

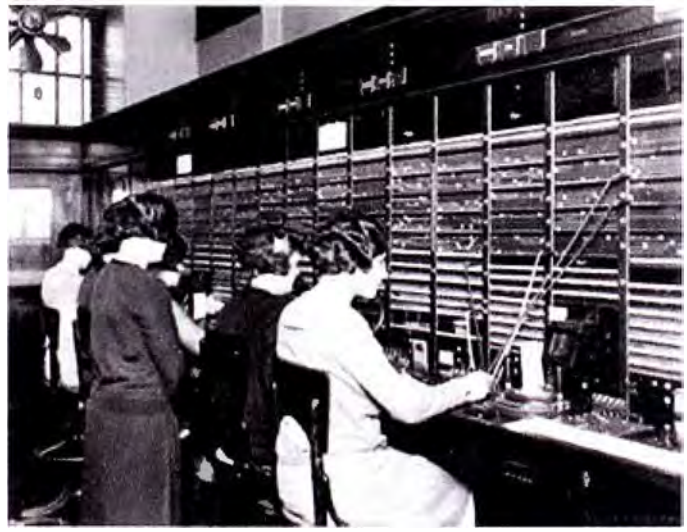


Figura 1.1 Imagen de una de las primeras centralitas telefónicas. Fuente: Anton A. Huurdeman, "The Worldwide History of Telecommunications".

Desde la invención de la conmutación de circuitos, las centrales telefónicas han evolucionado rápidamente hasta las modernas centrales digitales de hoy que constituyen elementos vitales para la mejora y potenciación de las redes de telecomunicaciones. Un importante hito, en la historia reciente de la conmutación en el marco de la era electrónica, fue el constituido por su división en dos técnicas básicas diferentes pero relacionadas entre si: la conmutación de circuitos, aplicada fundamentalmente a las redes telefónicas tradicionales y la conmutación por paquetes que conoce su pleno éxito en las redes de comunicaciones de datos.

Las redes de conmutación de circuitos consisten en una serie de centrales de conmutación (conmutadores) interconectadas entre sí, de manera que a través de éstas se unen una serie de puntos, estableciendo el camino físico entre el origen y destino. La característica clave de esta técnica es que el camino es fijo y permanece establecido durante todo el tiempo que dura la transmisión, siendo independiente de la información enviada, es decir, aunque no se envíe información el trayecto permanece fijado. El camino físico se establece en cada punto de conmutación en función del destino, de los circuitos o enlaces libres y del tráfico cursado entre otros.

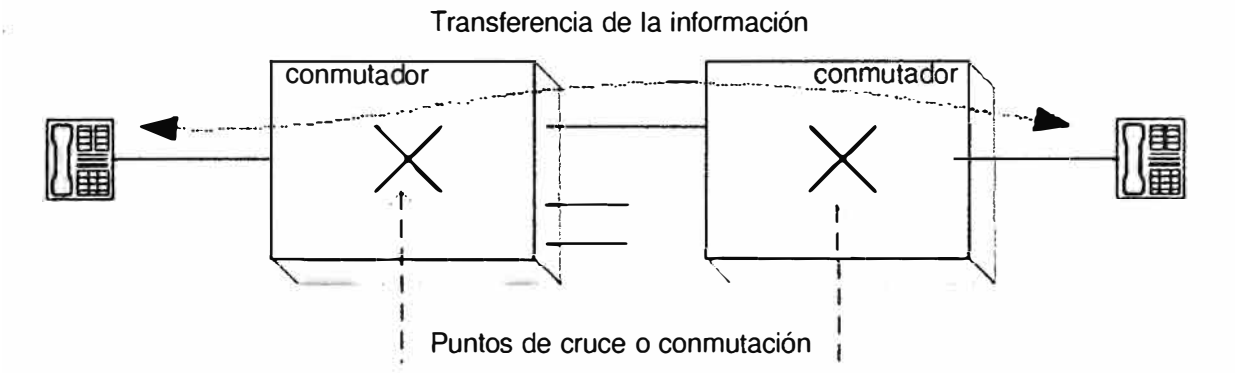


Figura 1.2 Conexión permanente de dos abonados a través de una red de conmutación.
Fuente: Enrique Herrera Perez, "Introduccion a las telecomunicaciones modernas".

La técnica de conmutación de circuitos presenta las características de: ancho de banda fijo e invariable, este ancho de banda es de unos 64kbps, por cada llamada, utilizando la multiplexación por división del tiempo (TDM), también presenta un retardo bajo en la fase de establecimiento de la conexión, de unos 20 ms aproximadamente. Además esta red se comporta de manera transparente a la información que viaja y como se muestra en la Figura 1.2, se establece un camino físico entre los extremos de la red que hace que el retardo de la información para llegar desde el origen al destino sea constante y muy bajo.

Las redes de conmutación de paquetes, son tipos de redes que pueden englobarse dentro de la familia de redes de almacenamiento y envió, que actualmente se están implantando de forma mayoritaria para servicios de comunicación de datos.

Las terminales de datos generan información agrupada, en la mayoría de los casos, en mensajes de bits de longitud finita. Si la longitud de los mensajes originados por los terminales es mayor que unos centenares de bits, se toma interés por el control de errores,

retransmisiones y retardos, fraccionando estos mensajes en unidades menores llamadas "paquetes" que son enviados independientemente a través de la red.

Frente a la conmutación de circuitos, en conmutación de paquetes, no existe fase de establecimiento. Cada uno de los paquetes lleva información de destino, bien sea la dirección del abonado llamado, o bien sea un número de circuito lógico asignado a la conmutación.

En la técnica de conmutación de paquetes, el transmisor comienza a transmitir tan pronto como haya un camino libre hasta el nodo o central al cual se encuentra conectado. El paquete es almacenado y procesado en este nodo y en cuanto se encuentra un camino libre hacia el nodo siguiente, el paquete es retransmitido hacia el mismo. La operación se repite hasta alcanzar el extremo receptor. De ahí la denominación de esta técnica de conmutación como de almacenamiento y envío. Las redes de conmutación de paquetes tienen diferenciados dos áreas de funcionamiento: la red de acceso y la red de transporte.

La red de acceso, en la cual el equipo terminal de datos accede al sistema utilizando diversas posibilidades que se ofrecen en el mercado; tales como una línea o circuito directo ya sea analógico, generalmente medios físicos como un par de cobre de la planta externa de las redes telefónicas, o digital a diferentes velocidades de transmisión.

La red de transporte, la cual esta conformada por concentradores, centros de conmutación regional, centro de gestión centro de servicios adicionales entre otros.

Conmutación de Circuitos	Conmutación de Paquetes
• Los equipos de conmutación deben establecer un camino físico entre los medios de comunicación previa a la conexión entre los usuarios. • Este camino permanece activo durante la comunicación entre los usuarios, liberándose al terminar la comunicación. • Su funcionamiento pasa por las etapas: solicitud, establecimiento, transferencia de archivos y liberación de conexión.	• El emisor divide los mensajes a enviar en un número arbitrario de paquetes del mismo tamaño. • Estos mensajes llevan una cabecera y la dirección origen y destino así como datos de control que luego serán transmitidos por diferentes medios de conexión entre nodos temporales hasta llegar a su destino. • Los nodos temporales almacenan los paquetes en colas en sus memorias que no necesitan ser demasiado grandes.

Cuadro1.1 Características de la conmutación de circuitos y la conmutación de paquetes.

Conociendo ya las características de cada método de conmutación se puede decir que la conmutación de circuitos, si bien fue una buena técnica para manejar la demanda de comunicaciones desde el inicio de la era telefónica, actualmente presenta limitaciones y desventajas frente a la conmutación de paquetes, entre los cuales se puede mencionar:

La demora para iniciar una comunicación, ya que se necesita un tiempo para realizar la conexión, lo que conlleva un retraso en la transmisión de la información.

El acaparamiento de recursos, ya que no se puede aprovechar el circuito en los instantes de tiempo que no hay transmisión entre la partes, se desperdicia ancho de banda mientras las partes no están comunicándose. Se tiene un circuito fijo, no se reajusta a la ruta de comunicación, adaptándola en cada posible instante al camino de menor costo entre los nodos. Una vez que se ha establecido el circuito, no se aprovechan los posibles caminos alternativos con menor coste que puedan surgir durante la sesión.

Poco tolerante a fallos, si un nodo intermedio falla, todo el circuito se viene abajo, hay que volver a establecer conexiones desde el principio.

Ante esto la conmutación de paquetes presenta las ventajas siguientes:

Tiempo nulo de establecimiento de llamada, ya que no existe fase de establecimiento.

Alta eficiencia, el circuito es compartido por diversas comunicaciones simultáneas, así como los recursos de la red que son compartidos estadísticamente por todos los usuarios.

Menor coste, al ser los recursos compartidos también se reparte los costes, resultando ventajoso para el usuario en comparación con otros medios como las líneas dedicadas.

Transmisión de información de identificación de destino, es necesario incluir alguna identificación de destino en cada paquete de la comunicación.

Necesidad de capacidad de almacenamiento en la red, sí, localizada en los nodos de conmutación de la red.

Gran flexibilidad en utilización de la red y posibilidad de rutas alternativas, en un tipo de conexión existente (datagrama), existe la posibilidad de que los paquetes viajen cada uno por distintas rutas.

Desequilibrio de velocidades, la velocidad o capacidad de transferencia de información en un extremo no tiene porqué ser la misma que en el otro, puesto que los nodos de la red tienen memoria de almacenamiento intermedio, la capacidad de transferencia en el origen puede superar a la del destino. La velocidad de la línea física de transmisión empleada es independiente de la velocidad de transferencia de información efectiva en cada instante, el ancho debanda se asigna dinámicamente, utilizándose solo cuando hay información a

transmitir. Entonces si tomamos en cuenta el gran crecimiento de las redes de comunicaciones, el ancho de banda creciente a nivel mundial, la alta demanda de los servicios de datos y la optimización de equipos para garantizar la calidad de estos servicios, hacen necesario que una empresa de telecomunicaciones este acorde con los avances tecnológicos, y tenga que integrar las redes de voz, datos y video. Como resumen se presenta en el siguiente cuadro las ventajas y desventajas de la conmutación de circuitos frente a la conmutación de paquetes.

Conmutación de Circuitos	Conmutación de Paquetes
Ventajas -La transmisión se realiza en tiempo real, siendo adecuado para comunicación de voz y video. -Acaparamiento de recursos. Los nodos que intervienen en la comunicación disponen en exclusiva del circuito establecido mientras dura la sesión. -No hay contención. Una vez que se ha establecido el circuito las partes pueden comunicarse a la máxima velocidad que permita el medio, sin compartir el ancho de banda ni el tiempo de uso. -El circuito es fijo. Dado que se dedica un circuito físico específicamente para esa sesión de comunicación, una vez establecido el circuito no hay pérdidas de tiempo calculando y tomando decisiones de encaminamiento en los nodos intermedios. Cada nodo intermedio tiene una sola ruta para los paquetes entrantes y salientes que pertenecen a una sesión específica. -Simplicidad en la gestión de los nodos intermedios. Una vez que se ha establecido el circuito físico, no hay que tomar más decisiones para encaminar los datos entre el origen y el destino. Desventajas -Retraso en el inicio de la comunicación. Se necesita un tiempo para realizar la conexión, lo que conlleva un retraso en la transmisión de la información. -Acaparamiento (bloqueo) de recursos. No se aprovecha el circuito en los instantes de tiempo en que no hay transmisión entre las partes. Se desperdicia ancho de banda mientras las partes no están comunicándose. -El circuito es fijo. No se reajusta la ruta de comunicación, adaptándola en cada posible instante al camino de menor costo entre los nodos. Una vez que se ha establecido el circuito, no se aprovechan los posibles caminos alternativos con menor coste que puedan surgir durante la sesión. -Poco tolerante a fallos. Si un nodo intermedio falla, todo el circuito se viene abajo. Hay que volver a establecer conexiones desde el principio.	Ventajas -Si hay error de comunicación se retransmite una cantidad de datos aun menor que en el caso de mensajes -En caso de error en un paquete solo se reenvía ese paquete, sin afectar a los demás que llegaron sin error. -Comunicación interactiva. Al limitar el tamaño máximo del paquete, se asegura que ningún usuario pueda monopolizar una línea de transmisión durante mucho tiempo (microsegundos), por lo que las redes de conmutación de paquetes pueden manejar tráfico interactivo. -Aumenta la flexibilidad y rentabilidad de la red. Se puede alterar sobre la marcha el camino seguido por una comunicación, se pueden asignar prioridades a los paquetes de una determinada comunicación. Así, un nodo puede seleccionar de su cola de paquetes en espera de ser transmitidos aquellos que tienen mayor prioridad. Desventajas -Mayor complejidad en los equipos de conmutación intermedios, que necesitan mayor velocidad y capacidad de cálculo para determinar la ruta adecuada en cada paquete. -Duplicidad de paquetes. Si un paquete tarda demasiado en llegar a su destino, el host receptor(destino) no enviara el acuse de recibo al emisor, por el cual el host emisor al no recibir un acuse de recibo por parte del receptor este volverá a retransmitir los últimos paquetes del cual no recibió el acuse, pudiendo haber redundancia de datos. -Si los cálculos de encaminamiento representan un porcentaje apreciable del tiempo de transmisión, el rendimiento del canal (información útil/información transmitida) disminuye.

Cuadro1.2 Ventajas y desventajas de la conmutación de circuitos frente a la conmutación de paquetes.

En este contexto la telefonía fija y móvil en la actualidad presenta una clara tendencia migratoria hacia las redes de IP, redes basadas en conmutación de paquetes, estas redes proveen un amplio rango de funcionalidades tan iguales y hasta superiores a las que puede ofrecer las empresas de telefonía pública, las cuales siguen el sistema de circuitos conmutados. Además que de esta manera se consigue que estas redes sean multiservicios y puedan entregar dos o mas servicios sobre la misma plataforma tecnológica. Una red que integra los servicios de voz, datos y multimedia esta enmarcada en la estructura de alta capacidad de comunicación y transporte de datos, esta red debe presentar una constante disponibilidad y alta confiabilidad la cual garantice que pueda responder a los requerimientos cambiantes de trafico, por eso se necesita una red conformada por un equipamiento que garantice estas características, que sea escalable y que permita una optima gestión.

1.2 Objetivo del Trabajo.

Analizar y evaluar el proceso de cambio de tecnología en el centro de conmutación de una red de telecomunicaciones.

Encontrar una tecnología de conmutación que este acorde con los nuevos requerimientos de los clientes y con las nuevas tendencias del servicio de telefonía, donde no solo se busca una comunicación de voz, también se busca una solución que este integrada con otros servicios, como son el video y la transferencia de datos.

Hallar la capacidad de procesamiento de un centro de conmutación de paquetes, con la finalidad de determinar el nivel de eficiencia respecto de un centro de conmutación de circuitos.

Describir el funcionamiento de una central tradicional y describir la tecnología empleada en un centro de conmutación de paquetes, así como su funcionamiento, para realizar una comparación entre ambos e indicar los beneficios de la conmutación de paquetes frente a la conmutación de circuitos.

Demostrar las ventajas económicas y tecnológicas que tiene una red de telefonía IP y su impacto al remplazar un centro de conmutación tradicional.

Evaluar el efecto de un equipamiento que trabaja sobre el protocolo IP y sus funcionalidades que dan servicios adicionales y características nuevas a la comunicación telefónica.

En la figura 1.3 se muestra un diagrama en donde se agrupa a modo de resumen los objetivos generales y los objetivos específicos.

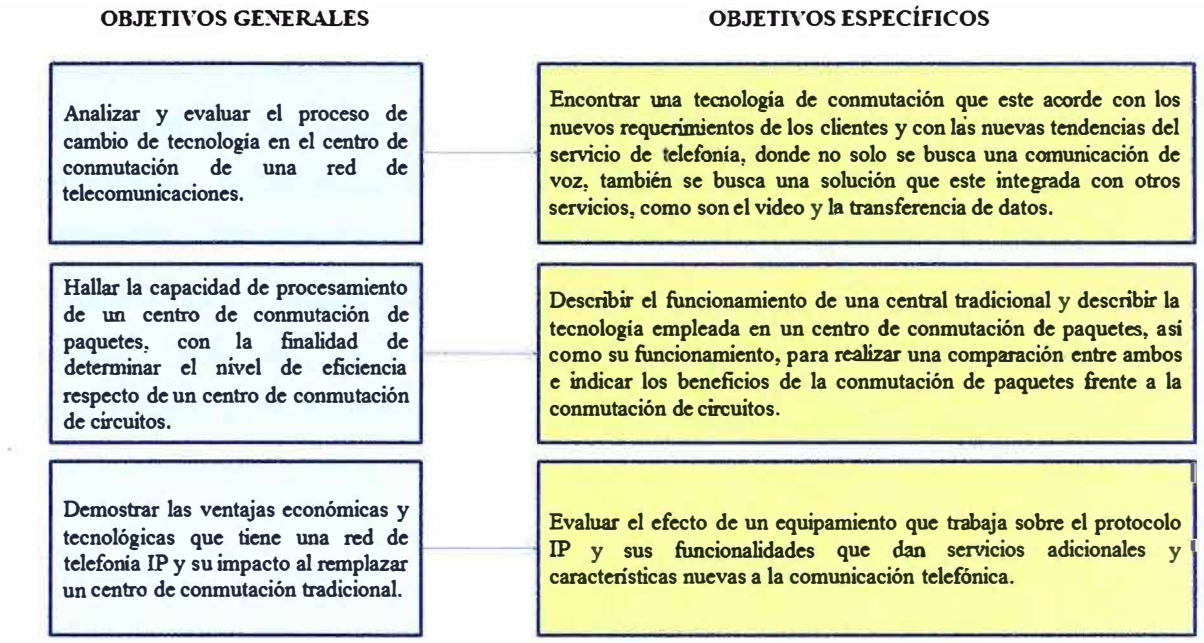


Figura 1.3 Cuadro resumen donde se muestra los objetivos generales y los objetivos específicos.

1.3 Evaluación del Problema.

Las empresas de telefonía en el Perú, con algunos años en el mercado, empezaron operando con centrales tradicionales y conectándose a la PSTN, ya que esta solución era aceptable para los mínimos requerimientos que tenían los usuarios en esos tiempos, donde el único servicio era dar una comunicación de voz. Con el avance acelerado de las tecnologías de redes de datos en estos últimos diez años, y el desarrollo de diferentes protocolos de comunicación, mas escalables y eficientes, así como el desarrollo de las comunicaciones móviles, estos requerimientos mínimos fueron aumentando y creando la necesidad de tener un servicio con mas características y aplicaciones adicionales, incluso obligó a las empresas a dar mas de un servicio sobre una misma plataforma.

Consecuencia de este desarrollo de las telecomunicaciones en los últimos años es que se esta orientando hacia un uso intensivo de sistemas de gran ancho de banda de manera de poder transmitir voz, imágenes y datos con altos niveles de calidad. Esta integración de servicios es lo que da pie al proceso de convergencia el cual abarca escenarios que presentan comportamientos y tendencias bien definidas. Dichos escenarios involucran los

aspectos regulatorios de servicios y mercados de organización empresarial y aspectos relacionados con la tecnología de punta.

La tendencia actual es que las redes de telecomunicaciones existentes, basadas en conmutación de circuitos, evolucionen en Redes de Siguiente Generación (NGN), basadas en conmutación de paquetes usando el Protocolo de Internet, originando impactos tecnológicos, económicos, regulatorios y normativos. Además estas redes son de multiservicio que permite soportar señales de voz, de imágenes, de datos; de manera simultánea y por la misma infraestructura.

Esta nueva situación implica cambios más complejos en los procesos tecnológicos, en la restructuración de la industria, en la normativa e incluso en las leyes regulatorias.

CAPÍTULO II.
MARCO TEÓRICO

2.1 Redes de Conmutación de Circuitos.

La conmutación de circuitos es la técnica más utilizada en redes de telefonía pública; en principio, se desarrolló para el tráfico de señales de voz analógicas y señales de voz digitales, pero también es capaz de gestionar tráfico de datos de manera poco eficiente. En estas redes se establece un canal dedicado para cada conexión que ocurra entre dos terminales, en donde se reservan los recursos de transmisión y conmutación de la red, durante todo el tiempo que dure dicha conexión.

En general, la transmisión se realiza a través de un conjunto de nodos, los cuales pueden estar conectados a otros nodos o directamente a equipos terminales o de abonado. La existencia de un canal dedicado entre estaciones, es consecuencia de la conexión sucesiva entre distintos nodos de la red, donde en cada enlace físico se dedica un canal lógico para el establecimiento de la conexión. Los enlaces entre nodos se multiplexan en FDM (Frequency Division Multiplexing) ó en TDM (Time Division Multiplexing), siendo este último el de mayor interés en este trabajo.

Una red telefónica pública de telecomunicaciones está formada por los siguientes elementos de red:

-Equipos de abonados: son los dispositivos de usuario que se conectan a la red como un teléfono, computador, fax, entre otros.

-Bucle de abonado: constituye el enlace entre la red y el abonado, está formado por un par de cables trenzados.

-Centrales telefónicas: son los nodos de conmutación de la red.

-Líneas principales: formados por los enlaces entre centrales; transportan tráfico multiplexado en FDM o TDM sincrónico. En la Figura 2.1 se muestra un esquema general de la arquitectura de una red telefónica pública.

La conmutación de circuitos implica tres fases:

Establecimiento de un circuito extremo a extremo: en la Figura 2.1 el nodo A envía una solicitud al nodo 4 pidiéndole una conexión con la estación E. El nodo 4 debe encontrar una ruta hacia el nodo 6 dependiendo de su tabla de enrutamiento y costo del enlace. Una

una ruta hacia el nodo 6 dependiendo de su tabla de enrutamiento y costo del enlace. Una vez que decide que es el nodo 5, éste toma un canal libre del enlace; el nodo 5 procede de manera similar hacia el nodo 6 y se le envía un mensaje solicitándole conexión al terminal E.

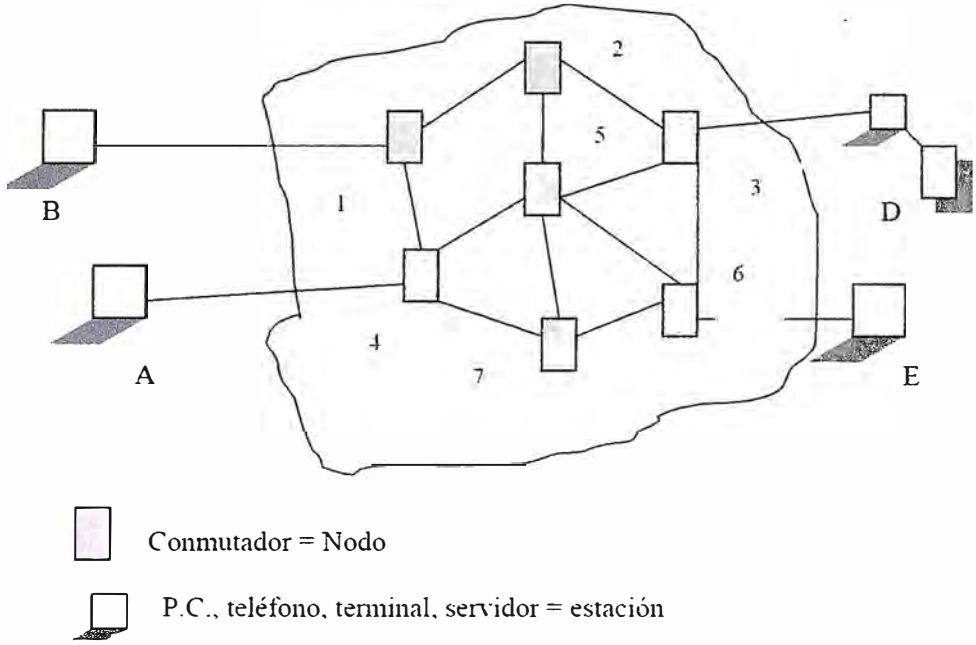


Figura 2.1 Esquema general de la arquitectura de una red telefónica pública.
Fuente: http://www.it.uniovi.es/docencia/Telecomunicaciones/arss/material/arssTema5-Conmutacioncircuitos.pdf.

Envío de información: bien sea analógica o digital siguiendo el camino prestablecido en el enlace.

Desconexión: sucede posterior a la transferencia de información; ésta se finaliza cuando alguno de los terminales da la orden de hacerlo. El mensaje de desconexión se envía a cada uno de los nodos involucrados para que procedan con la liberación de recursos.

2.1.1 Multiplexación por división en el tiempo TDM

Este sistema de multiplexación para transmisiones digitales, se encarga de dividir el tiempo de transmisión en intervalos llamados "time slots", esto se logra organizando el mensaje de salida en unidades de información llamadas tramas, y asignando intervalos de tiempo fijos dentro de la trama a cada canal de entrada; lo que permite recibir los canales de entrada en el receptor. A la salida, se tendrá un régimen binario que será la suma de todas las entradas ordenadas de manera estructural; este proceso se repite de manera constante en el tiempo, y a esta estructura se le denomina "trama". El sistema TDM sincrónico es un esquema de multiplexación en donde el tiempo es obtenido desde un reloj que controla tanto el

multiplexor como el canal fuente. En la Figura 2.2 se muestra la creación de una trama de segundo orden jerárquico a partir de los datos provenientes de 3 canales:

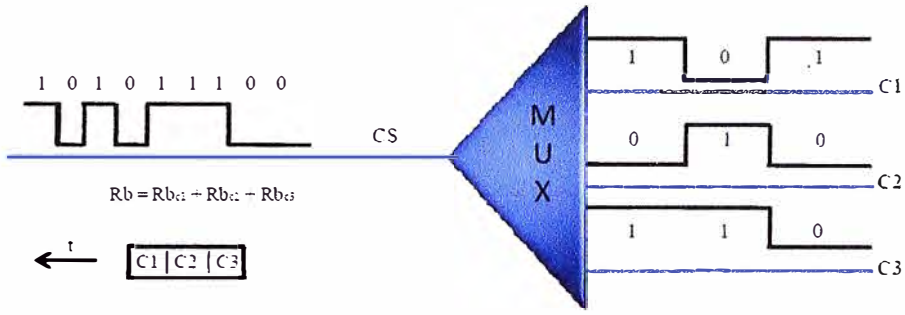


Figura 2.2 Creación de una trama.

Fuente: Estepa, R. EN: http://trajano.us.es/~rafa/ARSS/apuntes/tema6.pdf. Digitalización de la Red Telefónica: R.D.S.I.

La ITU, estableció diferentes jerarquías de multiplexación digital; una de ellas es la Jerarquía Digital Plesiócrona ó PDH (Plesiochronous Digital Hierarchy), todas controladas por equipos multiplexores con relojes de alta precisión; el primer nivel de la jerarquización está formado por un grupo primario, definido en la recomendación G.732 para Europa, véase anexo D, la cual agrupa 30 canales para tráfico a 64 Kb/s cada uno y dos canales de servicio, uno para uso de señalización y sincronización de multitrama y otro para sincronismo de trama y alarmas, ambos a la misma velocidad. La velocidad de transmisión del grupo básico es de 2048 Kb/s utilizando entrelazado de palabras de 8 bits, este grupo primario se le denomina E1. A partir del E1, y utilizando entrelazado de palabras de 4 bits se forman las jerarquías superiores E2, E3, E4 y E5, las cuales llevarán 120, 480, 1920 y 7680 canales de voz respectivamente, disponiendo éstas de espacios reservados para la justificación debido a la diferencia entre los relojes que componen las señales de entrada a la trama. En la Figura 2.3 se muestra la estructura de una trama E1:

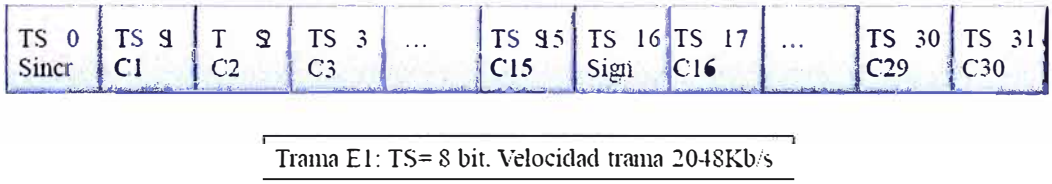


Figura 2.3. Trama E1.

Fuente: Ing. Héctor Figueroa. Estructura de Trama. En: www.desi.iteso.mx/telecom/comunicaciones_1/informacion/comunicacioin_digital_basica.

Con el uso masivo que tiene la fibra óptica, las velocidades de transmisión han aumentado considerablemente hasta el orden de los 10Gbps; dado a esto surgió una nueva jerarquía de multiplexación digital llamada SDH (Synchronous Digital Hierarchy). El nivel básico en la jerarquía SDH es el STM-1 (Synchronous Transport Module) de 155 Mb/s que es capaz de incorporar tributarios plesiócronos PDH dentro de su espacio de carga, lo que permite la convivencia entre ambas jerarquizaciones. Para los niveles superiores STM-4, STM-16, STM-32 y STM-64, la velocidad se multiplica por 4 en cada salto. En el cuadro 2.1 se muestra las velocidades de transmisión para cada uno de los niveles SDH.

Nivel SDH	Tasa de Transmisión
STM-1	155 Mbit/s
STM-4	622 Mbit/s
STM-16	2.5 Gbit/s
STM-64	10 Gbit/s

Cuadro 2.1 Tasa de transmisión de los niveles de la jerarquía SDH.

2.1.2 Señalización CCSS7 (Common Channel Signalling System 7)

Es un estándar global de telecomunicaciones creado por la UIT, el cual define los procedimientos y protocolos sobre cómo los elementos de las redes PSTN (Public Switched Telephone Network) intercambian información sobre una red de señalización digital para realizar enrutamientos y control de llamadas tanto en redes alámbricas como inalámbricas, las recomendaciones se muestran en el anexo E. Entre los usos principales de la red CCSS7 y sus protocolos están: conexión, manejo y desconexión de llamadas y servicios de roaming global, entre otros, como ejemplo de estos protocolos y procedimientos se puede mostrar los mensajes usados para la realización de una comunicación entre 2 usuarios de una red ISDN a través de centros locales distintos, como se muestra en la figura 2.4, en la cual se observa que el centro de conmutación local tiene comunicación mediante el SS7 tanto con el usuario como con el otro centro ISDN. En el medio se encuentran las funciones de gestión hacia ambos lados.

En la misma figura 2.4 se muestra un ejemplo para el protocolo de conexión y desconexión en la ISDN donde también se intercambian los siguientes mensajes:

IAM: (Initial Address Message:). Contiene la información inicial de llamada para el encaminamiento.

SAM: (Subsequent Address Message). Transporta las cifras no enviadas en el mensaje.

ACM: (Address Complete Message). Indica que se ha obtenido en acceso al destino.

ANM: (Answer Message). Indica que el usuario llamado ha respondido.

REL: (Release Message). Permite iniciar la liberación del canal.

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

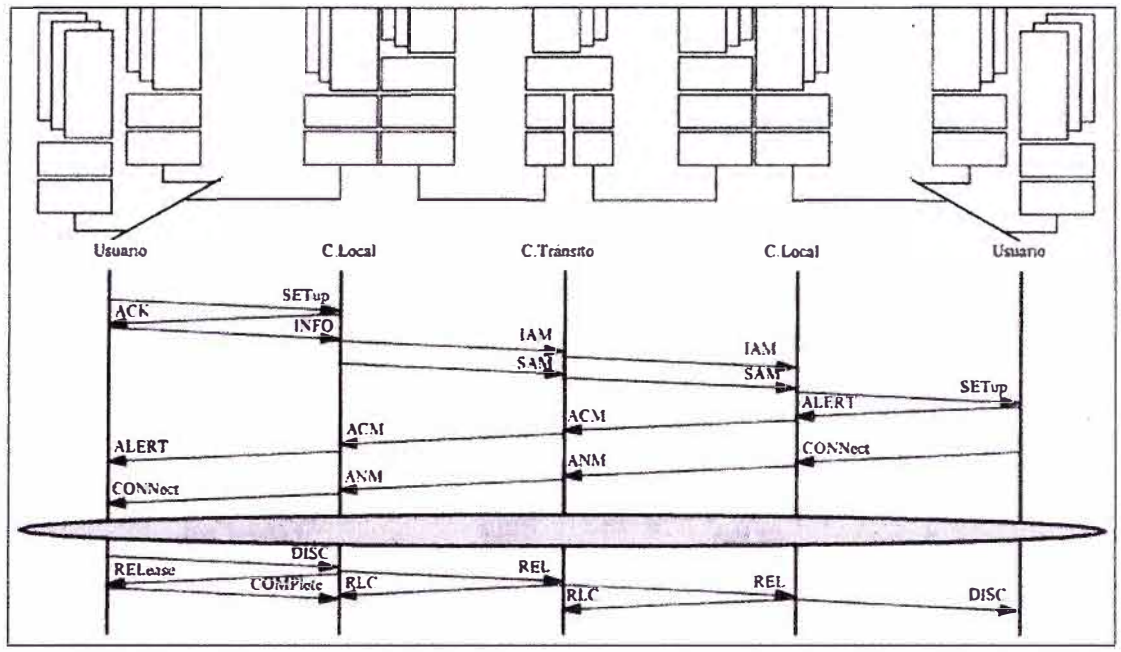


Figura 2.4. Proceso de comunicación en una red CCSS7.

Fuente: //pablodeolavide.dynalias.com/adeubeda

Adicional a esto, se encuentra relacionado el concepto de Red Inteligente, véase anexo F, el cual consiste en la evolución de las redes de telefonía básica, introduciendo una nueva arquitectura de red mediante la inserción de nuevos nodos que cumplen funciones especializadas y adicionales a las que ya se cumplen en estos sistemas, que permitan un manejo eficiente de un volumen considerable de datos, junto con tecnologías de la información y modernas técnicas de manejo de bases de datos. Estas redes permiten ofrecer servicios de tarificación especial como los números 800 y 900, reenvío de llamadas, identificación de llamadas, conferencia, llamada en espera, desvío de llamadas y servicios de redes privadas virtuales. Los elementos que conforman la red de señalización CCSS7 son:

a. Enlaces de señalización SL (Signalling Links): constituyen los canales bidireccionales donde se intercambian los mensajes CCSS7 entre los elementos de red a 64Kbps. La señalización ocurre fuera de banda en canales dedicados independientes de los canales de voz, esto permite una conexión más rápida de las llamadas, utilización más eficiente de los canales de voz y facilidad en el control de la red en general.

b. Puntos de señalización SP (Signalling Point): los puntos de señalización utilizan una tabla de enrutamiento para seleccionar el camino de señalización apropiado para cada mensaje. Cada punto de señalización es identificado con un único código; estos códigos están presentes en cada mensaje de señalización para identificar la fuente y el destino de cada mensaje. Un tipo de punto de señalización es el STP (Signal Transfer Point), en el cual se transfieren los mensajes de señalización al enlace de señalización correcto de acuerdo a la tabla de enrutamiento que estos poseen.

Los nodos que permiten ofrecer servicios de Red Inteligentes son nombrados a continuación:

SSP (Service Switching Point): constituyen los puntos donde se originan, terminan o transitan llamadas.

STP (Signal Transfer Point): SCP (Service Control Point): envían una respuesta al nodo SSP con información del código de enrutamiento que está asociado al número discado.

En la Figura 2.5, se muestra el esquema de una red típica de señalización N°7, para aplicaciones de Red Inteligente:

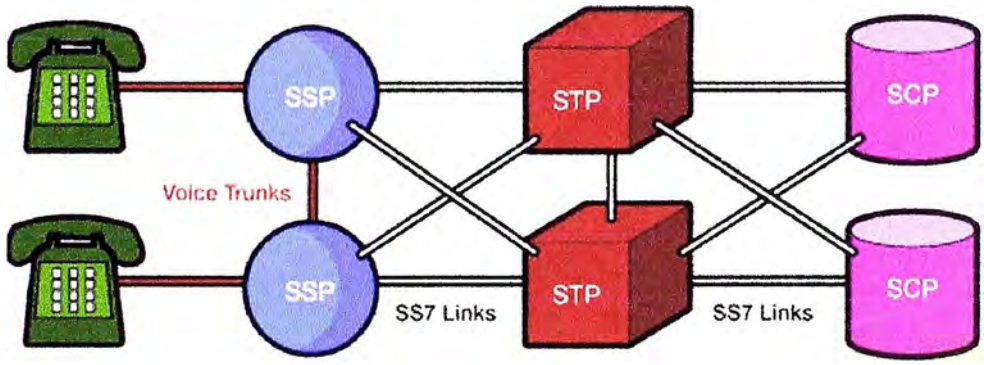


Figura 2.5. Esquema de Red CCSS7 para aplicaciones de Red Inteligente.

Fuente: http: //www.pt.com.

2.2 Redes de Conmutación de Paquetes.

En la conmutación de paquetes, la transmisión de información es estructurada o dividida en pequeñas unidades denominadas paquetes o datagramas; cada uno de estos paquetes es transmitido de manera individual a través de la red siguiendo cualquier ruta disponible hacia el destino, en donde estos son ensamblados según una secuencia prestablecida para obtener el mensaje original. El enrutamiento de estos paquetes no se realiza por una ruta fija, su camino depende de la congestión que tengan los nodos entre el origen y el destino; esto permite que el medio no se utilice para una única transmisión. A todo lo anterior se le conoce como Técnica de Datagramas. Informaciones como el origen, el destino, número de

paquetes que conforman la información, la secuencia, el chequeo de errores, entre otros, son almacenadas en una parte del paquete denominada "cabecera ó header" y la información de usuario final en el "espacio de carga o payload".

Otra manera de llevar a cabo la conmutación de paquetes, es a través de la denominada Técnica de Circuitos Virtuales utilizada en redes orientadas a conexión, en donde se envía un paquete de control antes de los paquetes que contienen los datos; este paquete se comporta como si fuera una petición de llamada, y establece un camino lógico de nodo en nodo, donde posteriormente se enviarán todos los paquetes con la información. Este sistema es similar al de conmutación de circuitos, pero con la salvedad de que cada nodo es capaz de mantener varios circuitos virtuales a la vez.

2.2.1 Modelo de referencia OSI (Open System Interconnection)

La Organización Internacional de Estandarización ISO, por sus siglas en inglés (International Standards Organization), crea en 1984 una norma universal para protocolos de comunicación en respuesta a la necesidad de interconectar e inter operar redes disímiles; este concepto introdujo a un modelo referencial de sistemas abiertos, denominado OSI.

El modelo de referencia OSI está conformado por siete niveles o capas los cuáles se pueden observar en la figura 2.6.

Figura 2.6. Modelo de referencia OSI

Fuente: http://fmc.axarnet.es/redes/tema_05.htm.

a. Nivel físico: es el primer nivel del modelo OSI, en éste se reglamentan todas las características físicas, eléctricas y mecánicas. Esta capa es la encargada directa de la

transmisión y recepción de bits a lo largo del canal de comunicaciones, sea este satelital, por microondas, radio enlaces, cable de cobre, fibra óptica, entre otros. Por otra parte, en éste se encuentran todos aquellos dispositivos activos y pasivos que permiten la comunicación como concentradores, conmutadores, equipos de modulación, aparatos terminales, etc. Cabe destacar que el nivel físico es el encargado de adecuar los datos provenientes de la capa de enlace, en señales adecuadas para transmitir en un medio.

b. Nivel de enlace: el nivel de enlace es el encargado de proporcionar la comunicación nodo a nodo en una red, para ello, éste proporciona las direcciones que permiten entregar los datos a los nodos correctos y a su vez traducir los mensajes provenientes de las capas superiores en bits que puedan ser transmitidos por la capa física. Estos bits los agrupa en tramas que contienen información de indicadores de inicio, dirección de origen y destino, información de control, datos e información sobre el control y detección de errores. El nivel de enlace es también encargado de gestionar y coordinar la manera en como se comparte el medio de transmisión.

c. Nivel de red: es el nivel encargado de proporcionar el esquema de direccionamiento que los mensajes siguen desde la fuente hasta el destino a través de encaminadores ó ruteadores (routers) intermedios. Éste debe ser capaz de manejar el establecimiento, mantenimiento y terminación de conexiones; así como evitar la congestión, y ser el responsable de realizar saltos de subred en caso de ser necesario. Esta capa es totalmente independiente de la capa física.

d. Nivel de transporte: es la que se encarga de controlar el flujo de datos entre los nodos involucrados en la comunicación; por otra parte, recibe los mensajes de la capa superior (Sesión) y los fragmenta con la responsabilidad de ensamblarlos nuevamente en el orden exacto en el receptor, y así obtener el mensaje original. Estos mensajes fragmentados son entregados a la capa de red para ser enviados a su destino. La capa de transporte está relacionada con la optimización del uso de servicios de la red y con la calidad de servicio requerida para un tipo de servicio específico, todo esto mediante el uso de los protocolos adecuados. Además, establece la transparencia de datos y asegura la confiabilidad de entrega de información entre sistemas.

e. Nivel de sesión: El nivel de sesión establece, maneja y termina las sesiones de comunicación. Las sesiones de comunicaciones consisten en peticiones y respuestas de servicios que ocurren entre aplicaciones localizadas en diferentes dispositivos de red. Estas peticiones y servicios son coordinadas por protocolos implementados en esta capa. Entre

los protocolos más usados se encuentran: ZIP (Zone Information Protocol), AppleTalk (coordina la referencia de nombres a dispositivos), SCP (Session Control Protocol), entre otros.

f. Nivel de presentación: La capa de presentación provee a la red de funciones de codificación y conversión que son utilizadas por la capa superior de aplicación. Estas funciones aseguran que la información enviada por la capa de aplicación de un sistema pueda ser entendida por otro. Algunos ejemplos de éstas son formatos comunes de representación de datos, formatos de conversión de caracteres, esquemas de compresión, encriptación, entre algunos otros. De igual manera, diferentes tipos de representación de texto y data como el código ASCII (American Standard Code Information Interchange), EBCDIC (Extended Binary Coded Decimal Interchange Code), Unicode; estándares para video como MPEG (Moving Pictures Experts Group), formatos de imágenes GIF (Graphics Interchange Format), JPEG (Joint Photographics Experts Group) , etc. En la figura 2.7 se muestra un ejemplo de relación de las capas del protocolo CCSS7 con el modelo OSI.

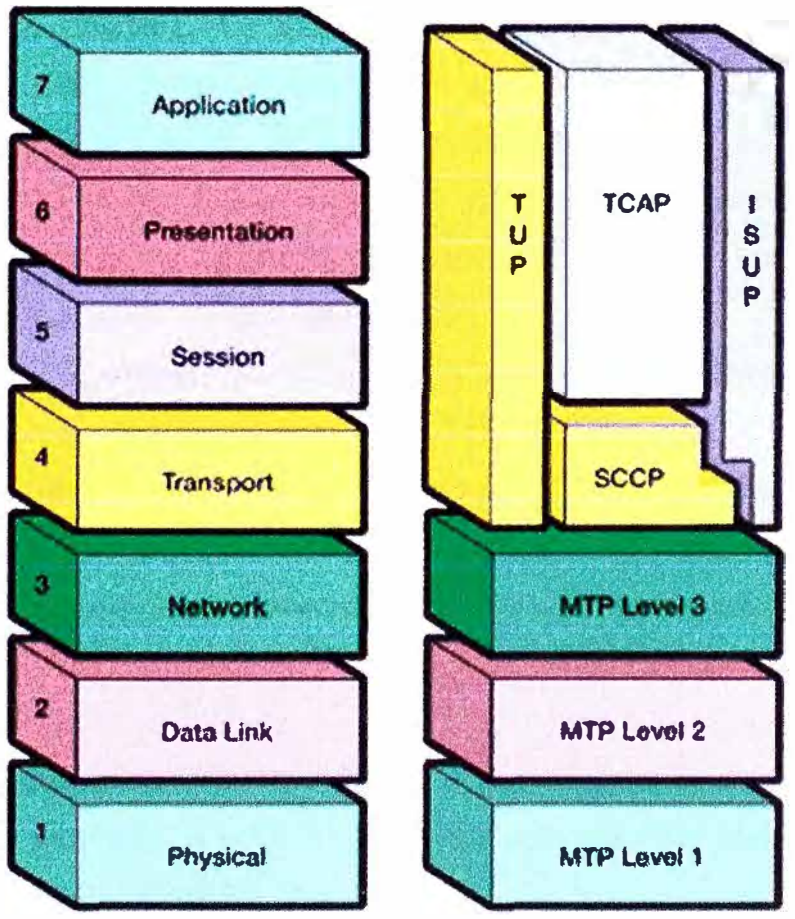


Figura 2.7. El modelo de referencia OSI y protocolo CCSS7.

Fuente: http: //www.pt.com.

g. Nivel de aplicación: es la capa más cercana al usuario final, y es la que representa el modo en que los usuarios interactúan con el ambiente OSI. Dicho nivel provee la interfaz al entorno de comunicaciones, el cual es usado por los procesos de aplicaciones. En resumen, es el encargado de comunicar los parámetros de los procesos de aplicaciones. Algunas otras funciones de la capa de aplicación son: transferencia de información, identificación de los equipos que hacen uso de estas aplicaciones (por nombre, dirección o algún otro parámetro), sincronización entre aplicaciones, determinación de la calidad de servicio, acordar quiénes son los responsable por la integridad de la data y por la recuperación de errores, determinación de los recursos disponibles para la comunicación, disponibilidad de los terminales al momento de la comunicación, etc. Varios ejemplos de implementaciones de la capa de aplicación son: Telnet, FTP (File Transfer Protocol) y SNMP (Simple Mail Transfer Protocol). Un buen ejemplo de la aplicación del modelo OSI es el basamento dado al sistema de señalización CCSS7 para el desarrollo de dicho protocolo.

2.2.2 Modelo TCP (Transmission Control Protocol) / IP

Este modelo surge a partir de los años 70 tras el financiamiento del Departamento de Defensa de los EE.UU (Estados Unidos) a través de ARPA (Advanced Research Projects Agency); la red informática de ARPA, denominada ARPANET (Advanced Research Projects Agency Network), estaba constituida por redes que interconectaban varias universidades, laboratorios y centros de investigación en Estados Unidos; esta red dio comienzo a lo que hoy se conoce como Internet.

Los protocolos más importantes que lo conforman son el TCP y el IP, el conjunto TCP/IP está formado por cuatro niveles o capas:

a. Capa de aplicación: constituye todos los protocolos de alto nivel como el SMTP, Telnet, FTP y HTTP[7] (HyperText Transfer Protocol), así como la representación, codificación, control de sesión y correcta paquetización de datos para ser presentados al nivel inferior. Esta capa corresponde con las capas de aplicación, presentación y sesión del modelo OSI.

b. Capa de transporte: nivel que da base a transmisiones de datos confiables, con control de flujo y detección de errores. Utiliza TCP como protocolo principal y coincide con la capa de transporte del modelo OSI.

c. Capa de Internet: esta capa se encarga de identificar si cada datagrama debe ser procesado de manera local o si debe ser transmitido; asignando para esto la ruta adecuada

dependiendo de la información contenida en la cabecera del mensaje. Corresponde al tercer nivel del modelo OSI ó de Red, y el protocolo principal utilizado es el IP.

d. Capa de acceso de red: su principal función consiste en encapsular los datagramas en tramas y mapear las direcciones IP en direcciones físicas; todo esto con el fin de realizar el enlace para la transferencia de información. Este nivel cumple con las funciones de la capa 1 y 2 (Físico y Enlace) del modelo OSI.

En la Figura2.8 se muestra el modelo TCP/IP y su relación con el modelo OSI:

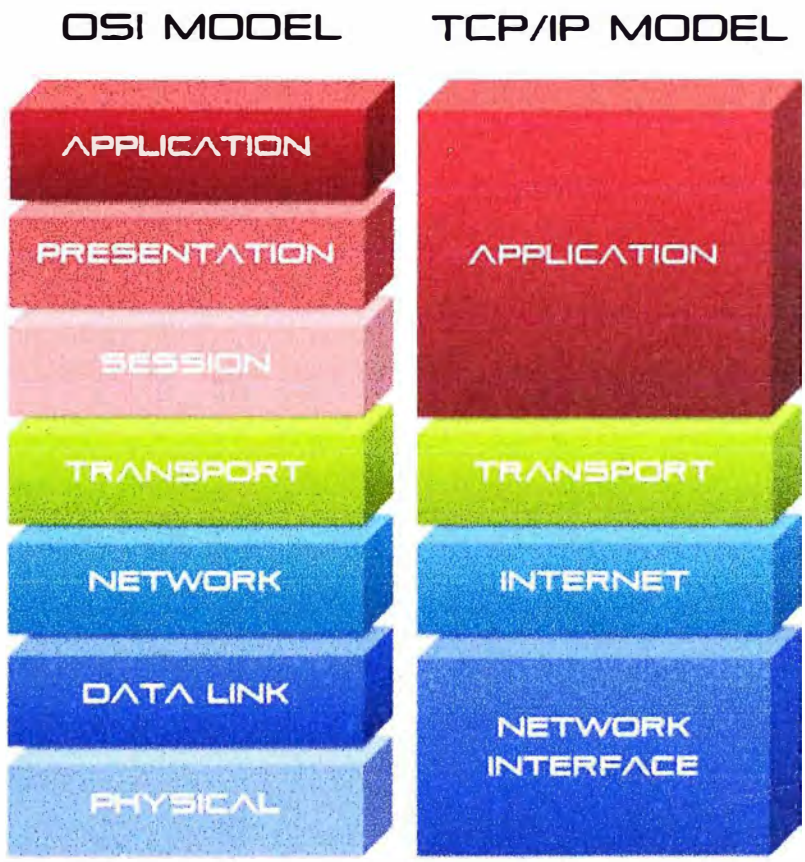


Figura 2.8. TCP/IP y el modelo OSI

Fuente: http: //www.textosciientificos.com/redes/tcp-ip/comparación-modelo-osi.

2.2.3 El Protocolo de Internet

IP es un protocolo de capa de red, el cual contiene información de direccionamiento y alguna información de control que permite el enrutamiento de los paquetes. Este protocolo fue diseñado para ser usado en redes que utilizan conmutación de paquetes; el mismo se encuentra documentado en la RFC 791 (Request For Comments) de la IETF, véase anexo G. Al respecto IP proporciona todas las funciones necesarias para el envío de un paquete desde el origen a su destino, pero sin embargo no garantiza el envío de mensaje de extremo a extremo. Para contrarrestar dicha limitante, IP se vale de los servicios que ofrecen los

protocolos de nivel de enlace para así proporcionar diferentes tipos de garantía y de calidades de servicio.

Mediante el uso de enrutadores, el protocolo IP tiene entre sus funciones, encaminar de manera eficiente los paquetes de acuerdo a la dirección de destino y otros campos ubicados en la cabecera de los mismos. Otra función importante es la de fragmentar y ensamblar nuevamente los paquetes IP dependiendo si el tipo de red requiere o no que éstos sean más pequeños. El protocolo IP presta su servicio utilizando la información de los siguientes campos de cabecera:

a. **Version:** utilizando 4 bits, este sector identifica la versión del protocolo utilizado para transmitir el mensaje, por ejemplo si es IPv4 ó IPv6.

b. **IHL (Internet Header Length)**: en este campo se indica la longitud de la cabecera del datagrama en palabras de 32 bits.

c. **ToS (Type of Service)**: indica los parámetros para el tipo de servicio requerido, dichos parámetros pueden ser utilizados por las redes para definir cómo debe ser tratado el paquete en su transporte; además en este campo se asigna el nivel de importancia del datagrama, esto para dar prioridades al momento del enrutamiento.

d. **Longitud total**: donde se especifica el número total de octetos que conforman el datagrama. Posee un campo máximo de representación de 16 bits o 65.535 octetos.

e. **Identificación**: contiene un valor que identifica el datagrama; con el uso de este campo se posibilita el reensamblaje en el destino de los distintos fragmentos que conforman el mensaje.

f. **Banderas (Flags)**: consiste de un campo de 3 bits, en los cuales los dos menos significativos son bits de control de la fragmentación, uno que indica cómo el paquete puede ser fragmentado y el otro indica si el datagrama contiene fragmentos adicionales; el último bit no está en uso.

g. **Posición del fragmento**: indica la posición relativa del fragmento respecto al inicio de la data en el datagrama original, esto permite la correcta reconstrucción del mismo.

h. **TTL (Time to Live) ó Tiempo de Vida**: es un campo de temporización utilizado para seguir el tiempo de vida de un datagrama, cuando este decrementa hasta cero tras el paso por nodos, el paquete es descartado.

i. **Protocolo**: indica qué protocolo de capa superior recibe los paquetes luego de todo el procesamiento IP.

j. **Suma de control de cabecera**: contiene una suma de comprobación de los datos de la cabecera, esto permite conocer si la información ha sido recibida correctamente.

k. **Dirección fuente**: identifica mediante 32 bits el nodo que envía el mensaje.

l. **Dirección destino**: especifica con un campo de 32 bits el nodo receptor.

m. **Opciones**: campo que no es de uso obligatorio; puede ser utilizado con propósitos de encaminamiento, seguridad, entre otros.

n. **Relleno (Padding)**: utilizado para rellenar con ceros el encabezado IP, asegurando que éste sea siempre múltiplo de 32 bits.

En la Figura 2.9 se muestra la estructura de una cabecera IPv4:

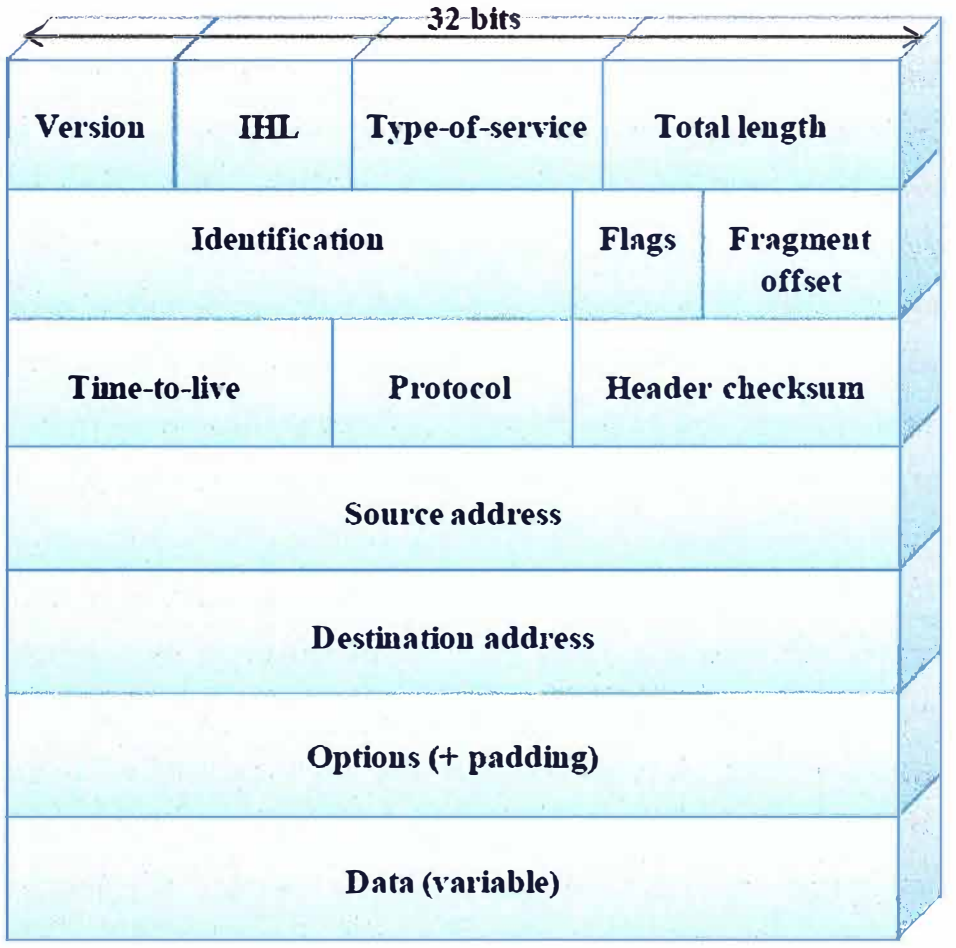


Figura 2.9 Cabecera IPv4

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160.

2.3 Teoría Básica y General Sobre el Equipamiento.

Desde la década pasada la industria de las telecomunicaciones ha sido testigo de impresionantes cambios en la manera como las personas y las organizaciones se

comunican. Muchos de estos cambios son consecuencia del crecimiento explosivo de Internet y de aplicaciones basadas en el Protocolo de Internet IP, como por ejemplo la ciberenseñanza, comercio electrónico, videoconferencias, transmisión en secuencias de video, etc. Es claro para las Empresas de telecomunicaciones actuales que el tráfico de voz y los servicios serán una de las mayores aplicaciones que sacarán gran provecho de IP y sus ventajas, esto basado en una serie de nuevas tecnologías conocidas como voz sobre IP, VoIP ó telefonía IP. Es en los años 90 cuando organizaciones como la ITU, la IETF y la IEEE comenzaron a establecer una serie de parámetros y recomendaciones para la transmisión de voz a través de redes IP, con lo cual pretendían estandarizar los protocolos y las tecnologías a implementar para asegurar la fácil y segura interconexión de productos de distintos fabricantes para el correcto funcionamiento de las redes que involucran servicios de VoIP. La VoIP no es más que el transporte vía Internet de servicios como voz, facsímil y aplicaciones de mensajería en lugar del transporte tradicional de éstos a través de redes telefónicas tradicionales (PSTN); en esta tecnología se encuentran involucrados procesos como la conversión de señales de voz analógicas en formatos de voz digital, así como la compresión y traducción de señales en paquetes IP para su transmisión sobre Internet. El objetivo principal que persigue la telefonía sobre Internet es la de proveer un servicio rentable y de alta calidad, similar a la que espera un usuario de una red telefónica tradicional.

2.3.1 Protocolos de Voz sobre IP

a. Protocolos de digitalización de voz: Como es sabido, los primeros sistemas telefónicos transmitían la voz mediante señales analógicas. Tras la evolución de la electrónica y de los circuitos integrados, la digitalización de voz se convirtió en un paso importante para solventar muchos de los problemas que tenían los primeros sistemas de voz, como control y señalización complejos, falta de encriptación, baja tolerancia a ruido, entre otros. Las técnicas de muestreo, cuantificación y codificación hicieron posible la digitalización de la voz mediante un esquema de modulación muy utilizado en entornos telefónicos como lo es la Modulación por Codificación de Pulsos ó PCM (Pulse Code Modulation). La codificación, entendida como el proceso completo de digitalización y compresión de la voz es lograda a través de un módulo codificador/decodificador (codec) que además de realizar la compresión analógica/digital, comprime la secuencia de bits y proporciona la cancelación de eco.

Esta codificación puede ser realizada mediante tres técnicas principales:

-Por codificación de forma de onda.

-Por codificación basada en modelos matemáticos (algoritmos) sobre la producción de voz,

-Por modelos que combinen las técnicas de codificación de forma de onda y codificación basada en modelos matemáticos.

El ahorro del ancho de banda es una de las principales razones por la que se busca realizar este tipo de codificaciones de la voz para ser transmitidas sobre redes digitales como las basadas en IP.

Los codecs tendrán a su salida una secuencia de bits que se empaquetan en paquetes IP, los cuales son transportados por la red IP hacia el destino, el cual debe estar preparado con los mismos estándares para realizar el proceso inverso, y así lograr una comunicación inteligible.

Hay que considerar que a mayor sea la compresión usada, menor es la calidad de la voz lograda; además se tendrá un mayor consumo de recursos de procesamiento en los equipos involucrados.

La ITU cubre entre sus protocolos, los correspondientes a codificación de voz, agrupados éstos en las recomendaciones G.7xx. En el cuadro 2.2 se muestran los códec comúnmente usados en telefonía.

Codec	Ancho de Banda (Khz)	Intervalo muestra(ms)	Aplicación
G.711 (PCM)	64	10	Telefonía
G.721 (ADPCM*)	32	10	
G.723.1 (MP-MLQ*)	6,3	30	Telefonía Internet
G.723.1 (ACELP*)	5,3	30	Telefonía Internet
G.726 (ADPCM*)	32	5	Telefonía
G.729 (CS-ACELP*)	8	10	Telefonía

Cuadro 2.2 Codecs comunes en telefonía

b. RTP (Real Time Protocol): Estándar que define las comunicaciones de audio y video en tiempo real que son cursadas a través de redes IP, lo que lleva a entender que es un protocolo adaptado a soportar la existencia de pérdidas, retardos y a la variación dinámica de las condiciones por las que pasa toda red de esta naturaleza.

RTP da funciones de transporte extremo a extremo, además de ofrecer servicios como identificación de la información transportada, numeraciones de secuencia, marcas temporales, entre otras. Los paquetes RTP constan de una cabecera, la cual contiene información para poder rearmar el flujo de bits generado por el códec emisor y otra parte de carga útil donde va el propio flujo de bits. La Figura 2.12 muestra la estructura de una cabecera RTP.

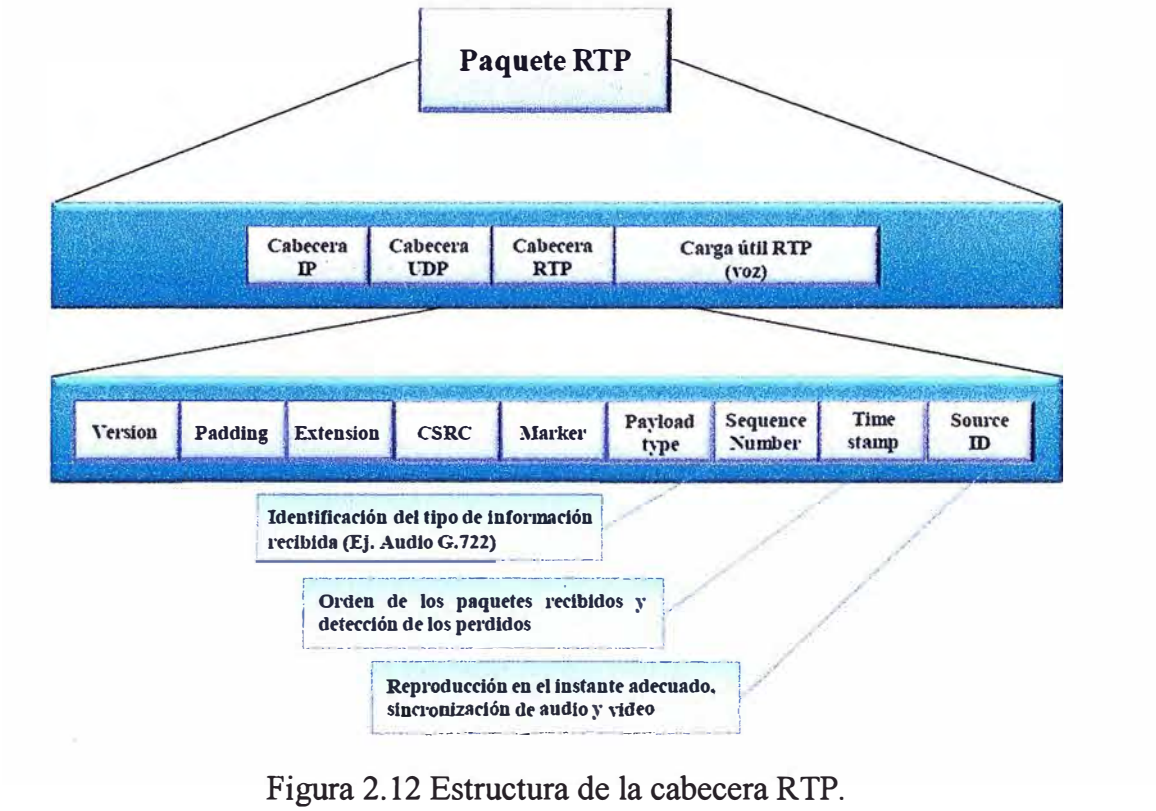


Figura 2.12 Estructura de la cabecera RTP.

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 146.

c. H.323: El estándar H.323 es un estándar (ITU-T), véase anexo H, que permite la transmisión de audio, video y datos a tiempo real a través de redes basadas en transmisión de paquetes, sus aplicaciones se extienden a áreas como consumidores, Empresas y aplicaciones de entretenimiento.

Está pensado para dar solución a necesidades de comunicaciones de servicios multimedia a través de redes LAN y WAN. Este estándar está especificado por el grupo de estudio 16 de la ITU-T (ITU Telecommunication Standardization Sector) y engloba a otros protocolos especificados más adelante.El estándar hace uso de elementos de red como terminales, gateways, gatekeepers y MCU (Multipoint Control Unit), este último empleado en comunicaciones simultáneas de más de dos usuarios, donde los flujos de audio y video son

distribuidos entre los participantes de la multiconferencia. H.323 está conformado por una suite de protocolos de la ITU, éstos y sus funcionalidades son presentados en la figura 2.13 se muestra su arquitectura y en el cuadro 2.3 se muestra los protocolos usados.

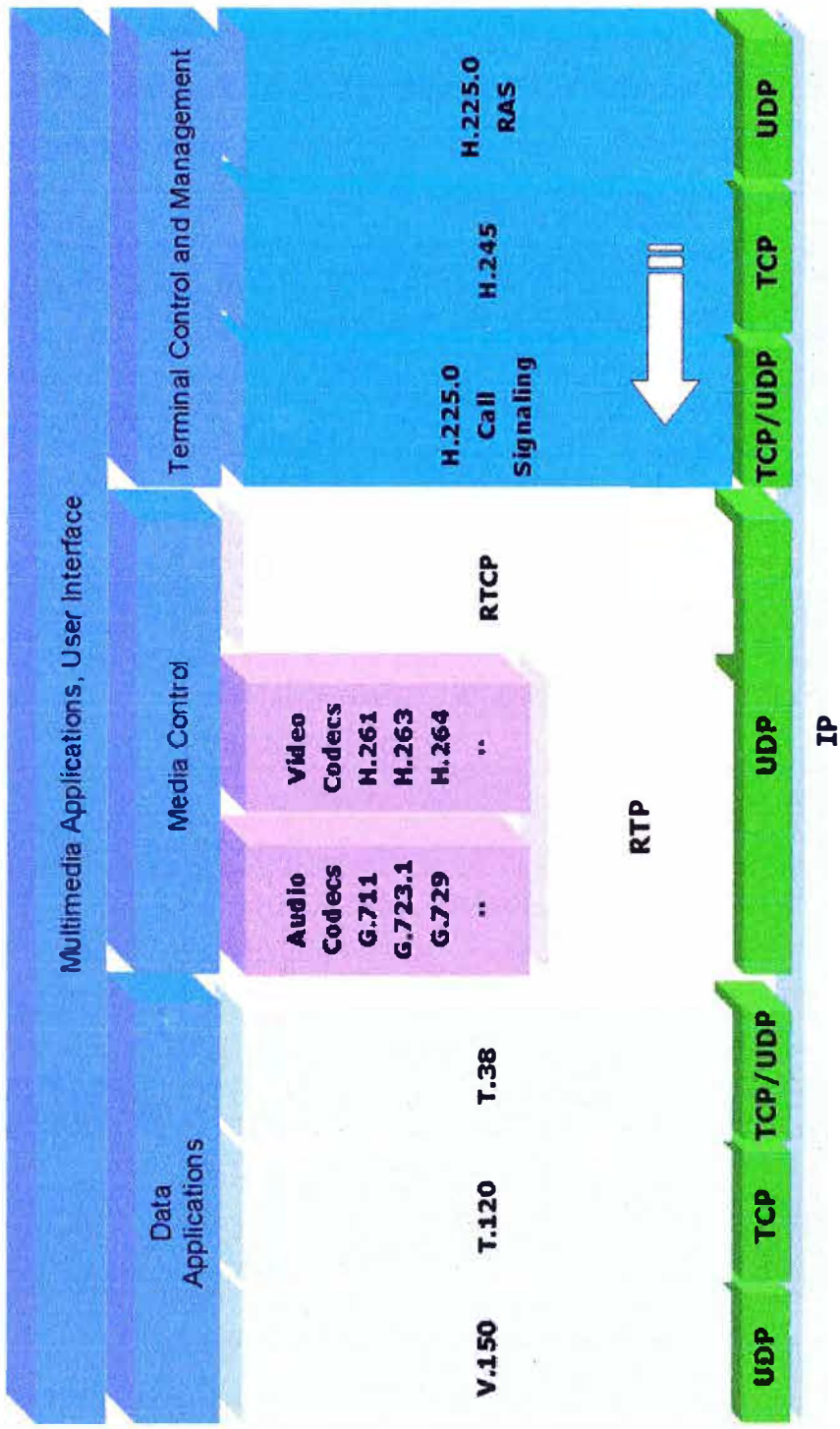


Figura 2.13 La arquitectura de una red H.323.

Fuente: http://kunaytec.blogspot.com/

d. SIP (Session Initiation Protocol). Protocolo de Inicio de Sesiones Estándar publicado por la IETF en el año 1.999 como alternativa a H.323 bajo la RFC 3261, está

caracterizado como un protocolo de control de la capa de aplicación el cual define cómo establecer, modificar o finalizar sesiones entre dos o más extremos sin importar el tipo de sesión que sea. En contraste a H.323, en SIP sólo se definen los elementos que participan en un entorno SIP y el sistema de mensajes que intercambian. Los mensajes en SIP están basados en HTTP y son empleados en funciones de registro, además se usan paraestablecer qué direcciones IP y puertos TCP y UDP (User Datagram Protocol) serán los encargados de intercambiar información.

Protocolos	Característica
H.225 Q.931	Manejo de inicialización y fin de llamadas. Paquetización, sincronización e inicio de llamadas mediante mensajes de señalización Q.931
H.225 RAS*	Registro, Admisión y Status de terminales en gatekeepers H.323
H.235	Autentificación y otras opciones de seguridad
H.245	Negociación de capacidades y manejo de canales lógicos
RTP	Comunicación de audio y video en tiempo real.
RTCP*	Control de mensajes relacionados con calidad de servicio, además de información como identificación, sincronización, y control de sesión
H.261/263	Codificación de video
G.7xx	Codificación de audio
T.120	Control de conferencias punto-punto, punto-multipunto

Cuadro 2.3 Protocolos usados en H.323

Esta puede ser la característica por la cual SIP se perfila como el protocolo por excelencia para desarrollar aplicaciones como telefonía y videoconferencia sobre redes IP. Otros de los protocolos utilizados en SIP, al igual que en H.323, son UDP y RTP para el transporte, H.26x para la compresión de video y G.7xx para la compresión de voz. Otra gran ventaja

es el basamento de SIP en el modelo de Internet y el uso del código de texto ASCII al igual que el de HTTP; el direccionamiento se hace de manera similar al del correo electrónico -User@host-, pudiendo ser User un nombre o un número telefónico.

SIP utiliza una arquitectura del tipo cliente/servidor, es decir, un cliente manda una solicitud, el servidor la procesa y envía una respuesta a dicho solicitante. Es considerada de igual manera una arquitectura descentralizada (peer-to-peer) donde gran parte de la inteligencia reside en los equipos terminales. Por otra parte, el estándar es capaz de distinguir los elementos que lo conforman. Los elementos que conforman una arquitectura SIP son:

Agentes de usuario ó UA(User Agent): corresponde a los equipos terminales de donde se originan las peticiones para inicio o culminación de llamadas, están formados por los UAC (User Agent Client) que inician las sesiones SIP y los UAS (User Agent Server) responsables de aceptar las peticiones recibidas. Ejemplos claros de UA son un teléfono IP y un softphone (Software que simula un teléfono tradicional).

Servidor proxy: entidad intermedia que puede actuar como servidor o como cliente, debido a que se encarga de servir las peticiones internamente o redireccionarlas hacia otros servidores dependiendo a donde se dirija dicha petición.

Servidor de localización: encargado de dar información constante de la localización de usuarios en la red, de manera que éstas lleguen al destino correcto en un instante de tiempo.

Servidor de redirección: es el encargado de responder a la resolución de nombres de usuario (mapeo de direcciones). A diferencia de los servidores proxy, los de redirección no inician peticiones SIP, ni son capaces de aceptar o terminar llamadas.

Servidor de registro: acepta las peticiones de registro de los UAC, y almacena la información de ellos en una base de datos de localización.

Todas las peticiones, excepto la ACK (Acknowledge), tienen asociadas una respuesta del servidor, dicha respuesta tiene asociado un código numérico indicando el resultado de la petición, códigos tomados de http. El cuadro 2.4 muestra las peticiones y respuestas con sus respectivas funciones.

En la figura 2.14 se muestra la manera cómo se ejecuta una llamada en SIP, mostrando los mensajes de petición y respuesta de cada UA y de los servidores normalmente involucrados, también se puede observar en que parte de la mensajería se apertura el canal RTP.

Peticiones SIP	*Funciones*
INVITE	Mensaje de invitación enviado por el llamante
ACK	Respuesta del agente llamante ante mensaje de aceptación de llamada por parte del destino
BYE	Terminación de sesión
CANCEL	Cancelación de petición pendiente
REGISTER	Empleado por usuarios para el registro de su dirección de contacto actual
OPTIONS	Para hacer consulta de capacidades. por ej. Codecs
INFO	Información fuera de banda como DTMF
Respuestas SIP	*Funciones*
1xx	Mensajes de Información
2xx	Exito
3xx	Mensaje de desvío
4xx	Error en la petición
5xx	Error de servidor
6xx	Error generalizado

Cuadro 2.4 Peticiones y respuestas SIP

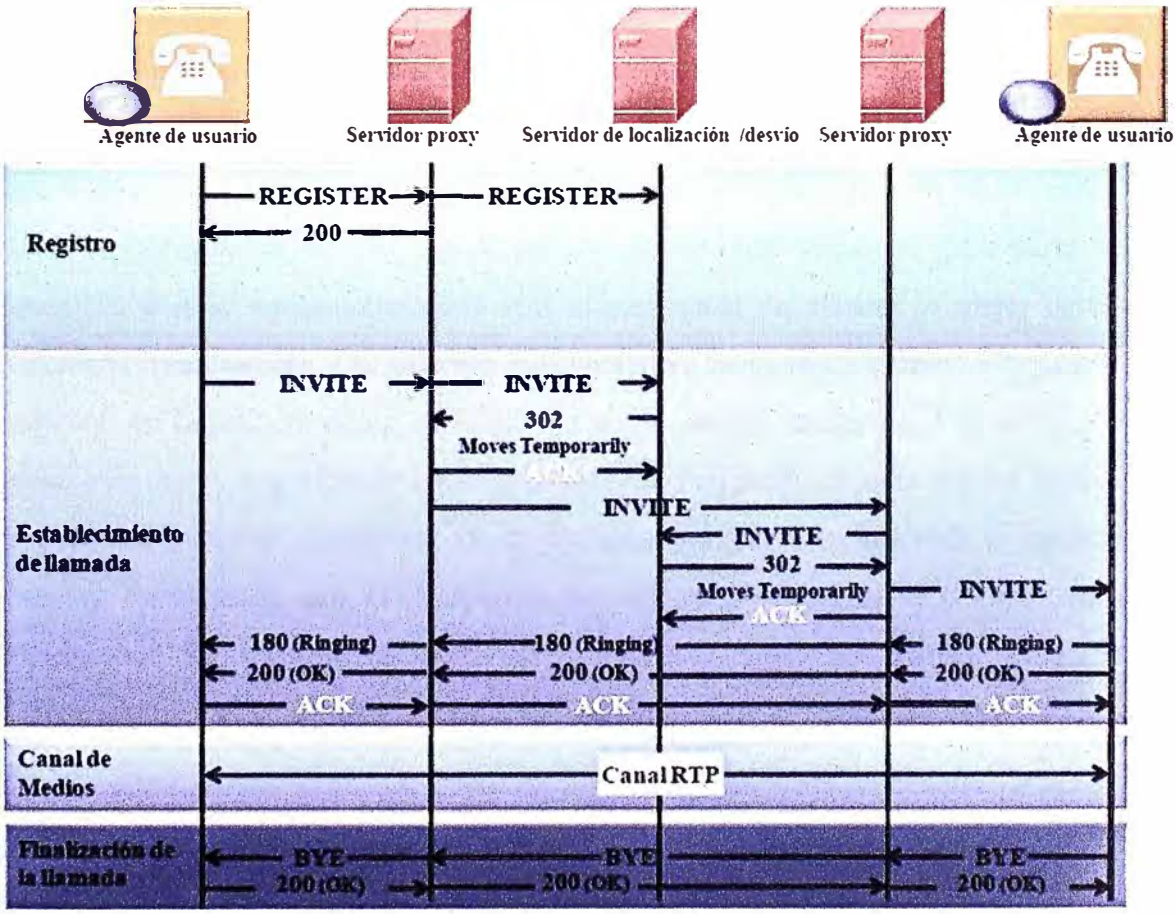


Figura 2.14 Llamada haciendo uso de SIP

Fuente: Huidobro, José Manuel – Martínez, David. Tecnología VoIP y Telefonía IP. (Libro). España, 2006. p. 160.

De la figura 2.14 se pueden resumir los siguientes pasos básicos necesarios para llevar a cabo una llamada en SIP:

- Registro, iniciación y localización del usuario.
- Descripción del tipo de sesión a establecer.
- Aceptación de la petición.
- Establecimiento de la llamada.
- Comunicación.
- Terminación de la llamada.

2.4 Teoría Básica y General Sobre el Software del Equipamiento.

2.4.1 Concepto de Softswitch y SBC (Session Border Controller)

La evolución de las redes basadas en conmutación de paquetes a través del Protocolo de Internet y la gran flexibilidad que éstas ofrecen, han llevado a los proveedores de servicio de telefonía, cuya infraestructura está basada mayormente en redes de conmutación de circuitos, a la búsqueda de conectar a sus clientes a través de redes convergentes basadas en el concepto de red de próxima generación NGN, con la fiabilidad, conveniencia y funcionalidad de las redes telefónicas tradicionales; aunado a esto, tener la capacidad de ofrecer servicios de voz, datos y video de calidad a un costo más reducido a través de una misma infraestructura de red. La tecnología Softswitch surge en gran parte para dar soluciones a estas necesidades, ésta será la encargada de ofrecer lo mejor de las redes telefónicas tradicionales y el Internet. Softswitch es un nombre genérico dado a la nueva evolución en la manera cómo se realiza la conmutación telefónica. Como su nombre lo indica, este nuevo esquema de conmutación se basa en software para emular las tareas que cumplen los Switches telefónicos tradicionales, y ofrecer a su vez toda la innovación en servicios multimedia que el desarrollo de software y las redes IP son capaces de proporcionar. El software es capaz de desempeñar funciones de control de llamada, enrutamientos, facturación y contabilidad (billing and accounting) además de ofrecer servicios de administración de operaciones. Esto denota la capacidad de los Softswitch de realizar las operaciones que hacen redes clase 5 para conectar abonados, interconectar múltiples centrales tandem o clase 4 y servir de centrales de larga distancia ó clase 3, de la misma forma que lo hacen las centrales actuales.

El concepto de Softswitch puede consistir en uno o varios componentes, esto es debido al abanico de tecnologías y equipos ofrecidos en el mercado actual, en donde las funciones

pueden residir en un solo sistema o expandirse a través de varios de ellos. El concepto de Softswitch está basado en los siguientes componentes básicos, según el ISC (International Softswitch Consortium), hoy IPCC (International Packet Communications Consortium).

a. **Controlador de Gateway:** referida anteriormente como Call Agent, definido como el centro operativo del Softswitch; controla el procesamiento de llamadas a través de otros entes sobre los cuales ejerce control como lo son el Media Gateway y el Signalling Gateway. Es conocido también como Softswitch.

b. **Media Gateway:** es el mediador entre la red PSTN y el entorno IP; encargado de dar apertura a los canales de voz, y de aplicar los codecs respectivos a dicha comunicación.

c. **Signalling Gateway:** traduce los mensajes de señalización entre la red PSTN y la IP, los cuales permiten la conexión, establecimiento y desconexión de sesiones. Por ejemplo, es capaz de hacer la traslación de una llamada generada en la PSTN con el uso de señalización CCSS7, la cual debe terminar en una red basada en VoIP, bajo protocolo SIP.

d. **Servidor de Media:** encargado de ofrecer funcionalidades adicionales de audio al sistema de Softswitch, puede proveer por ejemplo de sistemas de IVR (Interactive Voice Response) que ofrezcan valores agregados a la solución.

e. **Servidor de aplicaciones (Feature Server):** ofrece la interfaz de operación y es el encargado de controlar los datos provenientes de los componentes de Softswitch para generar aplicaciones de utilidad para la gestión del sistema como servicios localizados, uso de recursos, facturación, alarmas, entre otras.

La última tecnología en equipos de Softswitch trae como implementación lo que se conoce como controlador de sesiones de borde ó SBC (Session Border Controller), de igual forma ocurre con equipos que tienen como principal función la de SBC e incorporan soluciones de Softswitch integradas. Los SBC son dispositivos que manejan sesiones de voz y multimedia en los bordes de las redes IP, principalmente son los encargados de controlar las dos partes de una llamada sobre IP: señalización y media. La versatilidad de los SBC reside en el hecho de poderlos conectar en el borde entre el acceso y la red Core ó entre dos redes Core en el caso de Interconexión.

Otra función importante de los SBC es la de proveer servicios SIP a través de NAT (Network Address Translation) y Firewalls localizados en los predios del cliente o entre redes, adicionalmente, proteger al módulo de Softswitch de ataques de señalización identificando el trafico malicioso antes de que alcance el Core de la red.

En cuanto a calidad de servicio, los SBC ocupan una posición única en cuanto al control de la calidad de la comunicación del usuario final y refuerzo de los niveles de servicio prestado SLA (Service Level Agreements) mediante los sistemas de control de admisión, los cuales pueden monitorear el número de llamadas y el uso de ancho de banda, de manera de preservar la calidad de las llamadas establecidas. Permite manejar únicamente la señalización de las llamadas, dejando el flujo de información directamente entre dispositivos de clientes, lo que se traduce en un ahorro significativo de ancho de banda en la red.

CAPÍTULO III.
DETERMINACIÓN DE LOS REQUERIMIENTOS TÉCNICOS

3.1 Demanda Potencial.

La central de modelo IMSS 4030 de la marca ITALTEL, es el equipo con el que trabaja la empresa operadora de telecomunicaciones, este equipo soporta el tráfico de los servicios demandados como portador local, servicio portador de larga distancia nacional, servicio portador de larga distancia internacional, dentro de esta clasificación se puede enmarcar los productos de Llamada por Llamada, Multicarrier Móvil y Terminación Nacional y Local.

El producto de Llamada por Llamada es el que se brinda a los usuarios de telefonía fija de los diferentes operadores telefónicos, para que a través de un código de acceso se pueda realizar llamadas de larga distancia nacional y de larga distancia internacional.

Teniendo así la opción de poder elegir un operador distinto al de su cuenta fija para realizar comunicaciones de LD. Este mismo concepto pero llevado a los usuarios móviles es el que se detalla como Multicarrier móvil, con las restricción de solo poder realizar llamadas internacionales con otro operador distinto al que esta subscrito, pudiendo realizar llamadas nacionales solo usando el operador móvil al cual pertenece, esto por un tema regulatorio ya que así lo estableció el Estado Peruano.

Por ultimo se tiene la demanda originada por las terminaciones nacionales e internacionales, que es la venta de tráfico a diferentes operadores internacionales para poder terminar las llamadas que originan dichos operadores.

Estas llamadas pueden tener como destino clientes dentro del territorio nacional o destinos internacionales. Este tipo de tráfico es el que maneja mayor demanda y es vital ofrecer una buena calidad en las terminaciones como en la calidad de las llamadas.

A continuación se muestra los cuadros de la distribución de las interconexiones que se tiene con operadores nacionales.

En el cuadro 3.1 se observa el listado de los operadores internacionales, estos operadores envían llamadas en su mayoría hacia destinos locales y nacionales de Perú, así como también hacia destinos internacionales, adicional a esto estas interconexiones, que se tienen con ellos, sirve también para poder enviarles llamadas con destino internacionales.

Este cuadro también muestra la cantidad de canales de voz usados por cada uno, donde hay una gran preponderancia de operadores como Entel, Intelcom y Teletel, los cuales manejan gran cantidad de tráfico.

Operadores Internacionales	Cantidad de E1s	Cantidad de Canales de voz	Punto de Señalización
Entel Chile	11	330	10223
Telefónica del Perú	3	90	433
AT&T USA	6	180	6305
AMERICATEL USA	3	90	6462
Orange Barcelona	6	180	4343
Orange Madrid	6	180	4342
Intel-Telecom	20	600	1936
Global-Backbone	2	60	1163
Teletel	17	510	1938
ComputerTel	4	120	1938
Ibasis	5	150	1938
LD-Telecom	1	30	1938
Teleglobe	4	120	1938
IDT International	2	60	2304
Etelix	1	30	1938

Cuadro 3.1 Listado de Operadores Internacionales y de sus demandas actuales.

En el cuadro 3.2 se observa la distribución y asignación de cantidad de canales de voz para los operadores nacionales entre los cuales predomina los enlaces con Telefónica del Perú, ya que estos son los principalmente usados para terminar llamadas hacia la red fija de telefonía tanto en Lima como en provincias a través de las diferentes interconexiones establecidas en cada región y de las 2 centrales locales, Washington y San Isidro, en el caso de Lima las cuales presentan la mayor cantidad de canales de voz.

Operadores Nacionales	Cantidad de E1s	Cantidad de Canales de voz	Punto de Señalización
Claro Fijo	4	120	1000
Claro Móvil	2	60	1001
Movistar Móvil	2	60	15404
Movistar Fijo	1	30	4852

Level 3	2	60	1625
Telefónica Washington	21	630	433
Telefónica San Isidro	23	690	33
Telefónica Amazonas	1	30	4227
Telefónica Ancash	3	90	4351
Telefónica Apurímac	1	30	3327
Telefónica Arequipa	5	150	3390
Telefónica Ayacucho	1	30	2689
Telefónica Cajamarca	1	30	4421
Telefónica Cusco	2	60	3327
Telefónica Huancavelica	1	30	2751
Telefónica Huánuco	1	30	2623
Telefónica Ica	2	60	2239
Telefónica Junín	3	90	2751
Telefónica La Libertad	6	180	4477
Telefónica Lambayeque	3	90	4287
Telefónica Loreto	2	60	2367
Telefónica Madre de Dios	1	30	3269
Telefónica Moquegua	1	30	3199
Telefónica Pasco	1	30	2623
Telefónica Piura	3	90	4223
Telefónica Puno	1	30	3263
Telefónica San Martin	1	30	4415
Telefónica Tacna	1	30	3199
Telefónica Tumbes	1	30	4167
Telefónica Ucayali	1	30	2431

Cuadro 3.2 Listado de operadores Nacionales y de su demanda actual.

Estos enlaces de telefónica son usados para poder recibir el tráfico del servicio de llamada por llamada desde Lima y provincias hacia destinos nacionales e internacionales, en el caso de las llamadas hacia destinos internacionales son enviadas por las interconexiones del cuadro 3.1. Las llamadas que tienen como número llamado alguna serie fija del operador Telefónica son entregadas hacia la central de la respectiva provincia de destino o hacia las centrales en Lima en caso de un destino local. En esta lista también se observa las interconexiones con los operadores móviles a través de los cuales se envía todo el tráfico que tiene destino un abonado móvil o fijo inalámbrico, tanto del operador Claro como de Movistar. También se recibe de la red del operador celular las llamadas del servicio

multicarrier móvil hacia diferentes destinos internacionales; estas llamadas son terminadas por las interconexiones internacionales indicadas en el cuadro 3.1.

Adicional a esto la central de Larga Distancia presenta una gran cantidad de E1s conectados a una central privada que da el servicio de Telefonía digital a través de enlaces Primarios y utilizando el protocolo ISDN, esta cantidad de clientes generan gran tráfico que es enrutado por la central de Larga Distancia como se muestra en la figura 3.1, y en el cuadro 3.3 se puede ver la cantidad de canales de voz configurados entre dichas centrales.

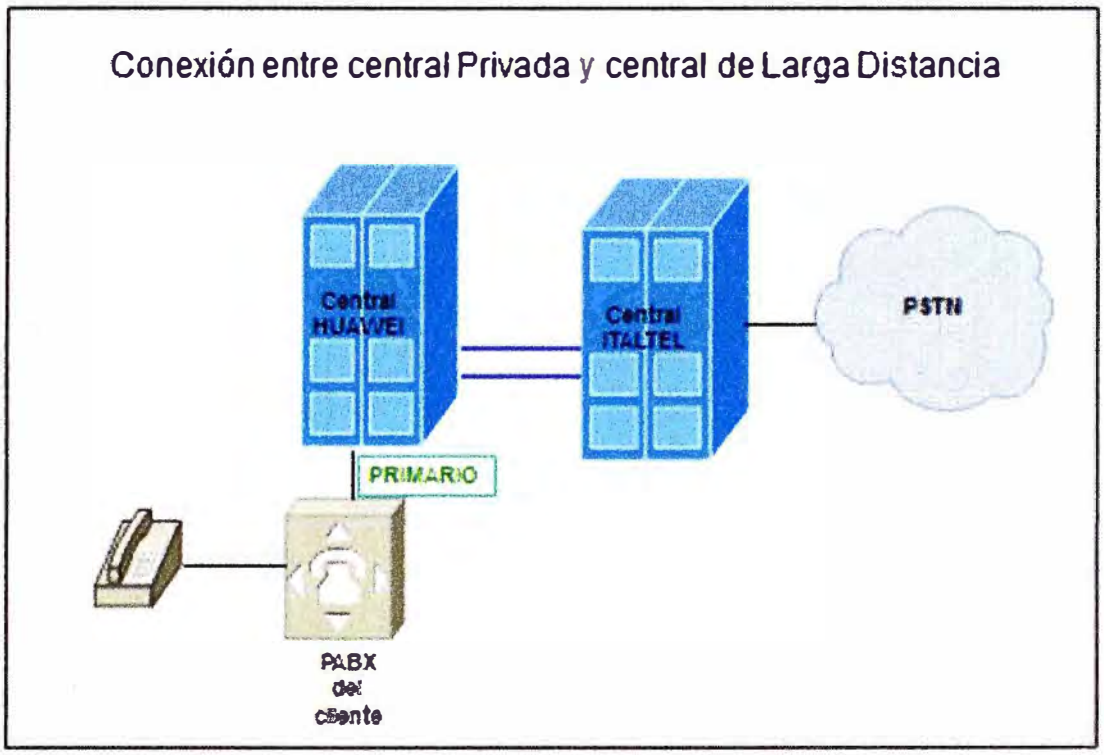


Figura 3.1 Conexión entre central privada y central de Larga Distancia.

Fuente: Elaboración propia.

	Cantidad de E1s	Cantidad de Canales de voz	Punto de Señalización
Central Privada	29	870	1948

Cuadro 3.3 Cantidad de E1s configurados entre la central privada y la central de larga distancia.

Todas estas interconexiones son las configuradas en la central de larga distancia y son las que representan el tráfico que se tiene cursando, si realizamos un análisis del historial de la cantidad de minutos que se cursan para las interconexiones con telefónica tanto para Lima como para provincias, se tiene el cuadro 3.4.

Cuadro 3.4 Cantidad de minutos traficados por las interconexiones de provincias.

DEPARTAMENT	ene-11	feb-11	mar-11	abr-11	may-11	jun-11	jul-11	ago-11	sep-11	oct-11	nov-11	dic-11	ene-12	TOTAL
Amazonas	47,813	45,863	26,172	37,707	61,762	55,390	56,284	55,050	70,543	76,134	68,674	71,950	69,475	742,816
Ancash	1,575,160	1,543,229	1,318,026	1,109,979	1,375,250	1,188,237	1,046,225	1,124,863	1,127,841	1,539,108	1,306,115	1,867,655	1,662,524	17,784,211
Apurimac	81,187	73,122	62,620	63,488	102,743	94,751	96,553	91,304	103,732	124,835	109,861	119,304	115,208	1,238,709
Arequipa	671,463	522,503	543,047	601,634	868,816	839,161	1,017,114	878,840	871,117	1,215,785	1,071,098	1,457,568	1,386,716	11,944,864
Ayacucho	99,464	106,366	66,903	88,396	120,731	99,618	132,339	111,441	119,735	142,100	138,573	173,823	167,292	1,566,781
Cajamarca	188,770	234,512	172,516	186,250	226,492	214,535	202,536	161,294	236,045	316,965	297,177	269,314	327,668	3,034,073
Cuzco	322,408	359,510	330,040	335,210	449,481	407,013	371,819	373,718	349,100	494,091	354,246	490,379	499,144	5,136,161
Huancavelica	16,724	14,157	13,217	12,552	13,624	13,747	17,234	15,268	21,680	21,579	13,225	24,941	20,462	218,409
Huanuco	136,558	197,127	81,438	122,467	243,218	194,487	187,280	150,080	203,652	257,814	250,596	272,833	251,465	2,549,015
Ica	716,999	969,896	488,625	672,992	981,827	860,676	1,175,417	1,241,079	1,258,862	1,407,277	1,268,259	1,364,066	1,470,080	13,876,055
Junin	810,813	637,336	633,900	625,681	964,845	789,713	658,372	818,158	709,811	1,032,861	946,390	1,147,568	1,056,244	10,831,691
La Libertad	3,234,333	2,843,057	3,115,530	2,822,316	3,521,625	2,997,091	3,075,959	3,139,619	3,836,962	4,155,341	3,785,164	4,399,888	3,176,335	44,103,220
Lambayeque	935,537	878,969	888,758	873,880	1,051,660	990,681	1,141,168	1,127,988	1,171,258	1,533,551	1,520,536	1,841,405	1,832,973	15,788,365
Lima	15,787,394	12,969,728	9,516,332	9,684,369	18,683,655	22,385,065	26,789,943	28,216,575	22,171,769	22,848,566	23,167,309	24,635,746	21,018,562	257,875,012
Loreto	284,612	399,135	332,281	255,513	439,036	422,403	412,869	295,714	406,431	578,236	559,962	658,883	491,622	5,536,695
Madre de Dios	40,082	43,873	27,927	32,970	51,994	49,452	63,059	66,327	39,351	56,393	54,847	61,477	59,532	647,285
Moquegua	67,168	89,060	39,678	73,783	101,329	87,663	107,525	127,929	146,117	149,227	86,679	136,110	134,793	1,347,062
Pasco	43,522	44,319	28,636	32,245	42,741	46,723	88,201	93,110	88,385	99,893	61,837	83,185	76,678	829,473
Piura	664,110	769,962	463,448	1,188,040	1,036,315	695,346	660,205	636,922	1,079,325	1,314,869	1,455,961	1,671,698	1,463,957	13,100,158
Puno	40,991	50,290	36,024	51,119	76,144	64,566	83,569	72,214	75,288	87,164	82,762	99,274	76,715	896,120
San Martin	301,493	349,742	250,905	290,722	478,938	331,102	417,128	462,362	489,356	534,134	516,418	518,146	476,767	5,417,211
Tacna	87,769	92,240	65,669	95,204	149,217	148,462	226,185	225,906	207,367	254,698	236,663	278,638	293,552	2,361,571
Tumbes	58,230	69,899	41,419	84,975	91,339	69,576	73,286	76,524	91,296	107,141	92,239	100,899	106,400	1,063,223
Ucayali	169,980	212,080	155,771	212,375	257,842	252,048	273,218	223,740	259,901	314,516	318,316	386,974	392,292	3,429,053
TOTAL	26,382,579	23,515,975	18,698,883	18,952,231	31,390,623	33,297,508	38,373,489	39,786,026	35,134,925	38,662,279	37,762,907	42,131,723	36,626,453	421,317,234

Los datos que se encuentran en los cuadros 3.5 y 3.7 recopilan las estadísticas de reportes de tráfico del área de "Ingeniería de Tráfico y Operaciones" de la empresa Americatel Perú, tomando como referencia el valor pico máximo en Erlang traficados en un periodo de un año para cada ruta; estos datos permitirán comprobar el estado de las rutas actuales y dimensionar la capacidad necesaria para soportar dicho tráfico.

Los valores del cuadro 3.5 se han obtenido teniendo en cuenta dos factores importantes:

-La tasa de llegada de sesiones de comunicaciones, es decir de la cantidad de llamadas por minuto (Q).

-La duración promedio de cada sesión, es decir la duración promedio de cada llamada (HT).

Si Q se expresa en llamadas/minutos y HT en minutos el tráfico promedio en erlang(E) viene dado por:

$$E = Q * HT$$

Como ejemplo tomemos los canales del departamento de Cajamarca, del cual se tiene en su hora pico una tasa de 210 llamadas/hora y cada una dura en promedio 2.097 minutos, entonces el tráfico promedio ofrecido a la red es de:

$$E = \frac{210}{60}[llamadas/min] * 2.097[minutos] = 7.34\ erlang$$

Mediante la utilización de la tabla de Erlang B, la cual se encuentra en el Anexo A, es posible hallar el número correcto de canales para dimensionar el sistema acorde al tráfico presentado, tomando como parámetro de grado de servicio el valor de 0,01, el cual indica que una de cada cien llamadas puede ser bloqueada. Los valores de dicha tabla son obtenidos a partir de iteraciones sucesivas haciendo uso de las fórmulas del modelo de Erlang B, las cuales se presentan como ecuación a continuación:

$$B(N,A) = \frac{(A^N/N!)}{\sum_{i=0}^{N}(A^i/i!)}$$

$$B(0,A) = 1$$

$$B(N,A) = \frac{A * B(N-1,A)}{N + A * B(N-1,A)}$$

Donde N es el número de circuitos disponibles, A es el tráfico ofrecido en Erlangs y B es la probabilidad de bloqueo.

DEPARTAMENTO	Cantidad de E1s actuales	Erlang Pico ene-12
Amazonas	1	1.556336246
Ancash	1	37.24292861
Apurímac	1	2.580827733
Arequipa	3	31.06442764
Ayacucho	1	3.747589606
Cajamarca	1	7.340223641
Cuzco	1	11.18153412
Huancavelica	1	0.458377016
Huánuco	1	5.633170176
Ica	4	32.93188844
Junín	2	23.66137657
La Libertad	1	72.4537052
Lambayeque	4	41.06121229
Lima	19	470.8459125
Loreto	1	11.01303502
Madre de Dios	1	1.333595803
Moquegua	1	3.019551225
Pasco	1	1.717691906
Piura	3	32.79472969
Puno	1	1.718517772
San Martin	1	10.68026359
Tacna	2	6.575975956
Tumbes	1	2.383519639
Ucayali	2	8.787913306

Cuadro 3.5 Erlangs pico para los enlaces nacionales.

Evaluando la cantidad de Erlangs que obtendría en cada departamento y su proyección a corto y largo plazo se tiene:

DEPARTAMENTO	Cantidad de E1 Necesario	Corto Plazo E1 adicional	Largo Plazo E1 adicional
Amazonas	1	1	1
Ancash	3	1	2
Apurímac	1	1	1
Arequipa	5	3	6
Ayacucho	1	1	1
Cajamarca	1	1	2
Cuzco	2	1	2

Huancavelica	1	1	1
Huánuco	1	1	2
Ica	2	4	6
Junín	3	2	3
La Libertad	6	1	1
Lambayeque	4	4	8
Lima	45	19	37
Loreto	2	1	2
Madre de Dios	1	1	1
Moquegua	1	1	1
Pasco	1	1	1
Piura	3	3	6
Puno	1	1	1
San Martin	1	1	2
Tacna	1	2	3
Tumbes	1	1	1
Ucayali	1	2	3

Cuadro 3.6. E1s necesarios para las rutas nacionales.

En el cuadro 3.4 se puede deducir el aumento en la cantidad de trafico con respecto al año anterior donde se puede indicar un aumento aproximado de 10 millones de minutos, lo cual puede dar una estimación de a corto plazo de 40 millones de minutos o en un largo plazo de 80 millones de minutos. Si lo analizamos con una medida de tráfico como son las unidades Erlangs se tiene la estimación de la cantidad de E1s a corto plazo y a largo plazo, como se presenta el cuadro 3.6. Si ahora realizamos un análisis para las demás interconexiones internacionales y verificando el tráfico para cada ruta, estos datos permitirán comprobar el estado de las rutas actuales y dimensionar el ancho de banda necesario para soportar dicho tráfico.

Operadores Internacionales	**Cantidad de E1s**	**Erlang pico**
Entel Chile	11	345.8
Telefónica del Perú	3	90.6
AT&T USA	6	170
AMERICATEL USA	3	83.1
Orange Barcelona	6	197.2
Orange Madrid	6	187
Intel-Telecom	20	615.2
Global-Backbone	2	57.9

Teletel	17	520.5
ComputerTel	4	138.3
Ibasis	5	152.6
LD-Telecom	1	20
Teleglobe	4	114.3
IDT International	2	69
Etelix	1	24.6

Cuadro 3.7. Erlangs pico por ruta internacional.

De los datos de la tabla anterior, es posible realizar el estudio de tráfico para comprobar el estado de los enlaces actuales, utilizando nuevamente la tabla de Erlang que se encuentra en el Anexo A. El resultado de estos cálculos es presentado en el cuadro 3.8.

Operadores Internacionales	Cantidad de E1s Necesarios	E1s Adicionales a Corto Plazo	E1s Adicionales a Largo Plazo
Entel Chile	12.3	6.7	13.3
Telefónica del Perú	3.6	2.8	5.7
AT&T USA	6.3	1.7	3.3
AMERICATEL USA	3.3	1.5	3.0
Orange Barcelona	7.3	6.3	12.7
Orange Madrid	6.9	4.7	9.3
Intel-Telecom	21.4	7.2	14.3
Global-Backbone	2.4	2.0	4.0
Teletel	18.2	6.2	12.3
ComputerTel	4.6	3.1	6.1
Ibasis	5.7	3.7	7.3
LD-Telecom	1.0	0.2	0.3
Teleglobe	4.4	2.0	4.0
IDT International	2.8	4.0	8.0
Etelix	1.2	0.8	1.7

Cuadro 3.8. E1s necesarios para las rutas internacionales.

3.2 Evaluación de la Competencia.

Americatel Perú ofrece sus servicios de llamadas de larga distancia nacional e internacional en todos los departamentos del Perú, este servicio lo da tanto para usuarios de telefonía fija como para usuarios de telefonía móvil, estos servicios son también ofrecidos por los otros principales operadores.

Telefónica del Perú ofrece el servicio de voz para llamadas locales y también el servicio de larga distancia a través de su código multicarrier 1988, tanto para larga distancia nacional como para larga distancia internacional, adicional a esto, y gracias a su red celular desplegada, puede ofrecer este servicio para los usuarios móviles. Teniendo en cuenta que solo para los usuarios móviles puede ofrecer larga distancia internacional.

Otro servicio que ofrece Telefónica del Perú es el servicio de datos a través de sus líneas fijas mediante la tecnología XDSL, este servicio brinda internet y voz en un solo paquete.

Estos productos son ofrecidos tanto en el norte centro y sur del país teniendo sus principales mercados en las ciudades de Trujillo, Chiclayo, Piura y Loreto por el Norte, Lima e Ica por el centro y Arequipa, Cuzco por el sur. America Movil del Perú, con su marca TELMEX, ofrece el servicio de telefonía fija para abonados de Lima principalmente, extendiendo su cobertura de este servicio a las principales ciudades del norte como Trujillo y Chiclayo en su mayoría y al sur en Ica, Arequipa y Cuzco.

También ofrece el servicio de telefonía móvil en todo el territorio del Perú, teniendo como focos de concentración las principales ciudades del norte, sur y centro del país.

3.3 Productos a Ofrecer.

De manera de reducir costos operativos y facilitar la gestión de la plataforma de la Empresa a través de una única red, Americatel Perú plantea la migración de sus servicios de telefonía tradicional TDM a una basada en el Protocolo de Internet, esto gracias a la confiabilidad que ha venido ganando el hardware IP y a la mejora de las redes de transporte de fibra óptica sobre la cual se sustenta Internet. Esto permite a la Empresa cumplir su meta de ofrecer servicios integrados de telecomunicaciones a través de la más reciente tecnología, y ofrecerle a sus clientes actuales y futuros servicios confiables y a costos altamente competitivos. La migración de toda la plataforma requiere de una solución de ingeniería que permita cumplir con éxito los objetivos sin impactar el servicio actual con el que cuentan sus clientes, ni su calidad, es por esto, que el modelo que se propone requerirá de la convivencia de ambas tecnologías para la transmisión de voz (TDM e IP) hasta que finalmente se logre la incorporación total de la tecnología de VoIP.

Esta solución mixta requiere la utilización de Media Gateways que permitan la conversión entre el mundo TDM y el IP. Para asegurar el correcto funcionamiento de la red de telefonía, es necesario comprobar el dimensionamiento de la misma, tanto en canales utilizados como en ancho de banda; para esto se realizara un estudio del trafico actual de la red. Observando las cuadros 3.5 y 3.7, se puede notar una ligera congestión que presentan

algunas de las rutas en la actualidad, y también se puede ver mayor saturación que se tendrá en los enlaces según la proyección a corto y largo plazo, dicha situación se subsana con la futura migración de éstas a rutas IP. Para esta migración se tuvo la propuesta de 3 empresas que vinieron a presentar la tecnología ip que utilizarían:

3.3.1 Propuesta Denwa: Se presenta con su software Denwa NGN para la gestión de comunicaciones multimedia basado en tecnología IP. Este software es el principal dispositivo de la capa de control dentro de una arquitectura NGN (Next Generation Network), encargado de proporcionar el control y procesamiento de servicios multimedia. En las figuras 3.2, 3.3 y 3.4 se muestra la arquitectura de red de Softswitch Denwa. El equipo cuenta con las características de Clase 4 que sirve para interconectarse con redes tradicionales PSTN vía SS7, T1 o E1 y sus funcionalidades de clase 5 las cuales le permiten entregar servicios al usuario final. También presenta herramientas adicionales que son muy usadas en la actualidad como son el Real Time Billing (prepago, postpago y cuenta controlada), Control de Fraude, aprovisionamiento, portabilidad numérica, portal de distribuidores y portal del usuario. Las funcionalidades del Software Denwa NGN son:

- Carrier-Grade, escalable.
- ITU/ANSI/ETSI/CHINA/UK.
- MTP1, MTP2, MTP3, ISUP, TUP, TCAP, opcional SIGTRAN 16 SS7 Links - 1 a 32 E1.
- Múltiples POI - Centralizado o Descentralizado.
- CICs Locales o remotos, VoIP: SIP, opcionalmente H.323.
- Routing automático y manual (grupos y particiones).
- Provisionamiento remoto (XML) o gestión local.
- CDR (Call Detail Record), Calling Name, Calling name delivery, Toll Free y LNP.

Denwa también ofrece su modulo de transcoding, figura 3.5, el cual permite intercambio de los paquetes de media de diferentes formatos de manera segura. IP to IP transcoding es una práctica habitual entre Carriers ya que asegura la calidad, seguridad y costo en cada comunicación. Las soluciones de Telefonía IP requieren de transcoding para múltiples códec. Funcionalidades que presenta el Software Denwa NGN son las siguientes:

- Provisionamiento via Web.
- Transcoding Wireline G.711, G.722, G.722.1, G.726, G.729AB, iLBC, L16.
- Transconding Wireless AMR, GSM, AMR-WB, 30 a 10.000 sesiones de transcoding.
- Sin latencia ni uso de CPU, Recurso compartido de transcoding.
- Transcoding centralizado, Linux Base.

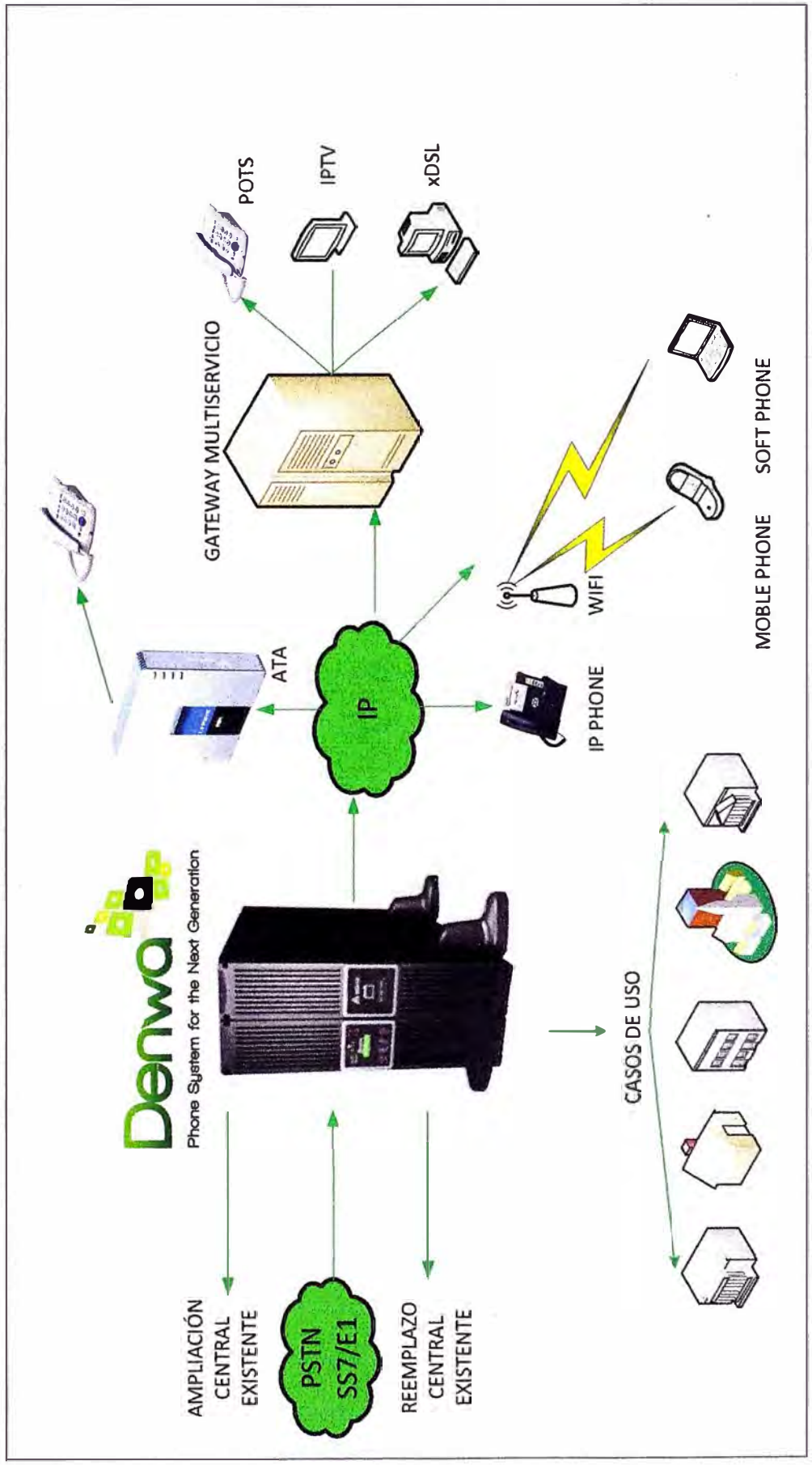


Figura 3.2 Arquitectura de Red Softwitch de DENWA.

Fuente: http://www.denwaip.com/softswitch.html.

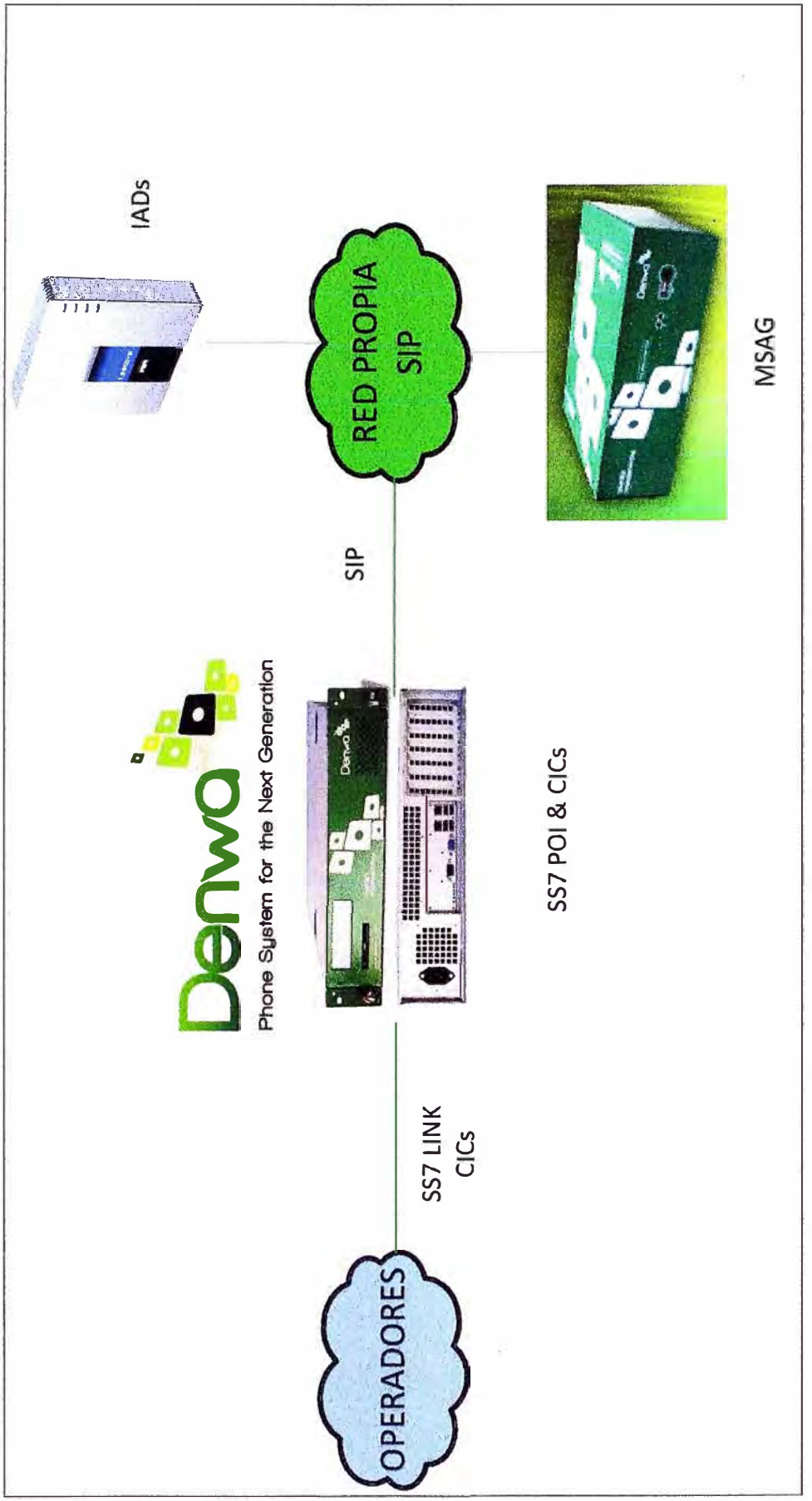


Figura 3.3 Tipo 1 de interconexión de equipo Denwa SS7.

Fuente: http://www.denwaip.com/ss7.html

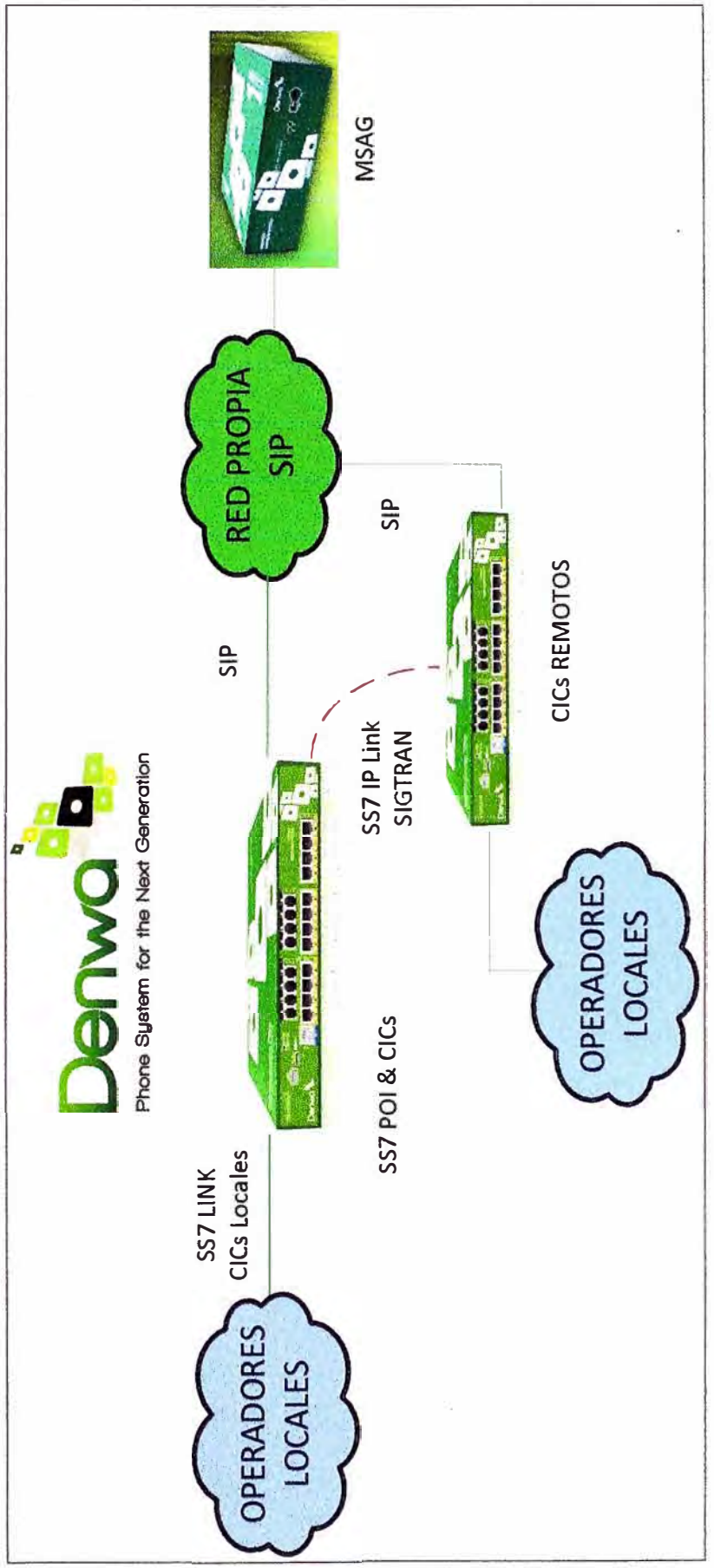


Figura 3.4 Tipo 2 de interconexión de equipo Denwa SS7.

Fuente: http://www.denwaip.com/ss7.html

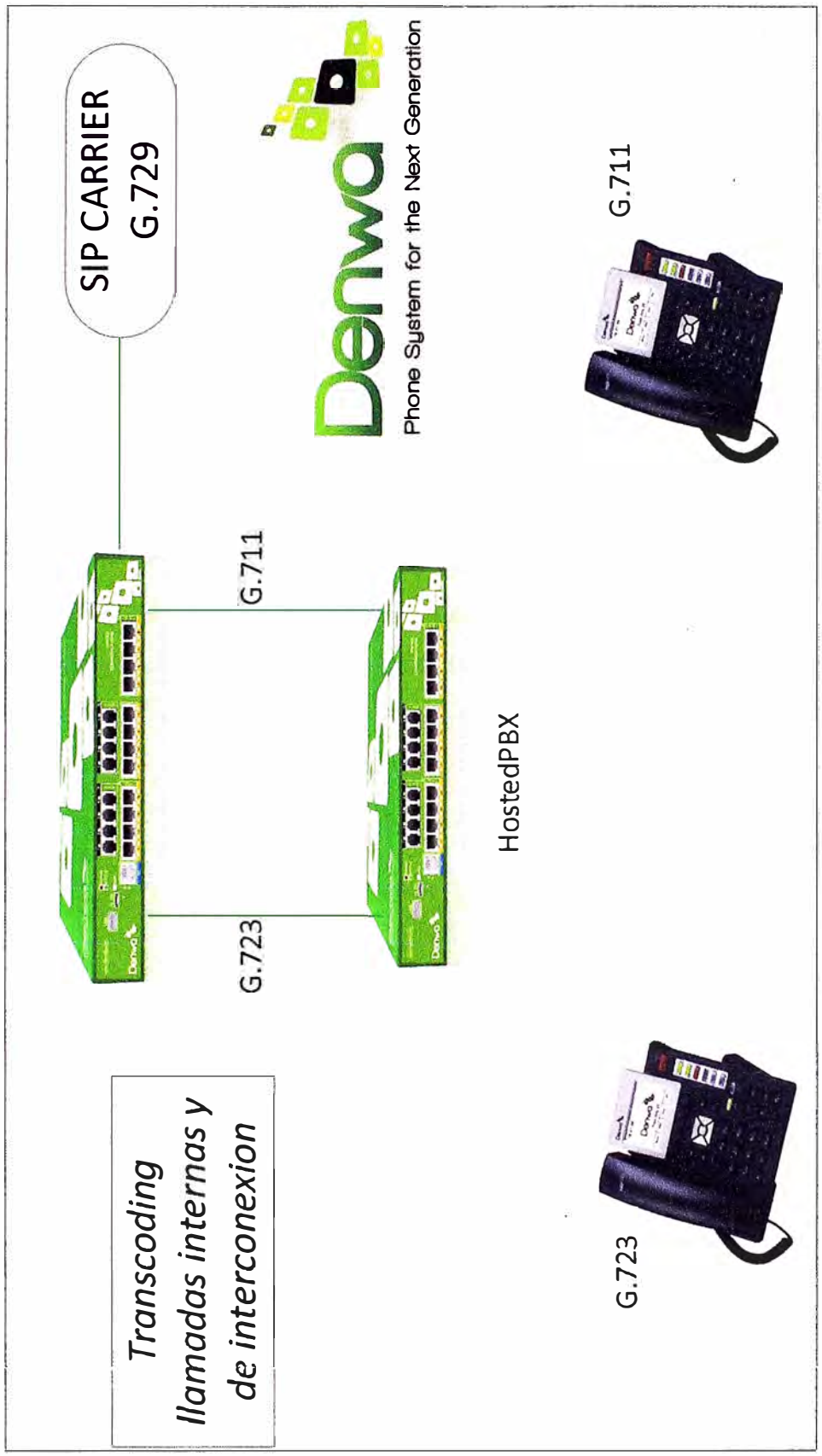


Figura 3.5 Plataforma de Transcoding Denwa compartiendo recursos.

Fuente: http://www.denwaip.com/transcoding.html.

3.3.2 Propuesta Audiocodes: Se presenta con una solución formada por cuatro productos, el primero es la línea de Media Gateway de alta disponibilidad y de nivel carrier, Mediant 8000, el cual ofrece una arquitectura robusta que satisface las estrictas exigencias de los proveedores de servicios en materia de alta disponibilidad. Esta arquitectura se basa en una redundancia costo efectivo de tipo N+1 de las tarjetas de procesamiento y una distribución de la carga de ventiladores y fuentes de alimentación. El Mediant 8000 provee un amplio soporte para interfaces PSTN regionales, amplias opciones en códecs de voz, funcionalidad de Gateway de Señalización, protocolos de control y funciones de seguridad avanzadas, que permiten una gran flexibilidad de despliegue multi servicio para distintos tipos de clientes (ILEC, IOC, CLEC, MSO, grandes empresas y centros de contacto) y aplicaciones. Puede ser utilizado para el backhauling de TDM sobre IP, como parte del remplazo de los conmutadores TDM de clase 4 y 5, interconexión IP, nodos de servicio IP, Aplicaciones IP Centrex y como Gateway PacketCable. En sistemas inalámbricos y móviles, también presenta integración con aplicaciones UMA y Femtocell.
El gateway Mediant 8000, que se muestra en la figura 3.6, es una plataforma modular que cuenta con una escalabilidad de hasta 16,000 canales protegidos, permitiendo a los clientes empezar con un punto de entrada de baja capacidad para luego pasar a una capacidad mayor gracias al aumento del número de tarjetas de procesamiento.

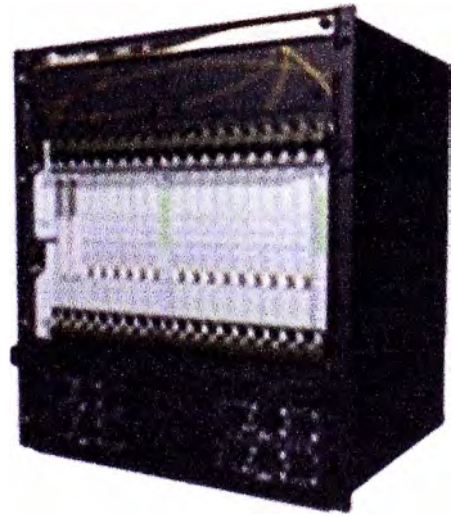


Figura 3.6 Gateway Audiocodes Mediant 8000.
Fuente: http://www.audiocodes.com/CPE.

Con la introducción de las Redes de Nueva Generación, existe una creciente demanda de transcoding IP – IP en escenarios de interconexión, acceso y convergencia fijo-móvil. El

Mediant 8000 puede ser instalado, en primer lugar, como un Gateway de Medios VoIP clásico, y luego puede pasar a satisfacer la creciente demanda de interconexión IP como consecuencia del retiro paulatino de las interfaces PSTN. Ofrece una gran calidad de voz con opciones que varían desde códec de bajo Bit Rate hasta códec de banda ancha, lo que permite una verdadera convergencia entre redes móviles/inalámbricas y redes de líneas fijas, por cable o de banda ancha en una única plataforma de Media Gateway.

Incluye interconexión con las interfaces PSTN más conocidas, incluyendo E1, T1, J1, DS3 y OC3/STM1. Con respecto a la seguridad el Mediant 8000 presenta funciones de seguridad avanzadas, tales como SRTP para medios, IPSec para control y OAM, TLS y PKI para SIP. El segundo elemento representa el software propietario de audiocodecs que tiene la funcionalidad de softswitch, el cual realizara el manejo del protocolo SS7 hacia el protocolo IP, aquí también se incluye las características de operación y mantenimiento, presenta las características de integración con otros UMG (Universal Media Gateway) debido a su manejo de protocolos M3UA, M2UA y H248, el requerimiento actual ofrece una licencia para 1000 abonados, la cual puede ser ampliada. El tercer elemento es el Sistema de Gestión de elementos (EMS) es una solución avanzada para la gestión basada en estándares de los Media Gateways Mediant así como los servidores IPmedia Medios, cubriendo todas las áreas vitales para el buen funcionamiento, administración, gestión y aprovisionamiento de estos productos de red VoIP. El EMS de AudioCodes permite a los proveedores de servicios, empresas y proveedores de equipos de red administrar de manera rentable sus redes VoIP. En la figura 3.7 se observa la interface gráfica del EMS.

El EMS usa un software basado en SNMP optimizado para soportar las actividades diarias del Centro de Operaciones de Red (NOC). Soporta fallas y gestión de alarmas, configuración, monitorización del rendimiento y de seguridad. EMS gestiona simultáneamente múltiples sistemas digitales de la red según Media Gateway y sus módulos, así como CPE analógicas y digitales gateways VoIP.

EMS de AudioCodes incluye interfaces de estándares abiertos para facilitar la integración con los sistemas de mayor capa de gestión y permitir el interfuncionamiento con sistemas de apoyo operativos heredados. Las interfaces de programación de aplicaciones (API) proporcionan un marco extensible, que permite al EMS estar bien integrado en prácticamente cualquier entorno operativo y está diseñado para funcionar en conjunto con los sistemas de gestión de red (NMS), y así proporcionar a los clientes una visión de extremo a extremo de toda su red.

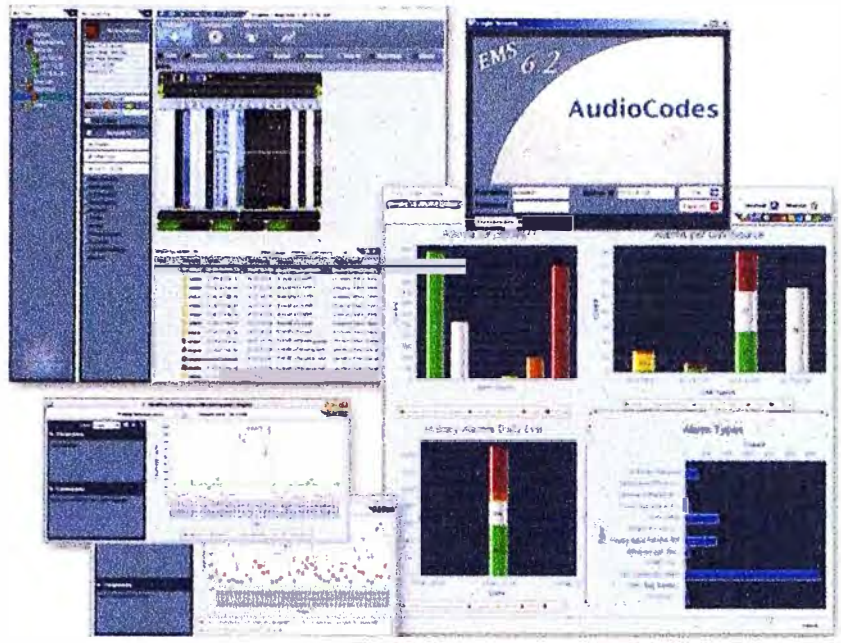


Figura 3.7 Interface grafica del EMS Audiocodes.

Fuente: http://www.audiocodes.com/products/ems

La solución incluye una interfaz atractiva gráfica de usuario (GUI) con herramientas de fácil uso para aumentar la productividad del operador durante la configuración y tareas de aprovisionamiento. Ofrece un acceso intuitivo a la información de estado, así como una rápida navegación a los objetos físicos y lógicos. El cuarto elemento es SBC (Session Border Controllers) como se muestra en la figura 3.8, que representa un componente clave para los proveedores de servicios y empresas que buscan migrar a una infraestructura de voz sobre IP. Este equipo permite la conectividad con otros operadores IP a través de la nube de internet, con la interconexión SIP Trunk, sirve como firewall y permite dar seguridad a la red interna. Presenta gran escalabilidad y eficiencia con varias sesiones concurrentes. Se caracteriza por mantener la calidad del servicio gracias a su gran manejo de códec y su rápida respuesta.

Los clientes pueden migrar de manera segura y transparente de los tradicionales PSTN a SIP Trunking con el SBC, un método rentable de aumentar el valor de la red de datos, al tiempo que protege sus inversiones de equipos de PBX. Además de las interfaces E1/T1, el SBC soporta alta densidad de interfaces PSTN, tales como T3, STM-1 y OC3. Es compatible con una amplia gama de codificadores de voz y tiene la capacidad de transcodificación entre los codificadores de voz de banda estrecha y de banda ancha, incluyendo la normalización de SIP, manejo de fax, control de ganancia y numerosas características adicionales de procesamiento multimedia. El SBC Audiocodes ofrece

interoperabilidad, lo que permite la mediación entre una extensa lista de centrales IP y TDM con proveedores de SIP Trunking.

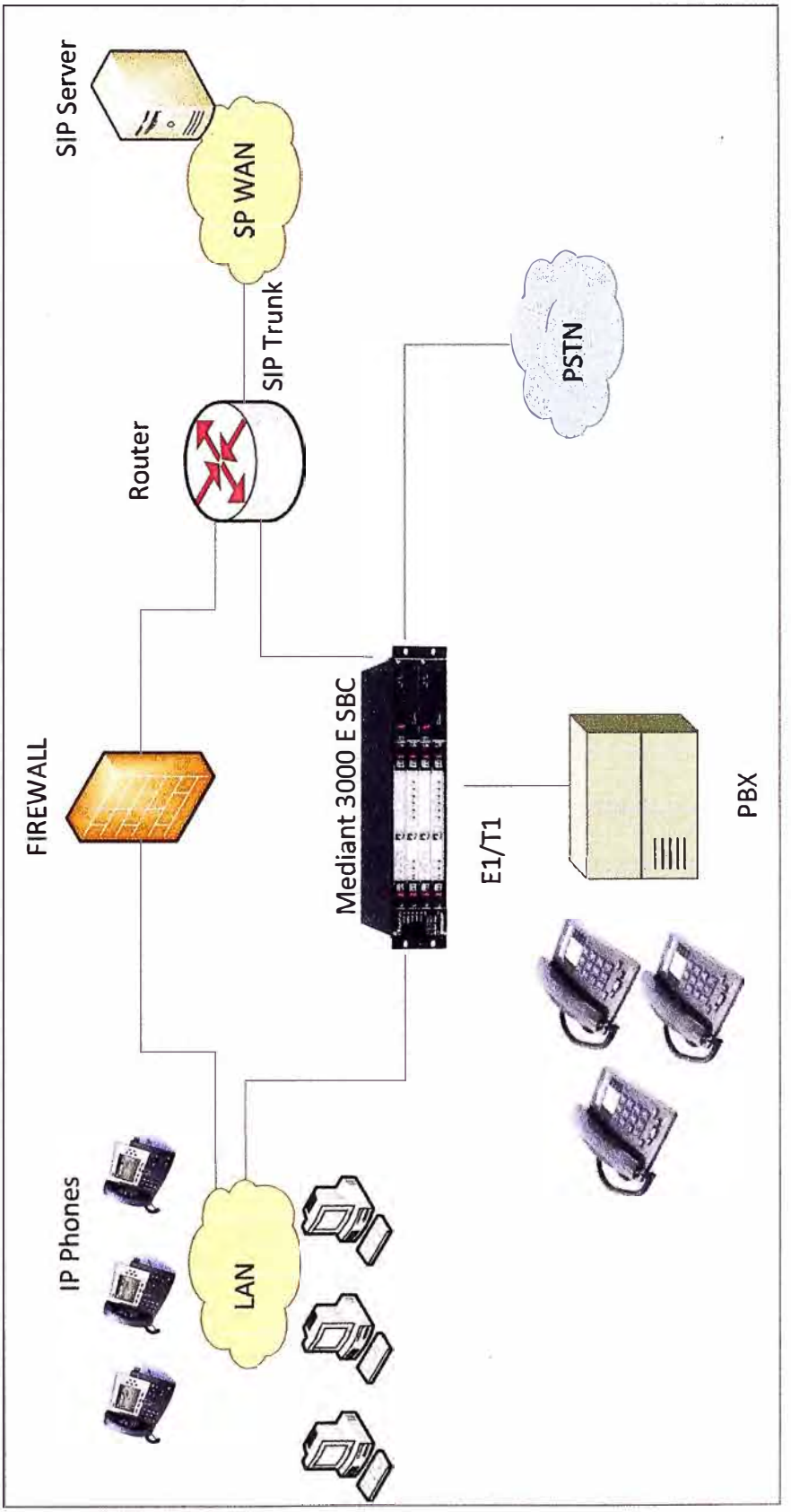


Figura 3.8 Ejemplo de topología en la que trabaja el SBC Audiocodes.

Fuente: http://www.audiocodes.com/products/mediant-3000.

3.3.3 Propuesta Huawei: La solución de integración IMS de Huawei ayuda al despliegue de la red IMS; desplegando rápidamente la red IMS de forma segura y sin problemas, se transforman en la red IMS de la tradicional red PSTN y exploran rápidamente el crecimiento de nuevos servicios IMS. En la figura 3.9 se muestra la topología del softswitch Huawei.

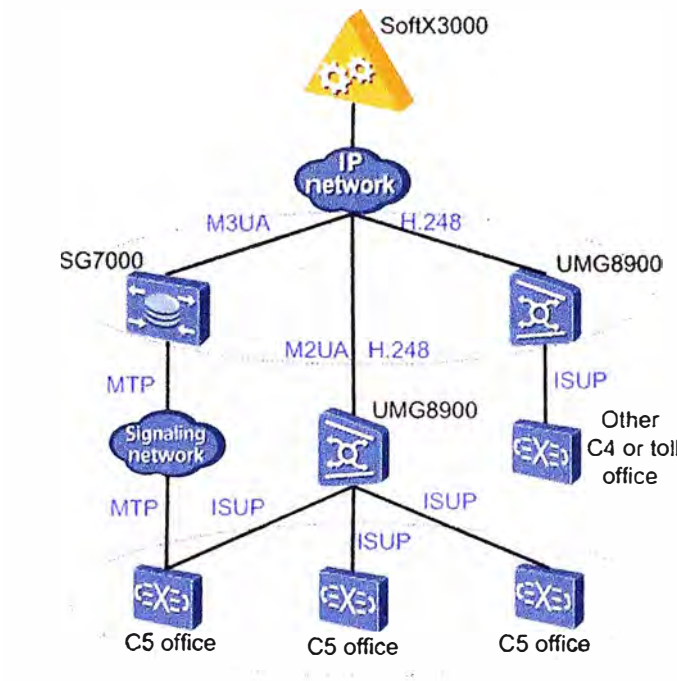


Figura 3.9 Topología de Softswitch de Huawei y UMG 8900 en una red SS7.
Fuente: http://www.huawei.com/en/products/core-network/singlecore/fixed-softswitch.

Como una reconocida arquitectura de núcleo de red para la próxima generación de convergencia fija y móvil (FMC), IMS es independiente del acceso, abierto a las aplicaciones, rica en servicios, y fácil de mantener y desplegar. Por lo tanto IMS puede resolver los problemas anteriores a que se enfrentan los operadores. Los operadores tradicionales sin embargo, están faltos de experiencia en la construcción y despliegue de redes. Por lo tanto, el servicio de integración de Huawei IMS puede conocer exactamente las necesidades del cliente. Para el caso presente Huawei propone su solución basada en 2 equipos, primero el SOFTX3000, que es el componente principal de la red fija. Implementa el control de llamadas y procesamiento de señales y protocolos para proporcionar servicios básicos y servicios suplementarios. También interactúen con el servidor de aplicaciones (AS) para proporcionar diversificados servicios de valor añadido a los abonados, permiten la evolución de la red sin problemas y proteger la inversión de los operadores existentes. También proporciona nuevos servicios, como los servicios

multimedia, servicios de voz sobre IP (VoIP), el mensaje corto (SM), apoyando el trabajo colaborativo a distancia servicios y comunicaciones unificadas sólo dentro de una empresa. Tiene una interfaz abierta y estándar para trabajar con dispositivos fabricados por otras compañías. De manera opcional Huawei ofrece su equipo de gestión N2000 para el monitoreo centralizado del SoftX3000 y del UMG8900.

El SoftX3000, sirve como una oficina de clase 4 (C4), oficina de clase 5 y como oficina de puerta de enlace, procesa diversos tipos de señalización, y proporciona servicios, incluyendo el punto de conmutación de servicio (SSP), listas negras y blancas con gran capacidad, autenticación, carga, e igual acceso. También interactúen con dispositivos de otras redes, como las redes de multiplexación por división de tiempo (TDM), Red, inteligente (IN) de terceros, redes H323/ SIP (sesión iniciación de protocolos), las redes móviles públicas (PLMN), Redes IMS (IP multimedia Subsystem), redes de acceso inalámbrico CDMA (acceso múltiple por división de código) y redes hibridas de fibra coaxial (HFC).

El segundo componente es el UMG8900 proporciona la conversión TDM-IP, permite el interfuncionamiento entre redes diferentes, y procesa los formatos de servicios de streaming. También se puede utilizar en la red NGN para proporcionar funciones de Gateway de señalización (SG) y Gateway de conmutación, los operadores pueden beneficiarse de un bajo costo, orientada hacia el futuro de la red de telecomunicaciones móviles.

CAPÍTULO IV.
INGENIERÍA DEL PROYECTO

4.1 Concepto Básico de la Solución.

En un sistema de telefonía IP el término "Softswitch" engloba los procesos y elementos informáticos que controlan las sesiones, el medio (voz, video o mensajes) y los servicios. En términos sencillos, el Softswitch separa los elementos de la red (Hardware) del control de la misma (Software). Recordemos que en la telefonía TDM tradicional el hardware y software no pueden estar completamente separados. Las redes de conmutación de circuitos están diseñadas para comunicaciones telefónicas y se construyen con elementos (HW + SW) dedicados específicamente a determinadas funciones, mientras que en las redes modernas de conmutación de paquetes con el protocolo IP, se puede comunicar voz, datos e imágenes con dispositivos completamente genéricos, capaces de comunicar los diferentes medios. Estos dispositivos se controlan por el software que conforma el Softswitch.

El Softswitch está compuesto por uno o varios ordenadores que controlan el tráfico de VoIP e incluso las pasarelas entre el STDP y la VoIP en cuyo caso enlazan ambos tipos de red y gestionan el tráfico, que en el caso más general puede estar formado por una combinación de voz, fax, datos y video. Los Softswitches también se ocupan de que la señal se procese, en función del tipo de medio que sea, se negocie que tipo de codec se utilizará en cada sesión, o incluso se trans-codifique de un codec a otro.

Los softswitches están en el lado IP de las redes y se basan en el Protocolo SIP, Session Initiation Protocol, o en el Protocolo H.323. Las Redes de Nueva Generación, (NGN) emplean Softswitches basados en IMS.

No obstante lo anterior, la razón del softswitch no es solamente para separar el hardware del software, sino que pretende que haya un entorno abierto de software que facilite la creación de servicios. Se da por supuesto que las Redes Inteligentes del futuro no seguirán los modelos tradicionales de control de llamadas, que por proceder de la telefonía tradicional están limitados, y en su lugar empleará modelos basados en sesiones, capaces de comunicar datos, voz y servicios multimedia. También es preciso señalar que un softswitch se puede entender como que es una fórmula centralizada (que cubre zonas o

regiones geográficas) propia de una compañía telefónica, y que las empresas mas pequeñas e ISPs generalmente no prestan sus servicios de telefonía IP mediante un softswitch, puesto que puede que prefieran emplear arquitecturas más sencillas del tipo peer-to-peer y componentes individualizados, de diferentes fabricantes o procedencias.

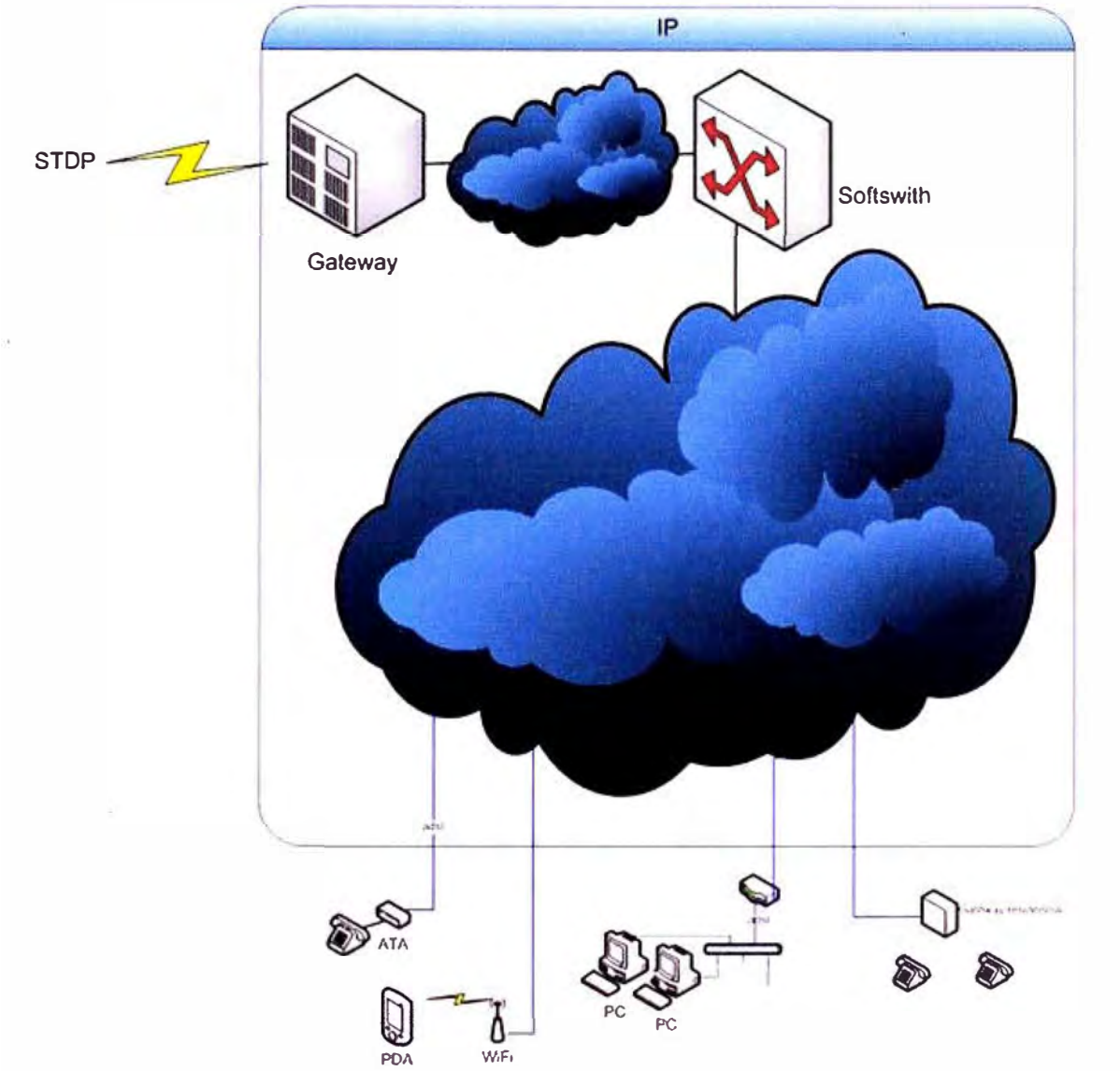


Figura 4.1. Arquitectura de Softswitch.

Fuente: http://es.scribd.com/doc/137562734/53995502-Soft-Switch.

En redes IP en las que haya control sobre la calidad de servicio (mediante MPLS o IMS) la arquitectura Softswitch puede presentar ventajas. Incluso un operador puede emplear esta arquitectura para interconectar Softswitches entre sí.

Los Softswitches (o elementos especializados con otro nombre) localizan y registran a los usuarios, dialogan, al nivel más bajo, con los dispositivos de acceso al usuario, como terminales SIP o pequeños Gateway, donde se inician y terminan las comunicaciones.

Controlan las pasarelas especializadas y los "Media Servers" que ofrecen locuciones, ponen a varios usuarios en conferencia, y consiguen que los medios atraviesen los Firewalls y NATs. También se ocupan de gestionar el mapeo de números telefónicos (ENUM) e incluso pueden usar dicha técnica para solucionar la portabilidad de número. ENUM es el proceso de unificación del sistema de numeración telefónico de la PSTN con las direcciones de internet, en síntesis, es un conjunto de protocolos para convertir números E.164 en URIs, y viceversa, de modo que el sistema de numeración E.164 tenga una función de correspondencia con las direcciones URI en Internet.

Y a un nivel más alto proporcionan servicios diversos, tanto al usuario como, por ejemplo, con servicios de presencia y relevancia de llamadas, como al operador (back office y OSS). Unos fabricantes engloban todos los conceptos de software bajo la denominación genérica de Softswitch, mientras que otros instalan dos o tres de las funciones en un ordenador profesional y le dan otro nombre. Los fabricantes y compañías de servicios informáticos más pequeñas o especializadas ponen las funciones que se deseen tener en ordenadores dedicados. Hay que tener en cuenta que gran parte del software basado en SIP es de dominio público.

4.2 Especificaciones Técnicas del Equipamiento.

4.2.1 SoftX3000

La arquitectura de software del SoftX3000 esta basada en la plataforma de Arquitectura Distribuida Orientada a Objetos Programable en Tiempo Real (DOPRA) de HUAWEI. Esta plataforma provee mecanismos para la realización de funciones de operación y mantenimiento, gestión de alarmas, medición de tráfico, seguimiento de llamadas/señalización, conmutación de protección de tarjetas, y otras funciones. A continuación se describen los principales subsistemas de la arquitectura de software del SoftX3000.

a. El subsistema de soporte de software: provee mecanismos para la realización de funciones de operación y mantenimiento, gestión de alarmas, medición de tráfico, seguimiento de llamadas/señalización, respaldo de datos, conmutación de protección de tarjetas, carga en línea y otras funciones.

b. El subsistema de base de datos: provee una plataforma centralizada para la gestión de bases de datos que administra toda la información requerida para la operación del sistema, incluyendo datos de hardware, datos de protocolos, datos de enrutamiento y datos de servicios. Este subsistema provee mensajes o APIs para el subsistema de

procesamiento de servicios, el subsistema de procesamiento de señalización y el subsistema de control de Media Gateway (MGW), usados para consultas, adición, remoción y otras operaciones.

c. **El subsistema de procesamiento de señalización:** es responsable de la implementación del transporte y el procesamiento de varios protocolos de señalización, tales como SS7, señalización de control de llamadas, protocolos de transporte de señalización y protocolos de enrutamiento de red.

d. **El subsistema de control de Media Gateway:** se utiliza para la gestión y el mantenimiento de los dispositivos MGW, así como para la gestión y el mantenimiento de los recursos de transporte en los dispositivos MGW.

e. **El subsistema de procesamiento de servicios:** se utiliza para implementar la variedad de servicios provistos por el SoftX300, tales como servicios básicos de voz, servicios suplementarios, servicios IP Centrex y servicios multimedia.

f. **El subsistema de servicios de terceros:** provee la interfase para la interacción con los servidores de aplicación de HUAWEI o de otros proveedores para la implementación de servicios avanzados.

g. **El subsistema de gestión (NMS):** es implementado por el servidor BAM y provee las interfaces necesarias para la gestión local y remota del sistema.

h. **El subsistema de tarifación:** es implementado por el servidor iGWB y se encarga del almacenaje temporal y la transferencia de la información de tarifación.

4.2.2 UMG8900

El universal media Gateway (UMG) es el segundo elemento que forma parte de la red NGN de Huawei, es un equipo que hace la transición entre la red TDM y el mundo IP. La estructura del UMG8900 cuenta con un bus TDM y un bus de datos en un mismo backplane. Además, el UMG8900 cuenta con una matriz de conmutación TDM de 256Kx256K y con una matriz de conmutación de paquetes de 128Gbit/s. Estas características le permiten interconectar redes PSTN existentes con la redes de conmutación de paquetes NGN, así como realizar el transporte y procesamiento de servicios TDM y NGN. Las tarjetas TNU trabajan en configuración de redundancia 1+1 y proveen la matriz de conmutación TDM. Las tarjetas NET trabajan en configuración de redundancia 1+1 y proveen la matriz de conmutación de paquetes. Las tarjetas OMU trabajan en configuración de redundancia 1+1 y se encargan de las funciones de gestión y mantenimiento del sistema.

La arquitectura de software del UMG8900 está también basada en la plataforma DOPRA de HUAWEI. El control de la operación del UMG8900 lo realiza el softswitch SoftX3000. El UMG8900 proporciona las interfases PDH/SDH para interconexión con la red PSTN y las interfases IP para conexión con la red NGN. Internamente cuenta con la funcionalidad de poder realizar la conmutación de tráfico TDM y de paquetes. Adicionalmente, el UMG89000 esta en capacidad de proveer directamente la señalización R2, numero 5 y también la señalización SS7 hacia la red PSTN y la señalización SIP/H.323, hacia la red IP.

4.2.3 N2000

El N2000 es un servidor que forma parte opcional de la red NGN de Huawei, este equipo se encarga de centralizar las alarmas del SOFTX3000 y del UMG8900. La solución NGN de HUAWEI proporciona el sistema de gestión de red integrada IManager N2000. Tomando como base el hardware SUN Solaris, IManager N2000 puede proporcionar una gestión unificada en todos los equipos de la red NGN. El Centro de Monitoreo del IManager N2000 ofrece un sistema de gestión de red integrada y un sistema de gestión de red de capa superior, proporciona funciones de centralización para la gestión de toda la red fija. Monitorea los recursos de la NGN de HUAWEI, incluyendo los recursos del dispositivo y los recursos de servicio. El IManager N2000 puede soportar dos tipos de configuración de red, es decir, en banda y fuera de banda. El modo fuera de banda se utiliza para la protección de los enlaces de gestión de red de SoftX3000 y UMG8900 mientras que el modo en banda podría reducir el costo de instalación de la red de gestión.
En lo que respecta a la capacidad de gestión, el IManager N2000 puede ampliar la capacidad de gestión mediante el uso de más servidores en caso que el sistema esté siendo ampliado y que los servidores existentes no sean suficientes.

4.3 Programa de la Implementación del Sistema.

Aquí se indica la metodología usada para realizar la migración del centro de conmutación de circuitos hacia el centro de conmutación de paquetes, lo cual pretende ser una guía de referencia para realizar trabajos semejantes en otras empresas de telecomunicaciones que requieran cambiar sus antiguas plataformas de telefonía.

4.3.1 Levantamiento de la información

Se realiza una recopilación de los enlaces y operadores externos conectados hacia la central Italtel, así como el tipo de señalización presente en cada uno, también se recolectara

enlaces que presentan señalización del tipo internacional, y en la figura 4.3 los enlaces del tipo nacional. También se muestra un grafico más especificado de los enlaces con Telefónica del Perú en cada departamento, figura 4.4 ya que estos manejan STP con las centrales de Lima (Washington y San Isidro).

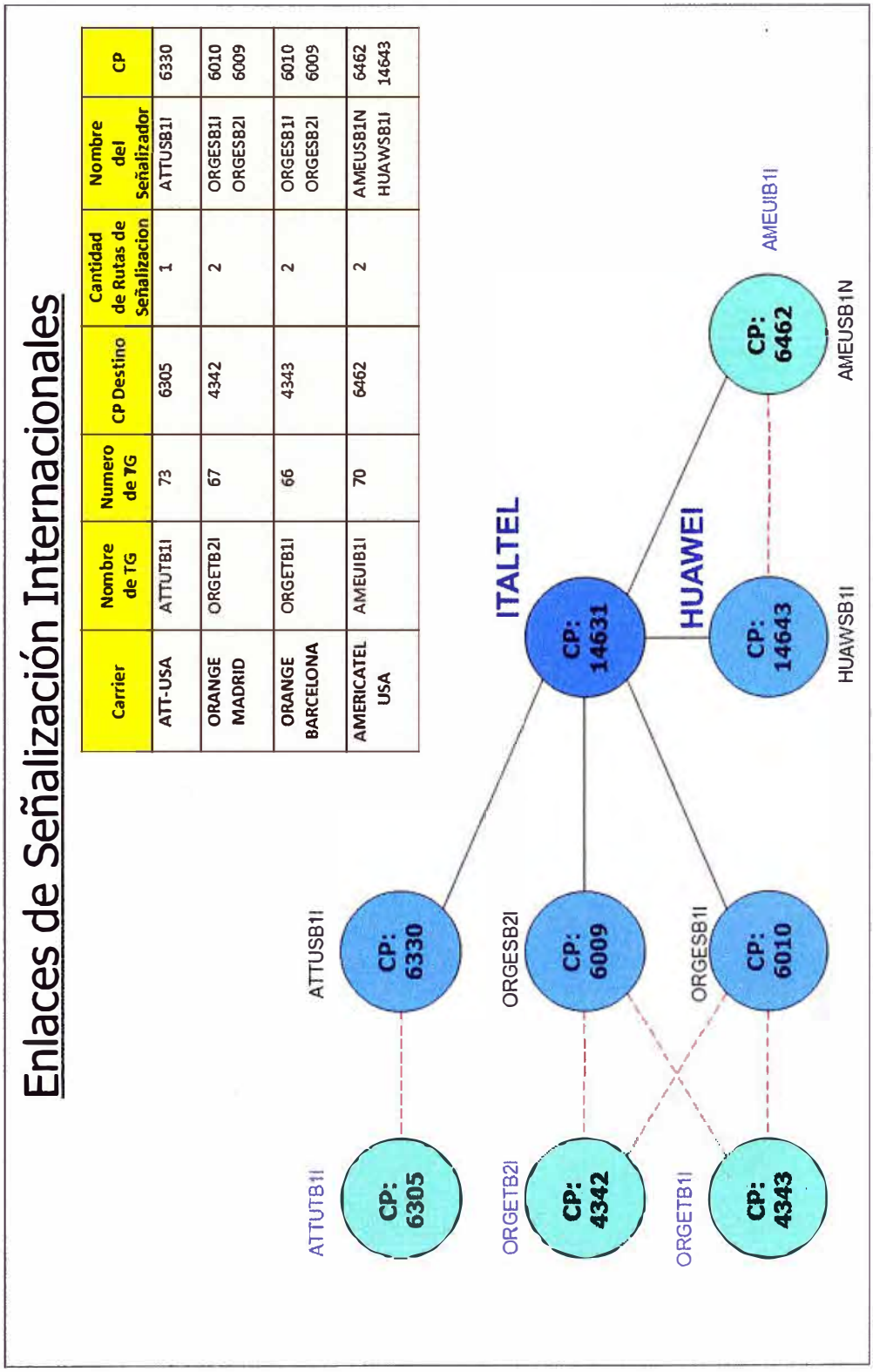


Figura 4.2 Enlaces del tipo Internacional.

Fuente: Elaboración propia, Empresa: Americatel Perú SA.

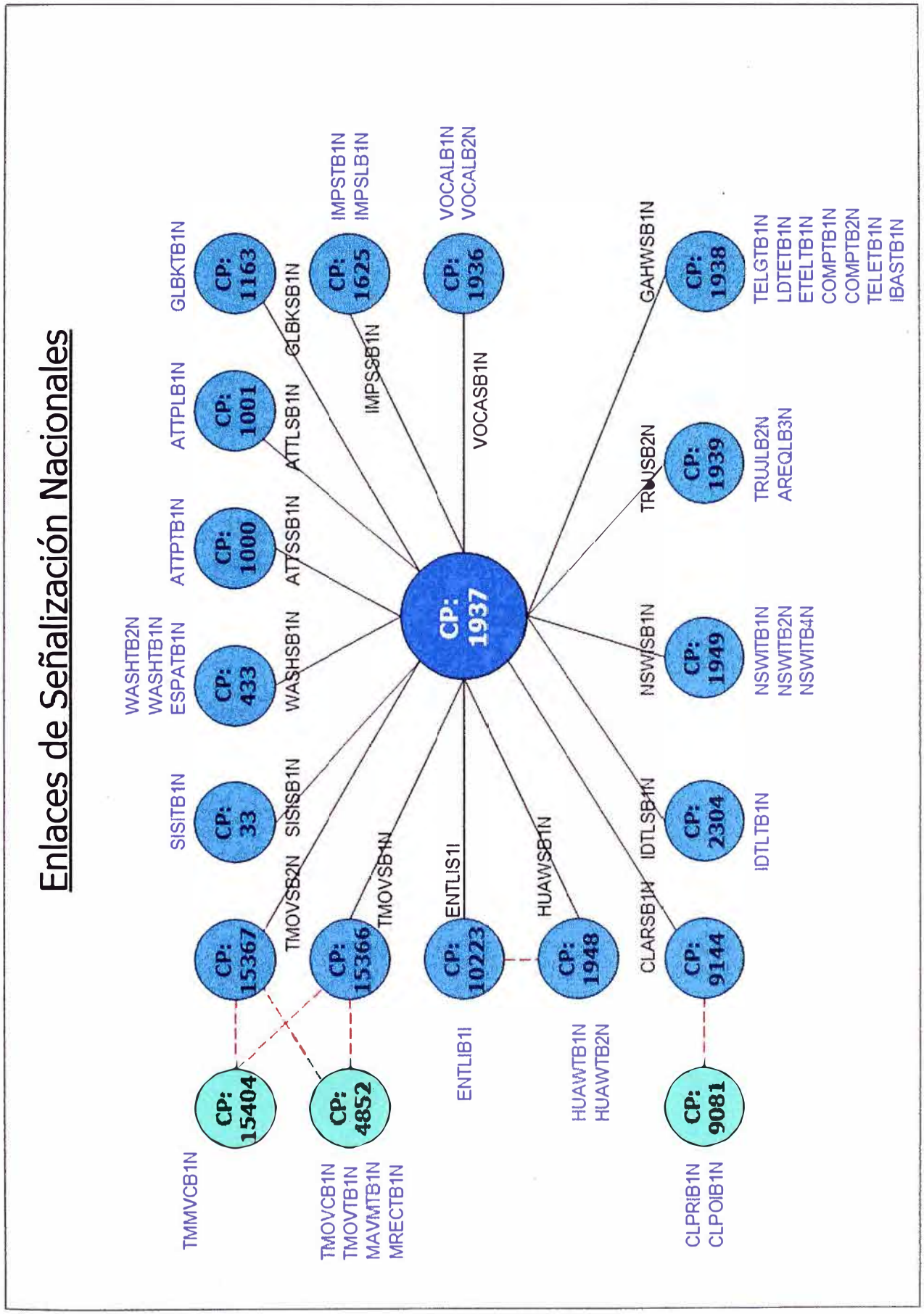


Figura 4.3 Enlaces del tipo Nacional.

Fuente: Elaboración propia, Empresa: Americatel Perú SA.

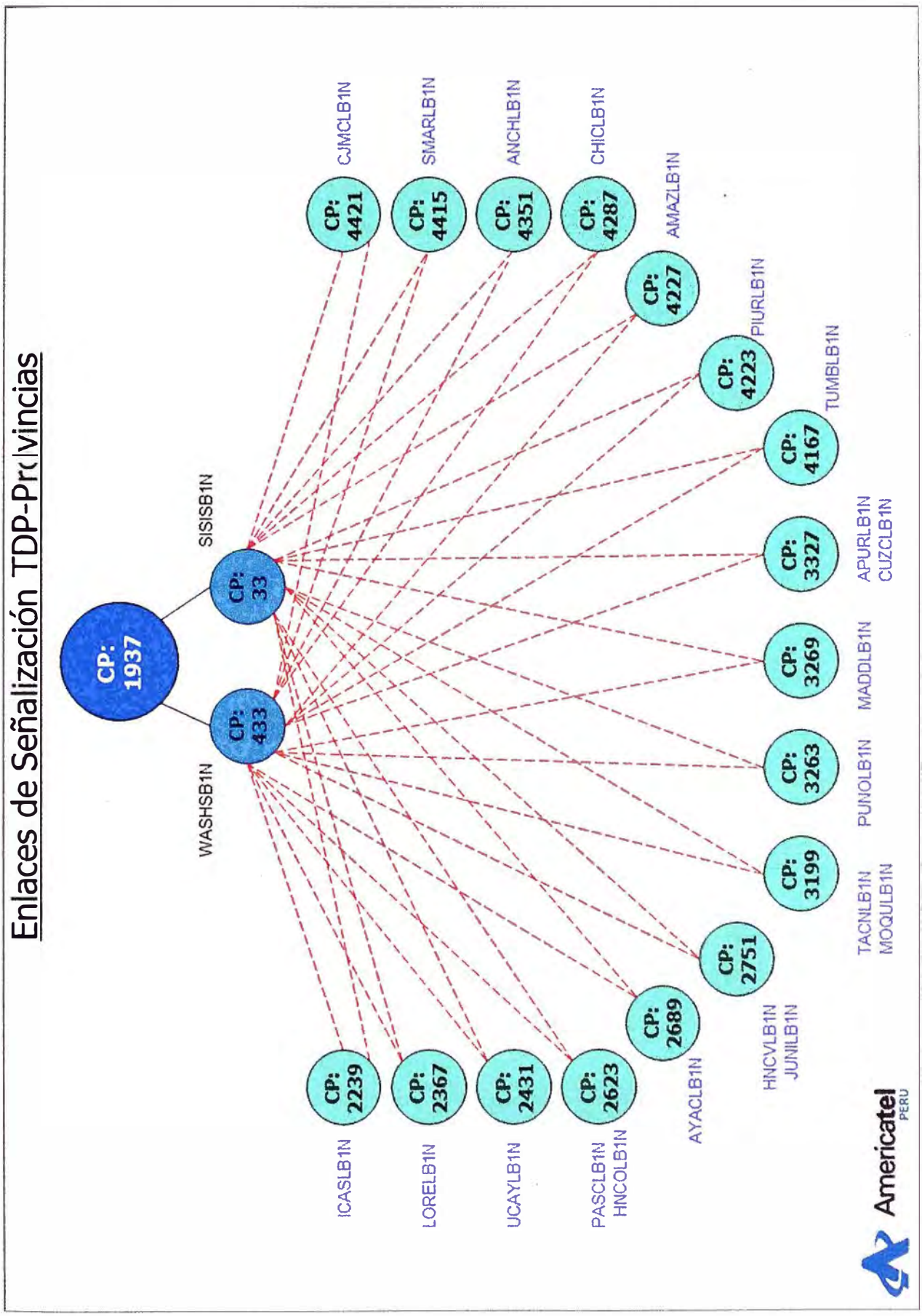


Figura 4.4 Enlaces de Provincias con Telefónica.

Fuente: Elaboración propia, Empresa: Americatel Perú SA.

4.3.2 Ingeniería propuesta

Se realiza el estudio de la red para poder dimensionar los equipos del core que soporten el nuevo trafico IP de los equipos nuevos que se instalaran, se hace necesario colocar nuevos equipos de ruteo y de concentración así como nuevas conexiones de las PCs de gestión y monitoreo. Se prepara los acondicionamientos necesarios para los equipos nuevos a instalar. En las figuras 4.5, 4.6 y 4.7 se muestra la instalación del cableado necesario para la interconexión de los equipos UMG8900, SOFT3000 y N2000 con la red de Americatel.

La conexión del Softswitch debe estar basada en la recomendación del fabricante en cuanto a interfaces y topología utilizada para la inserción del mismo a la red, es recomendable que éste sea soportado por una arquitectura redundante que ofrezca robustez a la solución.

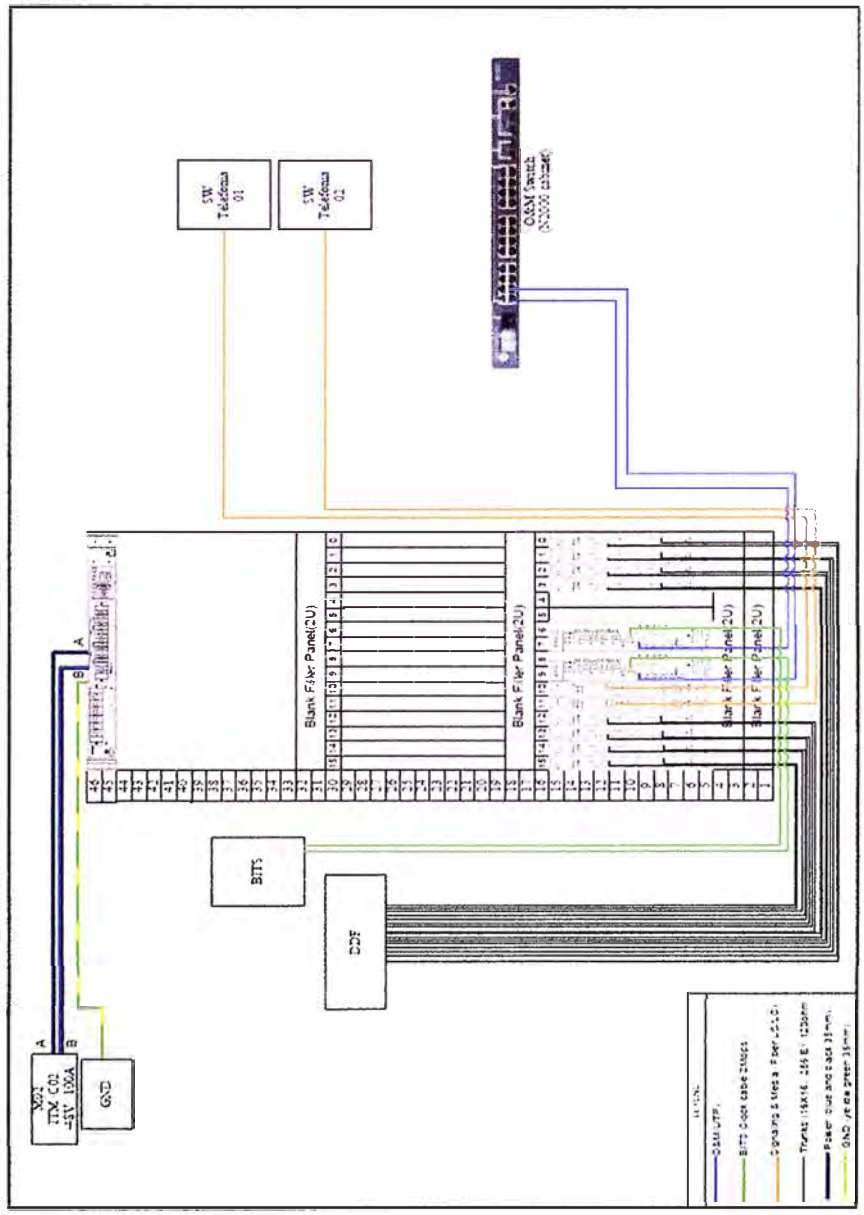


Figura 4.5 Diagrama de conexión del UMG8900.

Fuente: Americatel Perú, Area de Ing. De Trafico, Diagramas Proyecto Softswitch.

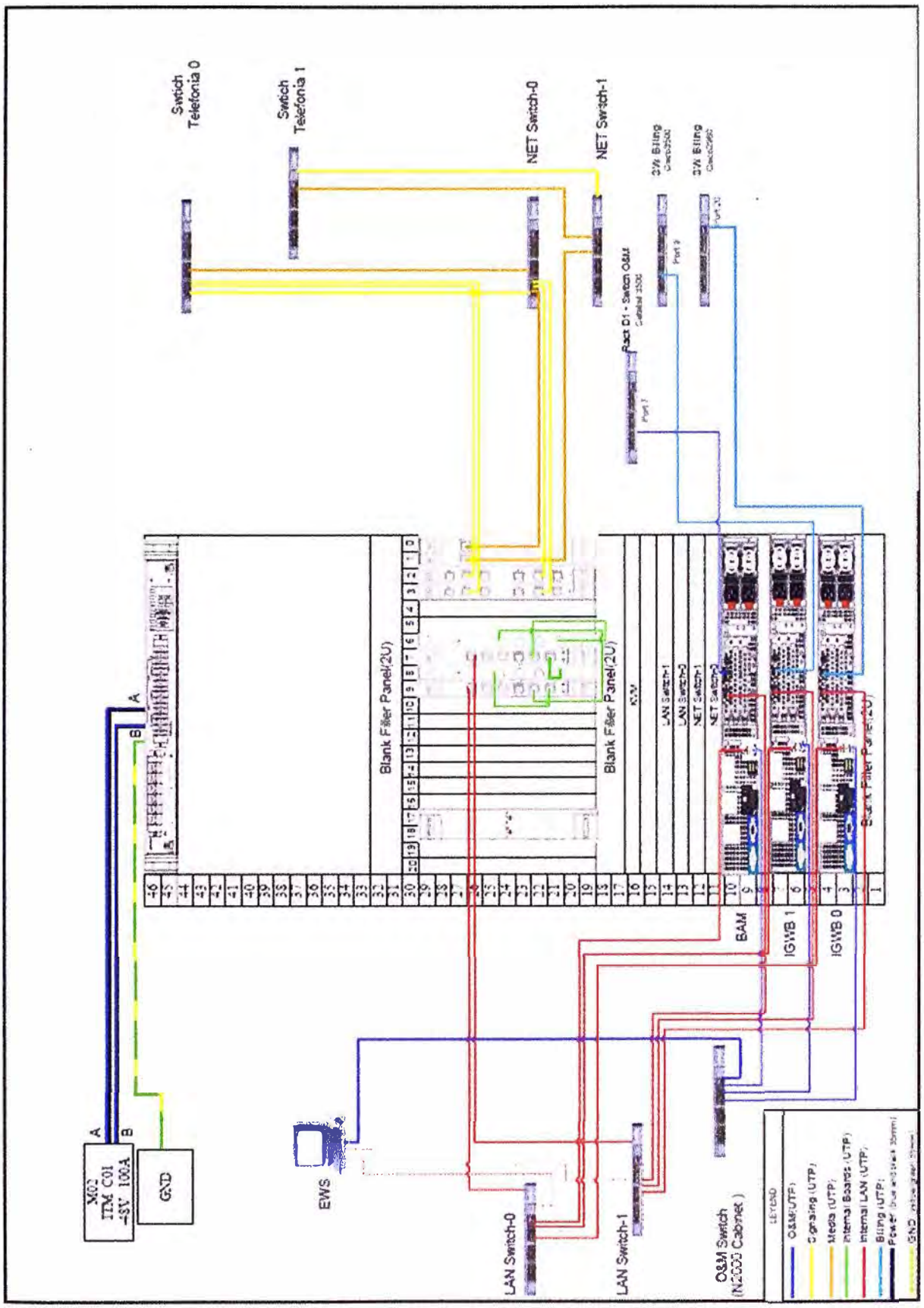


Figura 4.6 Diagrama de conexión del SOFTX3000.

Fuente: Americatel Perú, Area de Ing. De Trafico, Diagramas Proyecto Softswitch.

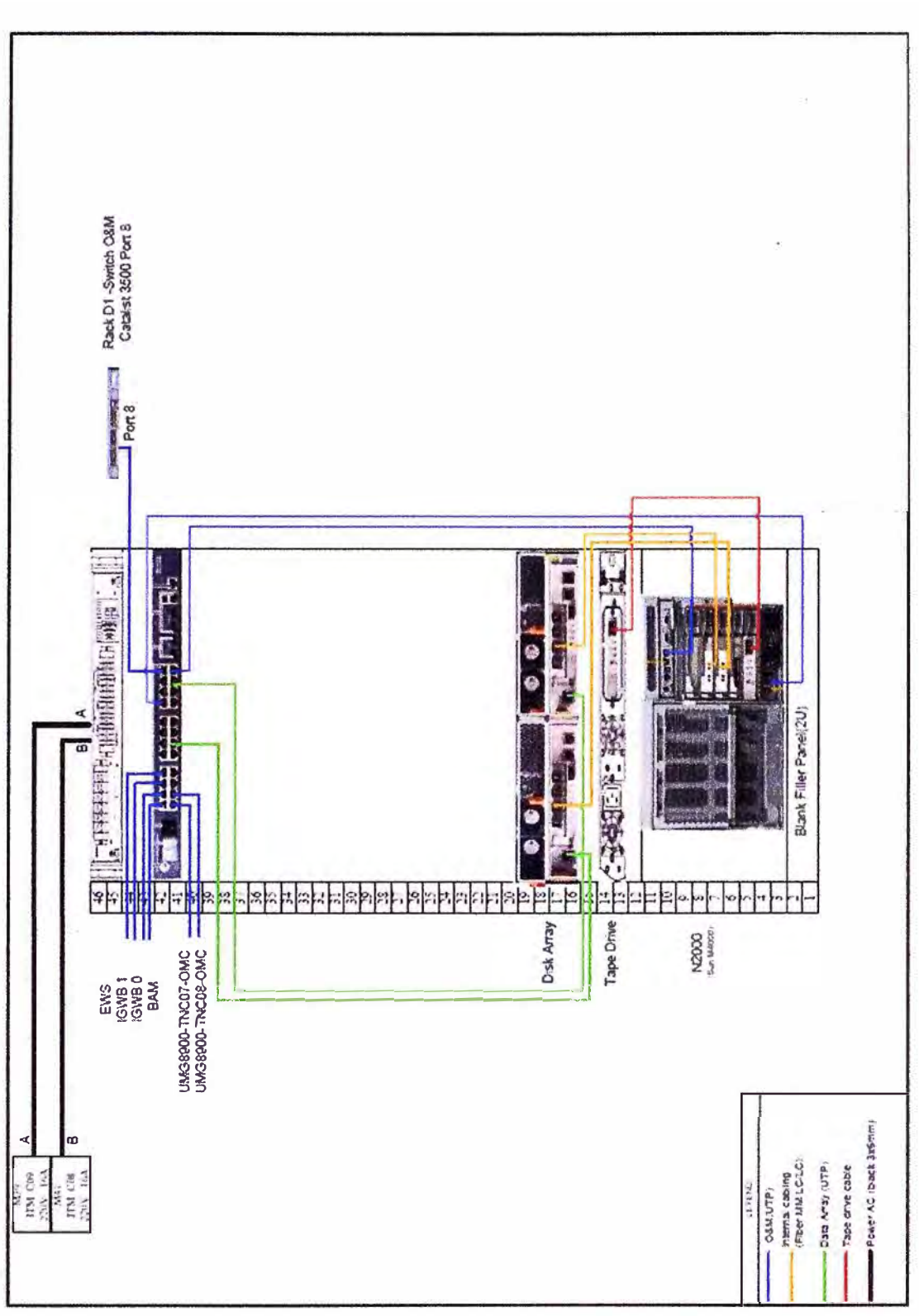


Figura 4.7 Diagrama de conexión del N2000.

Fuente: Americatel Perú, Area de Ing. De Trafico, Diagramas Proyecto Softswitch.

4.3.3 Protocolos de pruebas

Para asegurar una correcta implementación de la solución de VoIP, garantizar la interoperabilidad, el correcto funcionamiento de los equipos y asegurar que el

equipamiento adquirido se adapte a los requerimientos técnicos de la Empresa y cumpla con todas las especificaciones y capacidades que ofrece, es recomendable desarrollar e implementar un protocolo de pruebas que dé soporte a lo anteriormente señalado y en un escenario que se ajuste en lo posible al ambiente más cercano al de producción que tendrá la solución. El protocolo debe aplicarse a la mayor cantidad de aspectos que puedan afectar de manera directa el funcionamiento de la red, como pruebas de fiabilidad de los equipos, las cuales permiten comprobar el funcionamiento del hardware y la redundancia de éste, pruebas de estrés y de ataque de negación de servicio, con las que se pueden llevar los equipos al límite y simular una situación de alta carga o ataques al equipo y pruebas de calidad de servicio como niveles de jitter, delay, packet loss y MOS. De igual forma son de importancia pruebas de gestión como creación y generación de alarmas, configuración y respaldo. Se prepararon un proceso de pruebas de aceptación del funcionamiento de los equipos y realización del mismo. En el anexo C se tiene un resumen del listado de pruebas realizadas y los detalles de las pruebas se encuentran en el anexo B.

4.3.4 Migración de las rutas LDN y LDI TDM a IP

Al culminar la implementación y pruebas de los equipos se continuara con la migración de las rutas presentes en el sistema de telefonía TDM de la central Italtel. Con el uso del estudio realizado en el levantamiento de información, se hace posible diseñar un plan de migración que sea ejecutado de manera gradual y transparente de forma que impacte lo menor posible y no produzca paradas del servicio. En la figura 4.8 se muestra el diagrama de la red actual del operador Americatel y en la figura 4.9 se muestra como quedará luego de la migración. Para que tanto los operadores de larga distancia nacional e internacional no se vean afectados en esta transición se realizo la migración usando una topología tipo espejo, es decir reutilizando los códigos de puntos de los distintos operadores y configurándolos en el Softswitch en un lado, y de cara a los otros operados se configura los mismos códigos de puntos nacionales e internacionales de la central Italtel. No será necesario realizar ajustes de datos en al red PSTN y soportara la actualización sin problemas. Para el caso de los multiples puntos de señalización como se muestra en la figura 4.10, el X es el punto de señalización de la central Italtel, el Y es el punto de señalización del dispositivo STP y A es el punto de señalización del operador nacional o internacional, todos ellos están configurados como puntos de señalización en el softswitch. UN circuito de señalización es establecido entre X y el dispositivo STP, y también entre Y y C4. No hay cambios requeridos en los equipos C4, dispositivo STP y operador final.

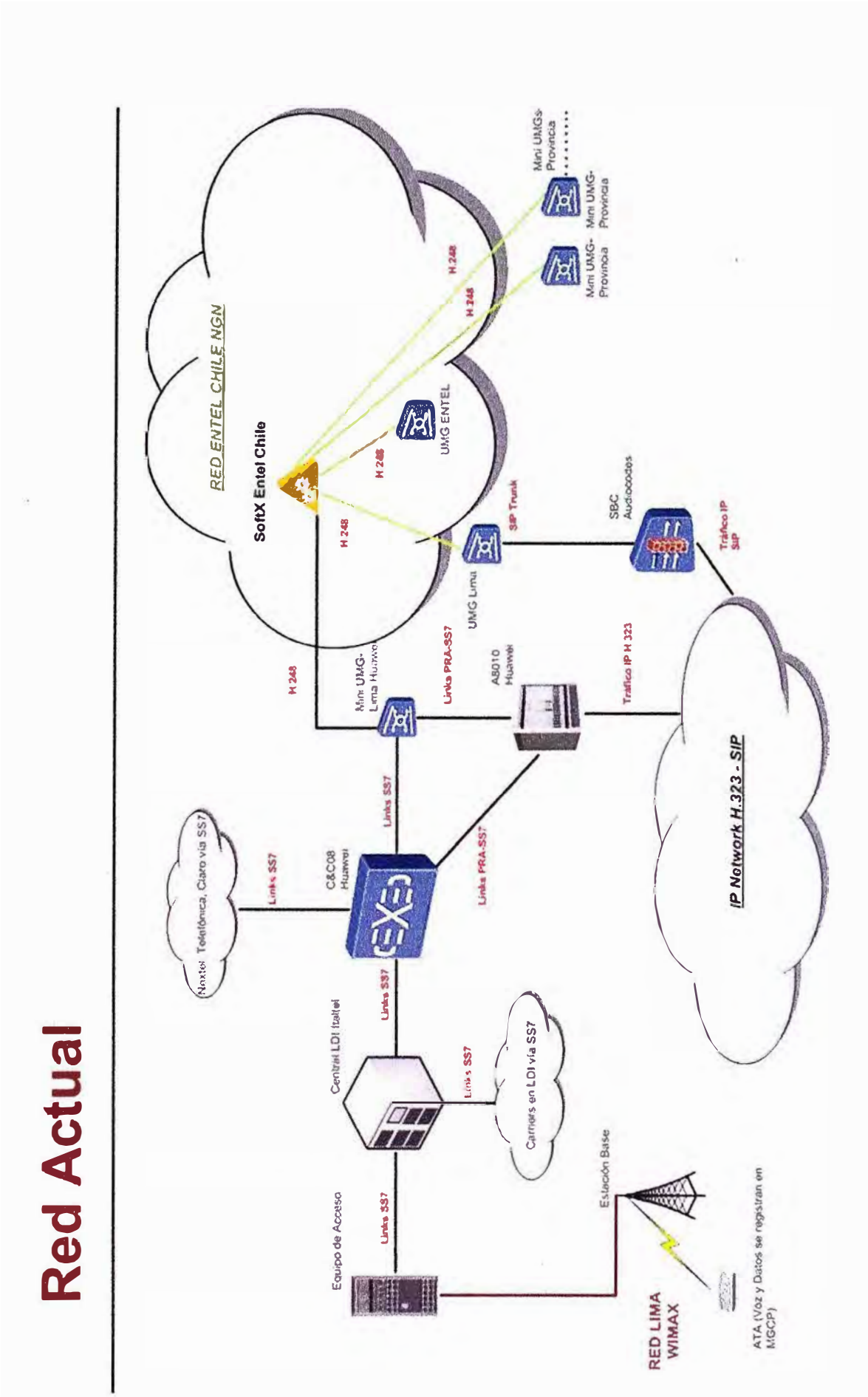


Figura 4.8. Topología de Red antes de la migración.

Fuente: Americatel Perú, Área de Ing. De Trafico, Diagramas Proyecto Softswitch.

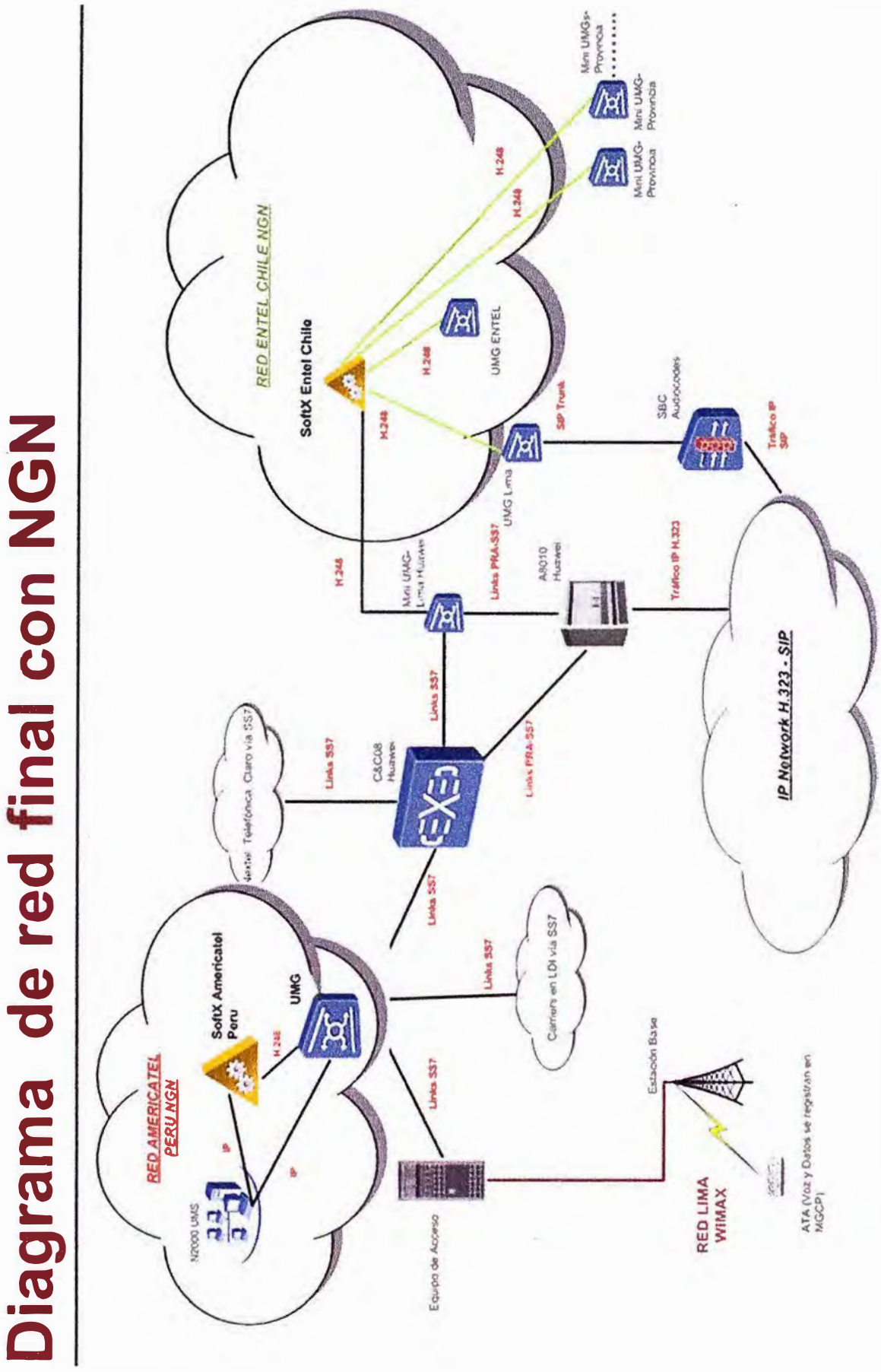


Figura 4.9. Topología de Red luego de la migración.

Fuente: Americatel Perú, Área de Ing. De Trafico, Diagramas Proyecto Softswitch.

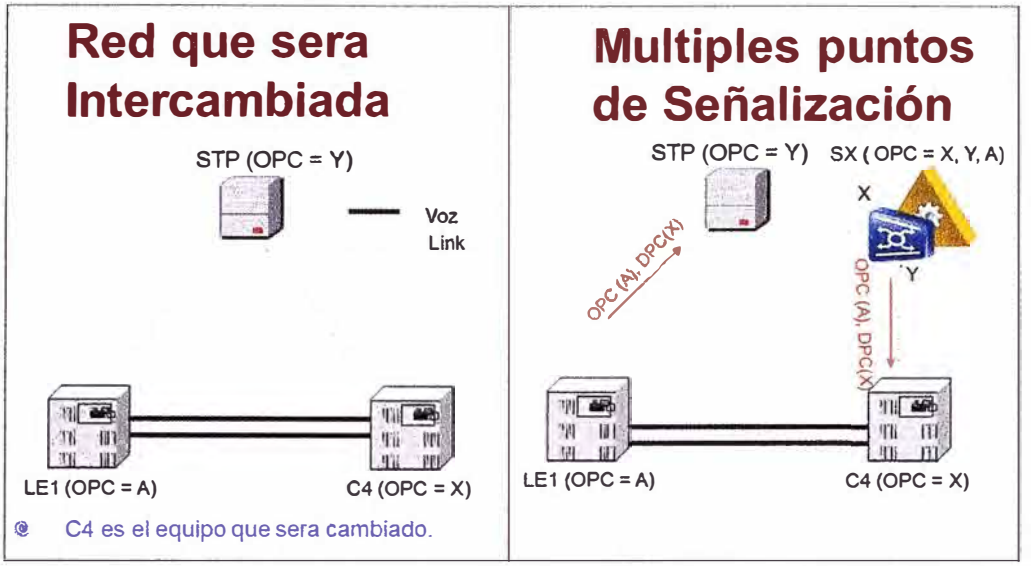


Figura 4.10 Diagrama de la solución que usa múltiples puntos de señalización.
Fuente: Americatel Perú, Área de Ing. De Trafico, Diagramas Proyecto Softswitch.

A continuación se ilustra en la figura 4.11 la migración de un enlace del operador Entel:

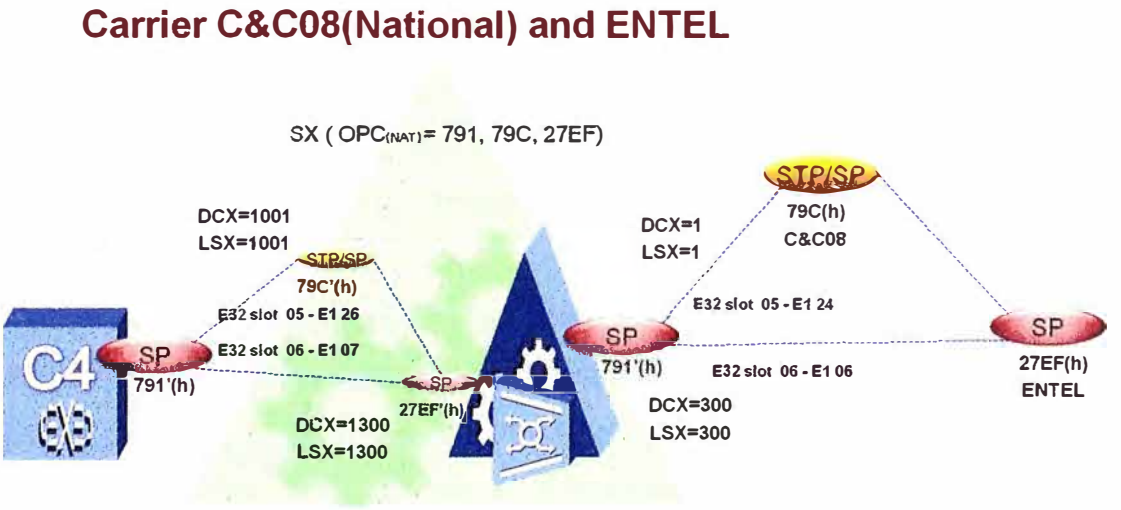


Figura 4.11 Escenario de migración del operador ENTEL con Softswitch en medio.
Fuente: Americatel Perú, Area de Ing. De Trafico, Diagramas Proyecto Softswitch.

La preparación del guion de comandos es de la siguiente forma:

a. Configuración de la parte MTP del UMG

ADD MTP2LNK: LNKNO=1, LNKNAME="HUAWEI_CC08-NAT_L1", IFBT=E32, IFBN=5, E1T1N=24, STRTTS=16, SPFBN=0, SUBBN=0, LNKTYPE=M2UA64K, LKS=0, BINIFID=1;

ADD MTP2LNK: LNKNO=23, LNKNAME="ENTEL_L1", IFBT=E32, IFBN=6, E1T1N=6, STRTTS=1, SPFBN=0, SUBBN=1, LNKTYPE=M2UA64K, LKS=0, BINIFID=300;

ADD MTP2LNK: LNKNO=101, LNKNAME="ITA_CC08-NAT_L1", IFBT=E32, IFBN=5, E1T1N=26, STRTTS=16, SPFBN=1, SUBBN=1, LNKTYPE=M2UA64K, LKS=1, BINIFID=1001;

ADD MTP2LNK: LNKNO=123, LNKNAME="ITA_ENTEL_L1", IFBT=E32, IFBN=6, E1T1N=7, STRTTS=1, SPFBN=1, SUBBN=0, LNKTYPE=M2UA64K, LKS=1, BINIFID=1300;

b. Configuración principal hacia el carrier desde el SoftX3000 con SPC 791

ADD N7DSP: DPX=1, NI=NAT, DPC="79C", OPC="791", DPNAME="HUAWEI_CC08-NAT", STPF=YES, ADJF=YES, SLSSM=B1111, PRT=ITU;

ADD N7DSP: DPX=300, NI=NAT, DPC="27EF", OPC="791", DPNAME="ENTEL", STPF=NO, ADJF=YES, SLSSM=B1111, PRT=ITU;

ADD N7LKS: LSX=1, ASPX=1, LSNAME="HUAWEI_CC08-NAT", SLSM=B1111;

ADD N7LKS: LSX=300, ASPX=300, LSNAME="ENTEL", SLSM=B1111;

ADD N7LNK: MN=136, LNKN=0, LNKNAME="HUAWEI_CC08-NAT_LNK1", LNKTYPE=M64K, M2LSX=0, BINIFID=1, LSX=1, SLC=0, SLCS=0, PRI=0, TID=5904;

ADD N7LNK: MN=136, LNKN=22, LNKNAME="ENTEL_LNK1", LNKTYPE=M64K, M2LSX=0, BINIFID=300, LSX=300, SLC=1, SLCS=1, PRI=0, TID=6337;

ADD N7RT: LSX=1, DPX=1, PRI=0, RTNAME="HUAWEI_CC08-NAT";

ADD N7RT: LSX=300, DPX=300, PRI=0, RTNAME="ENTEL_1";

ADD N7RT: LSX=1, DPX=300, PRI=0, RTNAME="ENTEL_2";

c. Configuración hacia la ITALTEL-SoftX3000 as OPC= (791, 79C, 27EF)'(h)

ADD OFI: IDX=1, NI=NN, OPC="00079C", MSTYPE=MASTER;

ADD OFI: IDX=39, NI=NN, OPC="0027EF", MSTYPE=MASTER;

MOD OFI: IDX=39, PA1=NN, PAC1="00079C", NI=NN, OPC="0027EF", CONFIRM=Y;

ADD N7DSP: DPX=1001, NI=NAT, DPC="791", OPC="79C", DPNAME="ITA_HUAWEI_CC08-NAT", STPF=NO, ADJF=YES, SLSSM=B1111, PRT=ITU;

ADD N7DSP: DPX=1300, NI=NAT, DPC="791", OPC="27EF", DPNAME="ITA ENTEL", STPF=NO, ADJF=YES, SLSSM=B1111, PRT=ITU;

ADD N7LKS: LSX=1001, ASPX=1001, LSNAME="ITA_HUAWEI_CC08-NAT", SLSM=B1111;

ADD N7LKS: LSX=1300, ASPX=1300, LSNAME="ITA_ENTEL", SLSM=B1111;

ADD N7LNK: MN=137, LNKN=0, LNKNAME="ITA_HUAWEI_CC08-NAT_LNK1", LNKTYPE=M64K, M2LSX=1, BINIFID=1001, LSX=1001, SLC=0, SLCS=0, PRI=0, TID=5957;

ADD N7LNK: MN=137, LNKN=22, LNKNAME="ITA_ENTEL_LNK1", LNKTYPE=M64K, M2LSX=1, BINIFID=1300, LSX=1300, SLC=1, SLCS=1, PRI=0, TID=6369;

ADD N7RT: LSX=1001, DPX=1001, PRI=0, RTNAME="ITA_HUAWEI_CC08-NAT";

ADD N7RT: LSX=1300, DPX=1300, PRI=0, RTNAME="ITA_ENTEL_1";

d. Trasmisión transparente de la señalización en el SOFTX3000

ADD OCISUP: OPC="0027EF", DPC="000791", NI=INT, SCIC=0, ECID=1087, TOPC="00079C";

ADD OCISUP: OPC="000791", DPC="0027EF", NI=INT, SCIC=0, ECID=1087, TOPC="000791";

4.4 Recomendación Para la Implementación del Softswitch Huawei.

Seguir las normas EIA/TIA de cableado estructurado, manejo de fibra óptica, implementación de centros e gestión, para garantizar de esta manera servicios de calidad.

Se recomienda tener diagramas actualizados de la red de telefonía como también los servicios soportados por cada plataforma. A fin de poder realizar una migración que no afecte la falla o falta de algún servicio.

Se recomienda realizar una capacitación básica de todo personal que interviene en algún proceso de implementación de la nueva plataforma. También una capacitación más profunda y especializada del personal encargado de la operación y mantenimiento de los equipos de la red de telefonía.

Es recomendable que el proveedor realice en su mayoría el proceso de migración con el apoyo de un personal asignado de la empresa Americatel, para poder tener una migración más eficiente y disminuir los errores. Desarrollar una metodología que incluya un cronograma técnico que tome en cuenta el estudio de la plataforma actual, la ingeniería de

tráfico, el estudio de soluciones, los tiempos de prueba e implementación, ya que el período de diseño, proceso licitatorio y de procura de equipamiento puede extenderse ampliamente afectando la implementación a tiempo de todo el proyecto.

Para realizar la sustitución del switch TDM por la tecnología de Softswitch, se deben tener totalmente implementados los equipos propuestos para el Core, de manera de contar con una arquitectura escalable que permita mantenerlos actualizados y den soporte a la Empresa con tecnologías recientes que impulsen nuevas soluciones en comunicaciones.

Es recomendable llevar a cabo el protocolo de pruebas planteado, mediante el cual se puede obtener una muy buena aproximación del comportamiento del equipo en situaciones de producción, lo cual permite establecer planes de gestión y contingencia acorde a los resultados.

Realizar pruebas futuras con nuevos protocolos y tecnologías, como servicios de video y multimedia en IP, de manera de ir adaptando la plataforma NGN para que permita ofrecer soluciones convergentes.

CAPÍTULO V.
COSTO DEL PROYECTO

5.1 Costo de Inversión del Proyecto (CAPEX)

Para este proyecto se muestra los costos de los equipos que formaran parte de la nueva red NGN, la cual remplazará a la central Italtel, esto se ve en el cuadro 5.1, en este cuadro se consideran los equipos que manejaran el tráfico como los equipos de gestión y monitoreo:

Equipo	Cantidad	Precio Total (USD)
SOFTX3000 V3000R010	1	$100,500.00
iManager N2000 UMS V200R012	1	$91,903.18
UMG8900 R8	1	$387,308.00
Subtotal		$579,711.18
Equipamiento DDP	1	$86,956.68
Servicio de Implementación	1	$66,000.00
TOTAL		**$732,667.86**

Cuadro 5.1 Costo de inversión del Proyecto.

5.2 Costo de Operación del Proyecto (OPEX)

Para analizar el costo de operación se tomó en cuenta, el precio de soporte técnico por un año, precio promedio de repuestos, gastos de utilización de gestores para el monitoreo, el mantenimiento anual y el costo de entrenamiento del personal, esto se ve en el cuadro 5.2.

Concepto	Cantidad por Año	Precio Total (USD)
Servicio de Mantenimiento	1	$40,000.00
Costo adicional por E1 adicional	1	$2,040.00
Soporte Anual	1	$65,000.00
Capacitación Local	1	$20,000.00
Total		**$127,040.00**

Cuadro 5.2 Costo de Operación del Proyecto.

5.3 Evaluación Económica y Financiera

Para la evaluación económica se presenta el cuadro 5.3 donde se realizó una comparativa de las tres soluciones presentadas.

COMPARACION ECONOMICA SOFTWSWITCH			
PROVEEDOR	**Huawei**	**Audiocodes**	**Denwa**
Equipamiento	SOFTX3000 iManager N2000 UMS NGN	Mediant 8000 Mediant 3000 EMS HW	IMG 1010 Gate Control Server 3000 HP DL380
Precio	UMG8900 $579,711.18	$600,000.00	$960,000.00
Implementación	$66,000.00	$0.00	$41,000.00
TOTAL	**$645,711.18**	**$600,000.00**	**$1,001,000.00**

Cuadro 5.3 Comparación delas propuestas.

Para poder realizar la elección del equipo se evaluó la mayor capacidad de tramas (E1) que ofrecía cada proveedor y usando un menor numero de equipos, ya que el requerimiento base era de 250 tramas E1, las marcas Audiocodes y Denwa ofrecían dichas capacidades pero con la utilización de dos o mas equipos en cascada, esto significaba un costo adicional al equipo base y además implicaba consumir mas espacio físico en los bastidores y mayor consumo de energía, ante esto la marca Huawei podía satisfacer esta demanda con un solo equipo y con tarjetas de expansión. Esto daba escalabilidad para poder aumentar las interconexiones según los requerimientos de los usuarios.

Otro punto importante a tomar en cuenta fue la capacidad de realizar tareas de red inteligente, como lista negra, lista blanca y registro de usuario, en esto la marca Huawei ofrecía todas estas características integradas en el equipo softswitch, sin embargo las otras marcas las ofertaban con un coste adicional e implementados en equipos adicionales a su softswitch.

Se tomó en consideración poder usar el protocolo SIP y empezar a dar este tipo de interconexiones con operadores internacionales nuevos así como incentivar a los actuales operadores a poder migrar a este tipo de interconexión, y en este sentido los equipos Huawei ofrecían mayor compatibilidad para integrarse a equipos controladores de sesiones

SIP (SBC), que son necesarios para poder tener seguridad cuando se quiere trabajar con grupos de troncales SIP.

Americatel Perú cuenta con clientes empresariales a los cuales se les brinda enlaces primarios usando el protocolo ISDN, esto para poder bridar la conexión de las centralitas(PBX) de los clientes con la PSTN a través de la red de Americatel, este protocolo es manejado por los tres proveedores de softswitch, en el caso de Audiocodes y Denwa lo presenta en un equipamiento adicional, para el caso de Huawei solo es necesario adquirir las licencias para su habilitación en el mismo equipo, esto facilita poder seguir brindando el servicio de Telefonía Digital y aumentar la capacidad de clientes ya que se contaría con un equipo adicional para brindar este servicio.

Un punto muy importante es el tema del soporte y ahí fue mas segura la decisión a favor del proveedor Huawei, ya que ellos aparte del soporte post-venta, ofrecían asesoramiento y apoyo técnico para poder realizar la migración de las interconexiones de la central de conmutación de circuitos hacia el softswitch, esto se diferencio mucho de los otros proveedores debido a que Denwa y Audiocodes no cuentan con un soporte completo en el país, los problemas mas complejos son escalados al exterior, en contra parte la marca Huawei, también escalas los temas mas complejos, pero atiende la mayoría de sus casos localmente debido a la gran presencia en el mercado peruano y en toda la región.

En resumen de estos tres proveedores el softswitch Huawei es el elegido por las características de escalamiento que presenta, su facilidad para adaptarse a nuevos dispositivos de red, las características adicionales que permiten ampliar la gama de servicios y poder entrar a competir con otras empresas que están empezando a usar los modelos de tecnologías de la información y además que permite la convergencia de voz datos y video un una sola plataforma.

CONCLUSIONES Y RECOMENDACIONES

1. De lo explicado se concluye que las redes de telefonía han evolucionado desde hace veinte años en lo que respecta a los nodos de conmutación y a los medios de transmisión, han podido integrarse a las redes de datos gracias a las nuevas tecnologías de centrales basadas en conmutación de paquetes.
2. El uso de la tecnología Softswitch permite a las empresas de telecomunicaciones proporcionar una diversidad de servicios de comunicaciones, como telefonía IP, videollamadas, conferencias, basados en el Protocolo de Internet, equivalentes a los servicios telefónicos básicos de voz que se tienen con las redes tradicionales, pero con la ventaja de contar con una diversidad de servicios adicionales, tales como datos y video.
3. El uso de la plataforma softtswitch permite adoptar otras tecnologías complementarias sobre la infraestructura de telecomunicaciones existente, usando nuevas tecnologías basadas en IP como el IMS.
4. La tecnológica de Softswitch permite la implementación de una gestión centralizada, lo cual representa una gran ventaja para el cumplimiento de las labores de mantenimiento, monitoreo de los elementos de red.
5. Se recomienda a las empresas de telecomunicaciones contar con una red NGN basada en paquetes, y usar las tendencias tecnologías presentes pero sin perder la fiabilidad, conveniencia, funcionalidad y rentabilidad de las redes telefónicas públicas conmutadas.
6. Es recomendable que al realizar una migración de un centro de conmutación de circuitos hacia un centro de conmutación de paquetes considerar la coexistencia de ambos centros de conmutación, para que así no se vea afectado los clientes con la perdida del servicio y el impacto sea menor.
7. Considerar realizar pruebas de las características adicionales que presenta el equipo y que no forman parte del objetivo principal, ya que pueden ser implementadas en un futuro próximo y así aumentar las funcionabilidades y servicios de la empresa de telecomunicaciones como por ejemplo, SIP trunk, enlaces ISDN, abonados SIP y MGCP.

ANEXO A
Tabla del Modelo Erlang B

Tabla Erlang B 0.01%

Canales	T.Erl	Canales	T. Erl	Canales	T. Erl	Canales	T. Erl	Canales	T. Erl
1	0	45	25	89	60	133	97.3	177	135.7
2	0	46	25.8	90	60.9	134	98.2	178	136.6
3	0	47	26.5	91	61.7	135	99	179	137.5
4	0.2	48	27.3	92	62.5	136	99.9	180	138.4
5	0.4	49	28	93	63.4	137	100.8	181	139.3
6	0.7	50	28.8	94	64.2	138	101.6	182	140.1
7	1	51	29.6	95	65	139	102.5	183	141
8	1.4	52	30.3	96	65.9	140	103.4	184	141.9
9	1.8	53	31.1	97	66.7	141	104.2	185	142.8
10	2.2	54	31.9	98	67.5	142	105.1	186	143.7
11	2.7	55	32.7	99	68.4	143	106	187	144.6
12	3.2	56	33.4	100	69.2	144	106.8	188	145.4
13	3.7	57	34.2	101	70	145	107.7	189	146.3
14	4.2	58	35	102	70.9	146	108.6	190	147.2
15	4.7	59	35.8	103	71.7	147	109.4	191	148.1
16	5.3	60	36.6	104	72.6	148	110.3	192	149
17	5.9	61	37.4	105	73.4	149	111.2	193	149.9
18	6.4	62	38.1	106	74.3	150	112	194	150.8
19	7	63	38.9	107	75.1	151	112.9	195	151.7
20	7.6	64	39.7	108	75.9	152	113.8	196	152.5
21	8.3	65	40.5	109	76.8	153	114.7	197	153.4
22	8.9	66	41.3	110	77.6	154	115.5	198	154.3
23	9.5	67	42.1	111	78.5	155	116.4	199	155.2
24	10.2	68	42.9	112	79.3	156	117.3	200	156.1
25	10.8	69	43.7	113	80.2	157	118.1	201	157
26	11.5	70	44.5	114	81	158	119	202	157.9
27	12.2	71	45.3	115	81.9	159	119.9	203	158.8
28	12.8	72	46.1	116	82.7	160	120.8	204	159.7
29	13.5	73	46.9	117	83.6	161	121.6	205	160.6
30	14.2	74	47.7	118	84.4	162	122.5	206	161.5
31	14.9	75	48.6	119	85.3	163	123.4	207	162.3
32	15.6	76	49.4	120	86.1	164	124.3	208	163.2
33	16.3	77	50.2	121	87	165	125.2	209	164.1
34	17	78	51	122	87.9	166	126	210	165
35	17.7	79	51.8	123	88.7	167	126.9	211	165.9
36	18.4	80	52.6	124	89.6	168	127.8	212	166.8
37	19.1	81	53.4	125	90.4	169	128.7	213	167.7
38	19.9	82	54.3	126	91.3	170	129.6	214	168.6
39	20.6	83	55.1	127	92.1	171	130.4	215	169.5
40	21.3	84	55.9	128	93	172	131.3	216	170.4
41	22.1	85	56.7	129	93.9	173	132.2	217	171.3
42	22.8	86	57.6	130	94.7	174	133.1	218	172.2
43	23.5	87	58.4	131	95.6	175	134	219	173.1
44	24.3	88	59.2	132	96.4	176	134.8		

ANEXO B
Pruebas de Hardware y Servicios del SOFTX3000

Part I Operation Guide

T01 Hardware

T01-01 Hardware Installation

T01-0101 Acceptance of Rack Installation

Objective	To check that the rack installation conforms to the re q uirements.
Test Networking Diagram	None
Preset Conditions	The racks have been installed.
Test Procedu res	Expected Results

Perform the acceptance test according to the following items.	1. Placement of racks and other chassis-type devices meets the following requirements: (1) Racks are installed in places complying with the engineering design documents. (2) Cabinets are stable after installed. (3) Chassis-type devices are placed according to customer's requirements. (4) Chassis-type devices are stable. They are fixed to the cabinet where they locate. 2. Installation of supports meets the following requirements: (1) Insulation fittings are installed between the support (anchor plate) and the floor, between the support (anchor plate) and the floor holder, and between the support (anchor plate) and the guide rail according to the structure design. (2) Customer-made bases are installed according to customer's requirement. (3) All expansion bolts fixing each support (foot) to floor are installed and tightened. The installation sequence of insulation washer. flat washer, spring washer, and nut is correct. The expansion bolts fit the mounting holes of the supports (feet). (4) Anchor plates of feet parallel the outer edges of cabinets. Or they form an angel of less than ten degrees. The anchor plates are pressed on the feet. The locking nuts are correctly installed. 3. Structural attachments of cabinets are correctly and firmly installed such as doors, guide rails, feet, floor holders, components for connecting cabinets, cabling troughs, baffle rings, and air filters. In addition, they meet the following requirements: (1) All the cabinet doors are installed, and there is no deformation after installation. The back and front doors of the cabinets can be closed and opened smoothly. (2) All cabling holes of cabinets are sealed. The diameter of the seam is no more than 1.8 cm. Cables are tied neatly. (3) The motion of mobile attachment of cabinets is normal. (4) All connection bolts of cabinets are correctly and reliably installed. The installation sequence of flat washer and spring washer is correct. (5) All bolts and screws are tightened. (6) Boards can be smoothly inserted and pulled out. The degree of tightness of screws on panel of boards is proper. Spring steel wires are intact. (7) All dummy panels are installed.

	(8) Cabinets are clean without any spare cable ties or screws left in them. (9) If row and column labels are available, they are neatly stuck to the label grid of cabinet. 4. After the cabinets are connected, adjacent cabinets are closely connected, stable and of the same height. Door panels of the whole row of cabinets are in the same plane without concaves and convexes. In addition, the cabinets meet the following requirements: (1) Use a horizontal ruler to check the levelness of the cabinets. The error is less than 2 mm/m^2. (2) The whole row of cabinets is evenly lined. The vertical deviation is less than 3 mm. (3) The side door panels of the cabinets that are close to the corridor form a straight line The error is less than 5 mm. (4) Paint on components of racks does not peel off. There is no damage or stain on devices affecting the appearance. Otherwise, paint or clean the devices. (5) There is no deformation on all components of racks. 5. Racks installed in an equipment room with antistatic floors meet the following requirements: (1) The expansion bolts fixing the supports are firmly installed. (2) Connection between guide rails and supports and that between supporting accessories for antistatic floors and guide rails are secure. (3) The four bolts connecting the rack to the guide rail are installed and tightened. 6. Racks directly installed on cement floors meet the following requirements: The washers adjusting the levelness of the cabinet are inserted between the insulating plate and the floor. 7. All the four expansion bolts fixing the rack are tightened.
Test Description	None
Internal Number	T01-0101

T01-0102 Acceptance of Signal Cable Installation

Objective	To check that the installation of signal cables meets the requirements.
Test Networking Diagram	None
Preset Conditions	The cables have been connected.

Part II Operation Guide

T01 Voice Services

T01-01 Test of Fax Functions

T01-0101 Automatic Fax Receiving – Inter-office ISUP Call

Objective	To verify a fax function: automatically receiving inter-office faxes through ISUP trunks.	
Test Networking Diagram	Figure 1	
Preset Conditions	The SoftX3000 and media gateways are working normally. The software commissioning between the SoftX3000 and media gateways is completed. Office A (SoftX3000) interconnects with office B (PSTN switch) through ISUP trunks. Fax subscriber A is in office A and fax subscriber B is in office B Subscriber A's fax machine and subscriber B's fax machine work normally and are in the idle state. Subscribers A and B have not registered any supplementary service. Subscribers A and B have inter-office call-in and call-out authorities.	
Test Procedures		Expected Results
1. Set subscriber B's fax machine to "automatic receipt". Subscriber A calls subscriber B. 2. Subscriber A sends a fax to subscriber B after hearing the signal tone for fax. 3. The fax is over.		1. Subscriber B's fax machine rings, and subscriber A hears the ringback tone. 2. Subscriber B receives the fax. 3. The call is released.
Test Description	Subscriber A can be an MGCP subscriber, an H.248 subscriber, an H.323 subscriber (only IAD subscriber) or a V5 subscriber. The test needs to be completed according to different combinations of subscribers.	
Internal Number	T02-0203	

T01-0102 Manual Fax Receiving – Inter-office ISUP Call

Objective	To verify a fax function: manually receiving inter-office faxes through ISUP trunks.
Test Networking Diagram	Figure 1
Preset Conditions	The SoftX3000 and media gateways are working normally. The software commissioning between the SoftX3000 and media gateways is completed. Office A (SoftX3000) interconnects with office B (PSTN switch) through ISUP trunks. Fax subscriber A is in office A and fax subscriber B is in office B. Subscriber A's fax machine and subscriber B's fax machine work normally and are in

	the idle state. Subscribers A and B have not registered any supplementary service. Subscribers A and B have inter-office call-in and call-out authorities.

Test Procedures	Expected Results
1. Set subscriber B's fax machine to "manual receipt". Subscriber A cells subscriber B. 2. Subscriber B presses the <receive> button on his/her fax machine. 3. Subscriber A sends a fax to subscriber B after hearing the signal tone for fax. 4. The fax is over.	1. Subscriber B's fax machine rings, and subscriber A hears the ringback tone. 2. Subscriber A hears the signal tone for fax. 3. Subscriber B receives the fax. 4. The call is released.

Test Description	Subscriber A can be an MGCP subscriber, an H.248 subscriber, an H.323 subscriber (only IAD subscriber) or a V5 subscriber. The test needs to be completed according to different combinations of subscribers.
Internal Number	T02-0204

T02 Charging and Billing

T02-0101 Charging Incoming Trunk Group

Objective	To verify whether the incoming trunk group can be charged normally
Test Networking Diagram	Figure 1
Preset Conditions	1. The SoftX3000 and media gateways work normally. 2. The software commissioning between the SoftX3000 and media gateways has been completed. 3. Local office subscriber A and opposite office subscriber B work normally. The link with the opposite office is normal. 4. Enter the command (for example, **MOD N1TG or MOD N7TG)** in the MML command input box to modify the trunk group, and set the charging source code of an incoming trunk group (R2\TUP\ISUP) to a valid value "X". 5. Enter the command **MOD VSBR** or **MOD MSBR** in the MML command input box, and set subscriber A's charging source code to a valid value "Y". 6. Enter the command **ADD CHGANA** in the MML command input box. For charging case 1, set "Charging office" to "Uncentralized charging", "Payer" to "Calling party", "Charging method" to "Detailed ticket", and then set the corresponding tariff. 7. Enter the command **MOD CHGMODE** in the MML command input box, and then set the charging mode of charging case 1. 8. Enter the command **ADD CHGGRP** in the MML command input box, and then define charging case 1 with the caller charging source code as "X", the callee charging source code as "Y", and the bearer capability as "All". Set the charging case to detailed ticket charging, and other charging data the same as that in "Generating Detailed Tickets Only".

Test Procedures	Expected Results

1. Subscriber B calls subscriber A through the incoming trunk(R2\TUP\ISUP). The call is connected. And then one of the subscribers hangs up. 2. Browse the ticket on the iGWB client.	1. Subscriber A calls subscriber B can talk normally, and the call can be release normally, There is the detailed ticket for the call through the incoming trunk in the ticket file. 2. The payer is the incoming trunk, and contents of other fields are consistent with the actual conditions. Particularly observe the caller number, callee number, start and end time of the call, call duration, call charge and calling device type. The caller number field may be null. It depends on whether the caller number of the opposite office can be obtained.
Test Description	In the charging case, modify "Detailed ticket" to "Meter table", set the meter tariff, and repeat the test. Before checking the ticket, execute the command **RST BILPOL** to update "Meter table" and "Statistics ticket table". The metering ticket content should be consistent with the actual conditions.
Internal Number	T04-0104

T02-0102 Charging Outgoing Trunk Group

Objective	To verify whether the outgoing trunk group can be charged normally	
Test Networking Diagram	Figure 1	
Preset Conditions	1. The SoftX3000 and media gateways work normally. 2. The software commissioning between the SoftX3000 and media gateways has been completed. 3. Local office subscriber A and opposite office subscriber B work normally. The link with the opposite office is normal. 4. Enter the command (for example, **MOD N1TG & MOD N7TG**) in the MML command input box to modify the trunk group, and set the outgoing trunk charging source code of an incoming trunk group (R2\TUP\ISUP) to "X". 5. Enter the command **MOD VSBR** or **MOD MSBR** in the MML command input box, and set subscriber A's charging source code to "Y". 6. Enter the command **ADD CHGANA** in the MML command input box. For charging case 1, set "Charging office" to "Uncentralized charging", "Payer" to "Calling party", "Charging method" to "Detailed ticket", and then set the corresponding tariff. 7. Enter the command **MOD CHGMODE** in the MML command input box, and then set the charging mode of charging case 1. 8. Enter the command **ADD CHGGRP** in the MML command input box, and then define charging case 1 with the caller charging source code as "X", the callee charging source code as "Y", and the bearer capability as "All". Set the charging case to detailed ticket charging, and other charging data the same as that in "Generating Detailed Tickets Only".	
Test Procedures		Expected Results

1. Subscriber A calls subscriber B through the outgoing trunk (R2\TUP\ISUP). The call is connected. And then one of the subscribers hangs up. 2. Browse the ticket on the iGWB client.	1. There is the detailed ticket for the call through the outgoing trunk in the ticket file. 2. The payer is the outgoing trunk, and contents of other fields are consistent with the actual conditions. Particularly observe the caller number, callee number, start and end time of the call, call duration, call charge and calling device type.
Test Description	In the charging case, modify "Detailed ticket" to "Meter table", set the meter tariff, and repeat the test. Before checking the ticket, execute the command **RST BILPOL** to update "Meter table" and "Statistics ticket table". The metering ticket content should be consistent with the actual conditions.
Internal Number	T04-0105

T02-02 Ticket Management Functions

T02-0201 Querying Tickets on iGWB

Objective	To verify whether tickets can be queried on the iGWB normally	
Test Networking Diagram	Figure 1	
Preset Conditions	1. The SoftX3000 and media gateways work normally. 2. The software commissioning between the SoftX3000 and media gateways has been completed. 3. There are original tickets on the iGWB.	
Test Procedures		Expected Results
1. Double-click a ticket on the iGWB client. The ticket format selection dialog is displayed. Select a ticket format and then confirm it. 2. You can also right-click the ticket and select [Ticket query]. The query condition dialog is displayed. Enter conditions and then confirm it. 3. Double-click a ticket.		1. All tickets of this format under the current directory are displayed in the window on the right of the interface. 2. All tickets that meet the conditions under the current directory are displayed in the window on the right of the interface. 3. Detailed information of the ticket is displayed.
Test Description	The format of iGWB bill library must be compatible with the nation code and version of the SoftX3000. Otherwise, some segment in the bills will not be properly displayed.	
Internal Number	T04-0201	

T02-03 Basic Functions of iGWB

T02-0301 Network Server Collecting Tickets

Objective	To verify whether the iGWB can allow the network server (such as the charging center) to collect tickets through the FTP interface
Test Networking Diagram	Figure 2
Preset Conditions	1. The network runs normally.

	2. The network server works normally and the FTP client is started. 3. The iGWB server works normally and the final ticket is generated. 4. The FTP server is started normally, and the storage directory of the final ticket is provided for the network server.

Test Procedures	Expected Results
1. The network server logs in to the iGWB through the FTP and fetches the final ticket.	2. The network server can log in to the iGWB through the FTP and correctly fetch the final ticket.

Test Description	If FTP is used as the charging interface protocol, this acceptance item is valid.
Internal Number	T04-0301

T02-0302 Checking iGWB Biplane

Objective	To verify whether the biplane connecting the iGWB with the SoftX3000 is normal
Test Networking Diagram	Figure 2
Preset Conditions	1. The network runs normally. 3. 2 The iGWB server works normally.

Test Procedures	Expected Results
1. Carry out the **ipconfig/all** command on the active server, and check the output information of the command. 2. Disconnect an Ethernet cable between the active server and the SoftX3000, and wait for one minute. Carry out the **ipconfig/all** command on the active server again, and check the output information of the command. 3. Reconnect the Ethernet cable on the active server. 4. One minute later, disconnect the other Ethernet cable between the active server and the SoftX3000, and wait for one minute. Carry out the **ipconfig/all** command on the active server, and check the output information of the command. 5. Disconnect all the Ethernet cables between the activated server and the SoftX3000. Wait for three minutes and check the state of the active and standby iGWBs. 6. Reconnect all the Ethernet cables. 7. Wait for six minutes. Do the test on another server and observe the result.	1. In step 1, the output information of the command indicates that both the two Ethernet interfaces connected with the SoftX3000 have IP addresses, and the iGWB runs normally. 2. In step 2, the output information of the command indicates that the Ethernet interface connected with the SoftX3000 has the IP address, while the disconnected one does not. The iGWB runs normally and the switchover does not happen. 3. In step 4, the output information of the command indicates that the Ethernet interface connected with the SoftX3000 has the IP address, while the disconnected one does not. The iGWB runs normally and the switchover does not happen. 4. In step 5, the switchover occurs. 5. In step 7, the result of the test on another server is the same as that of the first server. 6. For the active server, the switchover does not happen, when only one of the two Ethernet cables connected with the SoftX3000 is disconnected. The two cables work in the active/standby mode. 7. For the active server, when both the two Ethernet cables connected with the SoftX3000 are disconnected, the switchover occurs.

Test Description	This test can only be done when SwitchGroups of virtual IP addresses of the two Ethernet interfaces connected with the SoftX3000 are set with a same group number. The group number must be a positive integer.

Internal Number	T04-0304

T02-04 Basic Functions of Bill Console

T02-0401 Managing Operator

Objective	To verify whether the iGWB client can add a operator, delete a operator, modify operator attributes, and authenticate operator 's authorities
Test Networking Diagram	Figure 2
Preset Conditions	1. The network runs normally. 4. 2 The iGWB server works normally. 5. 3 The iGWB client is started.

Test Procedures	Expected Results
1. Enter a nonexistent operator or wrong administrator password. 2. Enter the correct administrator password, log in to the iGWB client, and add a operator. 3. Modify the attributes of the new operator. 4. Query the attributes of the new operator. 5. Delete the new account and log in with the account again.	1. In step 1, the login fails. 6. 2. In step 2, the new account is added successfully. 7. 3. In step 3, the attributes of the operator can be modified. 8. 4. In step 4, the modified attributes of the operator can be queried. 9. 5. In step 5, the account is deleted successfully, but the login fails.

Test Description	None.
Internal Number	T04-0401

T02-0402 Managing Logs

Objective	To verify whether the log can be browsed, queried and printed on the iGWB client
Test Networking Diagram	Figure 2
Preset Conditions	1. The network runs normally. 10. 2 The iGWB server works normally. 11. 3 Log in to the iGWB client as the administrator.

Test Procedures	Expected Results
1. Open the log query interface on the iGWB client, and enter the start and end time of the log to be queried. 2. Click one of the queried logs and browse the detailed information. 3. Save the queried log to the file which can be printed.	1. The log can be queried. 2. The detailed information of the log can be browsed. 3. The file saving the log is generated and can be printed.

Test Description	None.

ANEXO C

Lista de contenido de las pruebas

Table of Contents

Contents

Table of Contents

Table of Contents

Contents

Table of Contents

Table of Contents

ol

ANEXO D
Recomendación UIT-T (G.732)

Recomendación UIT-T (G.732)

Las normas y recomendaciones de G.732 fueron originalmente publicadas en el libro azul de la ITU-T y fueron hechas para regular las características de los equipos de multiplexación MIC que funcionen a 2.048 Mb/s (también llamados E1 de acuerdo a su Jerarquía).

La adición de las normas de G.732 al Cisco Signaling Link (SLT) ha sido de gran importancia para definir los requerimientos de homologación en muchos países, principalmente de Europa. Terminal. Estas normas se han convertido en parte esenciales del programa PGW-2200 de Cisco, que se encarga de normalizar los términos en los que se lleva a cabo la señalización.

Éstas son algunas de las recomendaciones descritas en el ITU-T (G.732):

- Características de E1:

- La Ley de Codificación utilizada, es la Ley A que se encuentra especificada en G.711. La velocidad del muestreo y el nivel de sobrecarga se encuentran especificadas también en dicha recomendación.

- La velocidad binaria nominal del E1 deberá de ser de 2048 Kb/s. La tolerancia para ésta velocidad es de ± 50 partes por millón (ppm).

- La señal de temporización para la transmisión de un equipo múltiplex MIC debe ser posible derivarla de una fuente interna, de la señal digital entrante y también de una fuente externa.

- La estructura de la Trama y el empleo de intervalos de tiempo para cada canal, se encuentran especificados en G.704. Si el intervalo de tiempo de canal 16, que está asignado a la señalización, no se necesita para señalización, podrá utilizarse para fines distintos dentro del equipo múltiplex MIC.

- Detección de Averías:

- Fallo de la fuente de alimentación.

- Fallo del códec (Excepto Códecs de un solo canal).

- Pérdida de la señal entrante en la entrada a 64 kbit/s.

- Pérdida de la señal entrante a 2048 kbit/s.

- Pérdida de la alineación de trama.

- Tasa de errores excesiva en los bits detectados mediante la monitorización de la señal de alineación de trama.

- Operaciones Consiguientes Tras la Detección de una Avería:

- Generación de una indicación de alarma de servicio para notificar que el servicio proporcionado por el múltiplex MIC ha dejado de estar disponible. Esta indicación debe transmitirse por lo menos al equipo múltiplex de señalización y/o al equipo de conmutación, según las disposiciones que se hayan tomado. La indicación deberá darse tan pronto como sea posible, y no después de 2 ms tras la detección de la correspondiente condición de avería.

- Cuando se utiliza la señalización por canal común, la indicación debe enviarse al equipo de conmutación por medio de un interfaz separado en el equipo múltiplex MIC.

- Generación de una indicación de alarma para mantenimiento inmediato para notificar que la calidad de funcionamiento es inferior a normas aceptables y que es necesario proceder a una operación local de mantenimiento.

- Transmisión de una indicación de alarma hacia el extremo distante, obtenida haciendo pasar del estado 0 al estado 1 el bit 3 del intervalo de tiempo de canal 0 en las tramas que no contienen la señal de alineación de trama. Esto debe efectuarse lo más pronto posible.

- Supresión de la transmisión en las salidas analógicas.

ANEXO E
Recomendaciones del Sistema de Señalización 7

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T Q.700

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/93)

ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 7

INTRODUCCIÓN AL SISTEMA DE SEÑALIZACIÓN N.° 7 DEL CCITT

Recomendación UIT-T Q.700

(Anteriormente «Recomendación del CCITT»)

Recomendación Q.700

INTRODUCCIÓN AL SISTEMA DE SEÑALIZACIÓN N.º 7 DEL CCITT

(Melbourne, 1988; modificada en Helsinki, 1993)

1 Generalidades

La presente Recomendación proporciona una visión global del sistema de señalización, describiendo los diversos elementos funcionales del sistema de señalización N.º 7 (SS N.º 7) y la relación entre dichos elementos funcionales. En esta Recomendación se hace una descripción general de las funciones y capacidades de la parte transferencia de mensajes (MTP, *message transfer part*), de la parte control de conexión de señalización (SCCP, *signalling connection control part*), de la parte usuario de telefonía (TUP, *telephone user part*), de la parte usuario de RDSI (PU-RDSI), de las capacidades de transacción (TC, *transaction capabilities*) y de la parte operaciones, mantenimiento y administración (OMAP, *operations, maintenance and administration part*) que se tratan en otra parte de la serie de Recomendaciones Q.7xx (que comprende las Recomendaciones Q.700 a Q.787). Sin embargo, en caso de contradicción entre una especificación y la Recomendación Q.700, se aplicará esa especificación.

En la serie de Recomendaciones Q.73x se describen los servicios suplementarios del SS N.º 7 en la RDSI.

Además de estas funciones del SS N.º 7 la serie de Recomendaciones Q.7xx describe la estructura de la red del SS N.º 7 y también especifica las pruebas y mediciones aplicables al mismo.

Esta Recomendación contiene información sobre otros aspectos tales como la arquitectura del SS N.º 7, el control de flujos y la norma general de compatibilidad que no están especificados en Recomendaciones separadas y son aplicables al objetivo global del SS N.º 7. La Recomendación Q.1400 también contiene información sobre arquitectura y compatibilidad.

El resto de la presente Recomendación describe

– cláusula 2: Conceptos, componentes y modos de la red de señalización;

– cláusula 3: Bloques funcionales en el SS N.º 7 y servicios que prestan;

– cláusula 4: Sistema de capas de protocolo del SS N.º 7 y su relación con los modelos OSI;

– cláusula 5: Direccionamiento de nodo, entidad de aplicación y parte de usuario;

– cláusula 6: Aspectos de operación, mantenimiento y administración del SS N.º 7;

– cláusula 7: Aspectos de operación de los bloques funcionales en el SS N.º 7;

– cláusula 8: Control de flujo, tanto para la red de señalización, como dentro de los nodos;

– cláusula 9: Reglas para la evolución de los protocolos del SS N.º 7 preservando su compatibilidad con versiones anteriores;

– cláusula 10: Referencias a un glosario de términos.

1.1 Objetivos y campos de aplicación

El objetivo global del SS N.º 7 consiste en proporcionar un sistema de señalización por canal común (CCS, *common channel signalling*) de aplicación general, normalizado internacionalmente:

– optimizado para el funcionamiento en redes de telecomunicaciones digitales junto con centrales con control por programa almacenado;

– que pueda satisfacer exigencias presentes y futuras de transferencia de información para el diálogo entre procesadores dentro de las redes de telecomunicaciones para el control de las llamadas, de control a distancia y de señalización de gestión y mantenimiento;

– que ofrezca un medio seguro de transferencia de información en la secuencia correcta y sin pérdidas ni duplicaciones.

Este sistema de señalización satisface las exigencias de la señalización de control de las llamadas para servicios de telecomunicaciones tales como telefonía y transmisión de datos con conmutación de circuitos. Puede utilizarse también como un sistema fiable para la transferencia de otros tipos de información entre centrales y centros especializados en redes de telecomunicaciones (por ejemplo, para fines de gestión y mantenimiento). Por consiguiente, puede utilizarse para aplicaciones múltiples tanto en redes especializadas para servicios específicos como en redes capaces de ofrecer múltiples servicios. Se pretende que este sistema de señalización sea aplicable en redes internacionales y nacionales.

El objetivo del SS N.º 7 abarca tanto la señalización relacionada con circuitos como la no relacionada con circuitos.

Son ejemplos de las aplicaciones del SS N.º 7:

– la RTPC;

– la RDSI;

– la interacción con bases de datos de la red y puntos de control del servicio;

– las comunicaciones móviles (red móvil terrestre pública);

– la explotación, administración y mantenimiento de redes.

El sistema de señalización está optimizado para funcionar en canales digitales de 64 kbit/s. También es adecuado para el funcionamiento a velocidades más bajas y en canales

analógicos. Es adecuado para enlaces punto a punto, tanto terrenales como por satélite. Si bien no tiene las propiedades especiales requeridas por el funcionamiento punto a multipunto, puede ampliarse en caso necesario para atender tal aplicación.

1.2 Características generales

La señalización por canal común es un método de señalización en el cual un solo canal transfiere, por medio de mensajes etiquetados, información de señalización relativa a varios circuitos y otras informaciones tales como la gestión de la red. Se puede considerar la señalización por canal común como una forma de comunicación de datos que está especializada para varios tipos de transferencia de información y de señalización entre procesadores en las redes de telecomunicaciones.

El sistema de señalización utiliza enlaces de señalización para la transferencia de mensajes de señalización entre centrales u otros nodos de la red de telecomunicaciones servidos por este sistema. Se prevén medios para asegurar la transferencia fiable de la información de señalización en presencia de perturbaciones de la transmisión o fallos de la red. Estos medios incluyen la detección y corrección de errores en cada enlace de señalización. En el sistema se emplea normalmente la redundancia en enlaces de señalización y se incluyen las funciones necesarias para la desviación automática del tráfico de señalización hacia trayectos alternativos en caso de fallos del enlace. Por tanto, se puede dimensionar la capacidad y fiabilidad de la señalización de acuerdo con los requisitos de las diferentes aplicaciones, mediante la disposición de múltiples enlaces de señalización.

1.3 Componentes del SS N.º 7

El SS N.º 7 está constituido por diversos componentes o funciones definidos en la serie de Recomendaciones Q.7xx.

Función del SS N.º 7	*Recomendaciones*
Parte transferencia de mensajes (MTP)	Q.701-Q.704, Q.706, Q.707
Parte usuario de telefonía (TUP) (Incluye algunos servicios suplementarios)	Q.721-Q.725
Servicios suplementarios (SS)	Serie Q.73x
Parte usuario de datos (DUP)	Q.741 (véase la Nota)
Parte usuario de RDSI (PU-RDSI)	Q.761-Q.764, Q.766
Parte control de conexión de señalización (SCCP)	Q.711-Q.714, Q.716
Capacidad de transacción (TC)	Q.771-Q.775
Parte operaciones, mantenimiento y administración (OMAP)	Q.750-Q.755

NOTA – Las funciones de la DUP se especifican en la Recomendación X.61.

Otras Recomendaciones de la serie Q.7xx que describen otros aspectos del sistema de señalización que no forman parte de las interfaces de señalización del SS N.° 7 son:

Título	*Recomendaciones*
Estructura de la red de señalización	Q.705
Numeración de códigos de puntos de señalización internacional	Q.708
Conexión ficticia de referencia para la señalización	Q.709
Aplicación en centrales automáticas privadas	Q.710
Especificación de pruebas del SS N.° 7 (Generalidades)	Q.780
Especificación de pruebas de la MTP de nivel 2	Q.781
Especificación de pruebas de la MTP de nivel 3	Q.782
Especificación de pruebas de la TUP	Q.783
Especificación de pruebas de la PU-RDSI	Q.784
Especificación de pruebas de servicios suplementarios de la PU-RDSI	Q.785
Especificación de pruebas de la SCCP	Q.786
Especificación de pruebas de la TCAP	Q.787

La cláusula 3 describe la relación entre estos componentes.

1.4 Técnicas de descripción en la serie de Recomendaciones Q.7xx

En la serie de Recomendaciones del SS N.° 7 se define el sistema de señalización utilizando una descripción escrita, complementada por diagramas SDL y diagramas de transición de estados. En el caso de que surgieran conflictos entre el texto y la definición SDL, se toma la descripción del texto como definitiva.

Para ilustrar los ejemplos de los procedimientos de señalización se utilizan gráficas de secuencias de mensajes y diagramas de flechas, pero los mismos no se consideran definitivos.
En las descripciones de datos se emplea cada vez más el método ASN.1.

2 Red de señalización del SS N.° 7

2.1 Conceptos básicos

Una red de telecomunicaciones a la que da servicio un sistema de señalización por canal común está compuesta de un número de nodos de conmutación y proceso interconectados

por enlaces de transmisión. Para comunicar cada uno de estos nodos utilizando el SS N.º 7 se requiere crear las características necesarias «dentro del nodo» del SS N.º 7, convirtiendo este nodo en un punto de señalización de la red del SS N.º 7. Además, surgirá la necesidad de interconectar estos puntos de señalización de tal manera que la información de señalización (datos) del SS N.º 7 pueda transferirse entre ellos. Estos enlaces de datos son los enlaces de señalización de la red de señalización del SS N.º 7.

El conjunto de puntos de señalización y sus enlaces de señalización de interconexión forman la red de señalización del SS N.º 7.

2.2 Componentes de la red de señalización

2.2.1 Puntos de señalización

En casos específicos puede ser necesario dividir las funciones de señalización por canal común en un nodo (físico) en entidades separadas lógicamente desde el punto de vista de la red de señalización; esto es, un nodo (físico) dado puede estar definido como más de un punto de señalización. Un ejemplo lo constituye una central en la frontera entre la red de señalización internacional y redes de señalización nacionales.

Dos puntos de señalización cualesquiera cuyas funciones de parte de usuario correspondientes tengan la posibilidad de comunicar entre sí se dice que tienen una relación de señalización de usuario.

El concepto correspondiente para una parte de usuario determinada se denomina una relación de señalización de usuario.

Se tiene un ejemplo de ésta cuando dos centrales telefónicas están conectadas directamente por un haz de circuitos vocales. El intercambio de señalización telefónica relativa a estos circuitos constituye pues una relación de señalización de usuario entre las funciones de las partes de usuario de telefonía de esas centrales, que actúan como puntos de señalización.

Otro ejemplo es el caso en que la gestión de los datos de usuario y de encaminamiento en una central telefónica está controlada a distancia desde un centro de explotación y mantenimiento por medio de una comunicación a través del sistema de señalización por canal común.

Son ejemplos de nodos, en una red de señalización, que constituyen puntos de señalización:

– centrales (centros de conmutación);

– bases de datos de redes inteligentes;

– puntos de transferencia de señalización;

– centros de explotación, gestión y mantenimiento.

Un punto de señalización al cual está destinado un mensaje, es decir, aquel en que está ubicada la función parte de usuario receptora, es el punto de destino de ese mensaje.
Para una determinada relación de señalización entre dos puntos de señalización, estos dos puntos funcionarán pues como puntos de origen y de destino para los mensajes intercambiados en ambos sentidos.

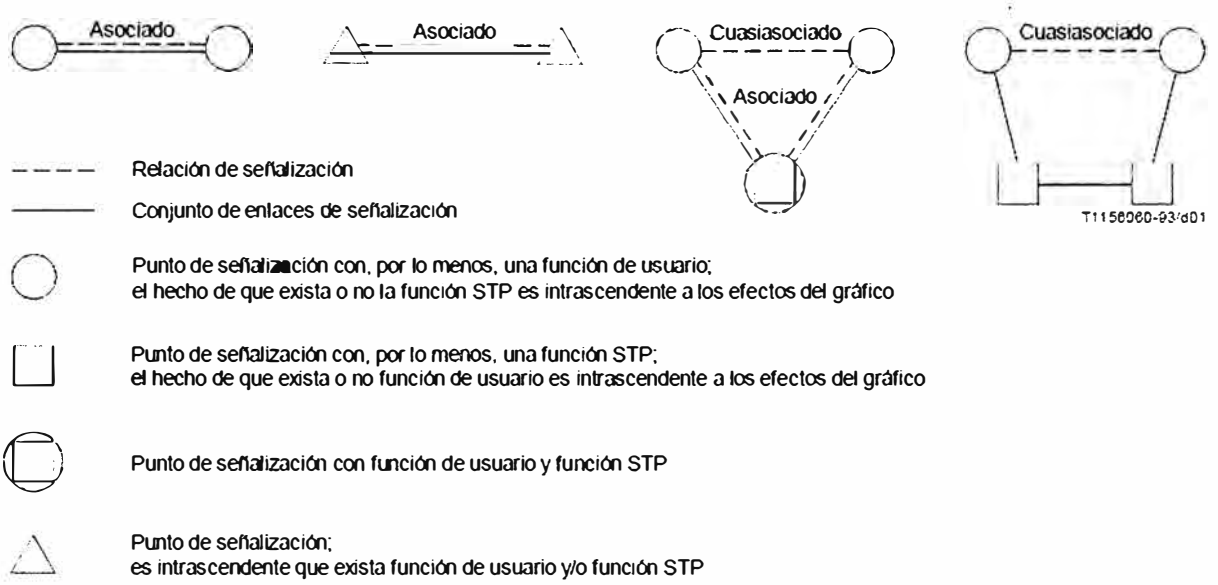


FIGURA 1/Q.700

Ejemplos de los modos de señalización asociado y cuasiasociado, y definición de símbolos gráficos utilizados para la red de señalización

Un punto de señalización en el cual un mensaje recibido por un enlace de señalización se transfiere a otro enlace de señalización, es decir, un punto en el cual no está ubicada la función parte de usuario emisora ni la receptora, es un punto de transferencia de señalización (STP, *signal transfer point*).

En el modo cuasiasociado, la función de un punto de transferencia de la señalización está situada generalmente en algunos puntos de señalización que pueden estar especializados en esta función, o cambiarla con alguna otra (por ejemplo, con la de conmutación). Un punto de señalización que actúa como punto de transferencia de la señalización funciona como punto de origen y punto de destino para los mensajes generados y recibidos por la función de nivel 3 de la MTP, también en los casos en que no existen funciones de usuario.

2.4 Rutas de señalización

El trayecto predeterminado, constituido por una sucesión de puntos de señalización/puntos de transferencia de señalización y por los enlaces de señalización de interconexión y utilizado por un mensaje a través de la red de señalización entre el punto de origen y el punto de destino, es la ruta de señalización para esta relación de señalización.

Todas las rutas de señalización que un mensaje puede utilizar entre un punto de origen y un punto de destino a través de la red de señalización son el conjunto de rutas de señalización para dicha relación de señalización.

2.5 Estructura de la red de señalización

El sistema de señalización puede utilizarse con diferentes tipos de estructuras de la red de señalización. En la elección entre diferentes tipos de estructuras de la red de señalización pueden influir factores tales como la estructura de la red de telecomunicaciones a que dará servicio el sistema de señalización y los aspectos administrativos.

En el caso de que la provisión del sistema de señalización se planifica, puramente relación de señalización por relación de señalización, se obtendrá probablemente como resultado una red de señalización asociada, complementada por lo general por cierto volumen de señalización cuasiasociada para relaciones de señalización de poco tráfico. La estructura de una tal red de señalización está determinada principalmente por las configuraciones de tráfico de las relaciones de señalización.

Otro planteamiento consiste en considerar la red de señalización como un recurso común que debe planificarse de acuerdo con la totalidad de las necesidades de señalización por canal común. La elevada capacidad de los enlaces de señalización digitales en combinación con las necesidades de redundancia para asegurar la fiabilidad, conduce generalmente a una red de señalización basada en un alto grado de señalización cuasi asociada complementada por un menor grado de señalización asociada. Este último planteamiento para la planificación de la red de señalización es el que más posibilidades ofrece de explotar el potencial de señalización por canal común, de modo que se dé servicio a facilidades de la red que requieran comunicación para otros fines distintos de la conmutación de circuitos.

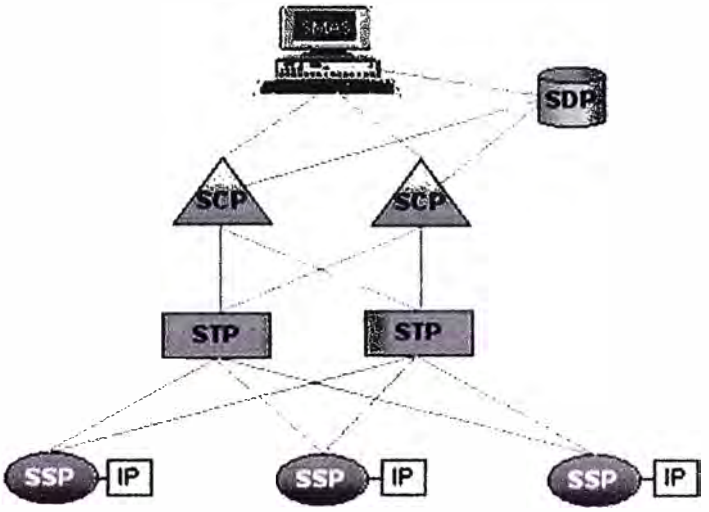
La red mundial de señalización está estructurada en dos niveles funcionalmente independientes, que son los niveles internacional y nacional. Esta estructura hace posible una división clara de la responsabilidad para la gestión de la red de señalización y permite que los planes de numeración de los puntos de señalización de la red internacional y de las distintas redes nacionales sean independientes unos de otros.

En la Recomendación Q.705 se hacen otras consideraciones sobre la estructura de una red de señalización y, en la Recomendación Q.701, sobre las consecuencias en la parte de transferencia de mensajes.

ANEXO F
Red Inteligente

Red Inteligente-Intelligent Network (IN)

La red inteligente (IN) es el estándar de arquitectura de red se especifica en las recomendaciones de la serie UIT-T Q.1200. Está destinado a fijar así como móviles de telecomunicaciones de redes. Permite a los operadores diferenciarse al ofrecer servicios de valor añadido, además de los servicios estándar de telecomunicaciones como PSTN, ISDN y servicios GSM en teléfonos móviles. La inteligencia es proporcionada por los nodos de red en la capa de servicio, distinta de la conmutación de la capa de red de núcleo, en oposición a las soluciones basadas en la inteligencia en los principales interruptores o equipos telefónicos. Los nodos IN están normalmente pertenecen a los operadores de telecomunicaciones (proveedores de servicios de telecomunicaciones).
IN es apoyado por el Sistema de Señalización n ° 7 (SS7) de protocolo de red entre los centros de conmutación telefónica y otros nodos de red son propiedad de los operadores de red, como se muestra en la siguiente figura:



Elementos de la red inteligente

Ejemplos de servicios IN:

- Televoto
- Filtrado de llamadas
- Teléfono portabilidad numérica
- Llamadas gratuitas / Llamada Gratuita
- Telefónica Prepagada
- Cuenta de tarjeta de llamada
- Las redes privadas virtuales (por ejemplo, llamadas de grupo familiar)
- Centrex servicio (Virtual PBX)
- Los planes privados de números (con los números que quedan sin publicar en directorios)
- Universal de servicio de telecomunicación personal (un número universal de teléfono personal)
- Mass-vocación de servicio
- Prefijo de marcación gratuita desde teléfonos móviles en el extranjero
- Seamless MMS acceso a mensajes del exterior.
- Cobro revertido

- Rebajas Inicio Área
- Llamadas de tarificación adicional
- Distribución de llamadas sobre la base de diversos criterios asociados con la llamada Location Based Routing
- Tiempo de enrutamiento basado
- Distribución de llamadas proporcional (por ejemplo, entre dos o más centros de llamadas o en oficinas).
- Cola de llamadas
- Transferencia de llamadas

El concepto de IN, la arquitectura y los protocolos fueron desarrollados originalmente como estándares por la UIT-T, que es la estandarización del comité de la Unión Internacional de Telecomunicaciones, con anterioridad a este una serie de proveedores de telecomunicaciones tenía en la propiedad de las soluciones. El objetivo principal de la IN era mejorar los servicios de telefonía básica que ofrecen las redes de telecomunicaciones tradicionales, que normalmente ascienden a hacer y recibir llamadas de voz, a veces con el desvío de llamadas. Este núcleo entonces proporcionaría una base sobre la cual los operadores pueden construir servicios adicionales a los que ya están presentes en un nivel central telefónica.

Una descripción completa de la IN surgió en un conjunto de la UIT-T estándares llamado Q.1210 a Q.1219, o conjunto de capacidades One (CS-1) como eran conocidos. Las normas definen una arquitectura completa que incluye el punto de vista arquitectónico, máquinas de estados, la ejecución física y los protocolos. Ellos fueron adoptados universalmente por los proveedores de telecomunicaciones y operadores, aunque muchas variantes fueron derivadas para su uso en diferentes partes del mundo.

Tras el éxito del CS-1, seguido de nuevas mejoras en la forma de CS-2. Aunque las normas se completaron, no fueron tan ampliamente implementados como CS-1, en parte por el creciente poder de las variantes, pero en parte también porque abordaban cuestiones que impulsaron los tradicionales centrales telefónicos a sus límites.

El conductor principal detrás del desarrollo del sistema era la necesidad de una forma más flexible de añadir servicios sofisticados a la red existente. Antes de IN se desarrolló toda la característica nueva y / o servicios que se iban a añadirse tenía que ser aplicada directamente en los sistemas centrales de conmutación. Esto hizo que los ciclos de liberación largos como la caza de errores y la prueba tuvo que ser extensa y exhaustiva para evitar que la red de la quiebra. Con el advenimiento de la IN, la mayoría de estos servicios (como números de llamada gratuita o conservación del número geográfico) fueron removidos de los sistemas centrales de conmutación y en servir a la auto-nodos (IN), creando así una red modular y más seguro que la permitida proveedores de servicios para desarrollar ellas mismas variaciones y servicios de valor añadido a su red sin la presentación de una solicitud al fabricante del interruptor principal y espere a que el proceso de desarrollo de largo plazo. El uso inicial de IN tecnología era para servicios de traducción de números, por ejemplo, al traducir a números gratuitos regulares PSTN números. Pero los servicios mucho más complejos desde entonces se han construido en IN, tales como servicios personalizados de área local de señalización (CLASS) y las llamadas telefónicas de prepago.

ANEXO G
RFC 791

RFC: 791

INTERNET PROTOCOL
(Protocolo Internet)

DARPA INTERNET PROGRAM

ESPECIFICACION del PROTOCOLO

Septiembre 1981
(Traducción al castellano: Mayo 1999)
(Por: Pedro J. Ponce de León <pjleon@arrakis.es>)

preparado para

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

por

Information Sciences Institute
University of Southern California
4676 Admiralty Way
Marina del Rey, California 90291

PREFACIO

Este documento especifica el Protocolo Internet Estándar del DoD (N.T.: Department of Defense, USA). Este documento está basado en seis ediciones anteriores de la Especificación del Protocolo Internet de ARPA, y el presente texto se basa en gran medida en ellas. Han habido muchos colaboradores en este trabajo en términos de conceptos y texto. Esta edición revisa aspectos de direccionamiento, tratamiento de errores, códigos de opción, y de las características de seguridad, prioridad, compartimientos y manejo de restricciones del protocolo Internet.

Jon Postel

Editor

RFC: 791
Sustituye a: RFC 760
IENs 128, 123, 111,
80, 54, 44, 41, 28, 26

PROTOCOLO INTERNET

DARPA INTERNET PROGRAM
ESPECIFICACION DE PROTOCOLO

1. INTRODUCCION

1.1. Motivación

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. A un sistema de este tipo se le conoce como "catenet" [1]. El protocolo internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo internet tambien se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.

1.2. Ambito

El Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits (un datagrama internet) desde un origen a un destino a través de un sistema de redes interconectadas. No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos host-a-host. El protocolo internet puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

1.3. Interfaces

Este protocolo es utilizado por protocolos host-a-host en un entorno internet. Este protocolo utiliza a su vez protocolos de red locales para llevar el datagrama internet a la próxima pasarela ("gateway") o host de destino.

Por ejemplo, un módulo TCP llamaría al módulo internet para tomar un segmento TCP (incluyendo la cabecera TCP y los datos de usuario) como

la parte de datos de un datagrama internet. El módulo TCP suministraría las direcciones y otros parámetros de la cabecera internet al módulo internet como argumentos de la llamada. El módulo internet crearía entonces un datagrama internet y utilizaría la interfaz de la red local para transmitir el datagrama internet.

En el caso de ARPANET, por ejemplo, el módulo internet llamaría a un módulo de red local el cual añadiría el encabezado 1822 [2] al datagrama internet creando así un mensaje ARPANET a transmitir al IMP. La dirección ARPANET sería deducida de la dirección internet por la interfaz de la red local y sería la dirección de algún host en ARPANET, el cual podría ser una pasarela a otras redes.

1.4. Operación

El protocolo internet implementa dos funciones básicas: direccionamiento y fragmentación.

Los módulos internet usan las direcciones que se encuentran en la cabecera internet para transmitir los datagramas internet hacia sus destinos. La selección de un camino para la transmisión se llama encaminamiento.

Los módulos internet usan campos en la cabecera internet para fragmentar y reensamblar los datagramas internet cuando sea necesario para su transmisión a través de redes de "trama pequeña".

El modelo de operación es que un módulo internet reside en cada host involucrado en la comunicación internet y en cada pasarela que interconecta redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar datagramas internet. Además, estos módulos (especialmente en las pasarelas) tienen procedimientos para tomar decisiones de encaminamiento y otras funciones.

El protocolo internet trata cada datagrama internet como una entidad independiente no relacionada con ningún otro datagrama internet. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo)

El protocolo internet utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de Cabecera.

El Tipo de Servicio se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. Esta indicación de tipo de servicio

será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama internet.

El Tiempo de Vida es una indicación de un límite superior en el periodo de vida de un datagrama internet. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el datagrama llegue a su destino, el datagrama internet es destruído. Puede pensarse en el tiempo de vida como en un plazo de autodestrucción.

Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y encaminamiento especial.

La Suma de Control de Cabecera proporciona una verificación de que la información utilizada al procesar el datagrama internet ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control de cabecera falla, el datagrama internet es descartado inmediatamente por la entidad que detecta el error.

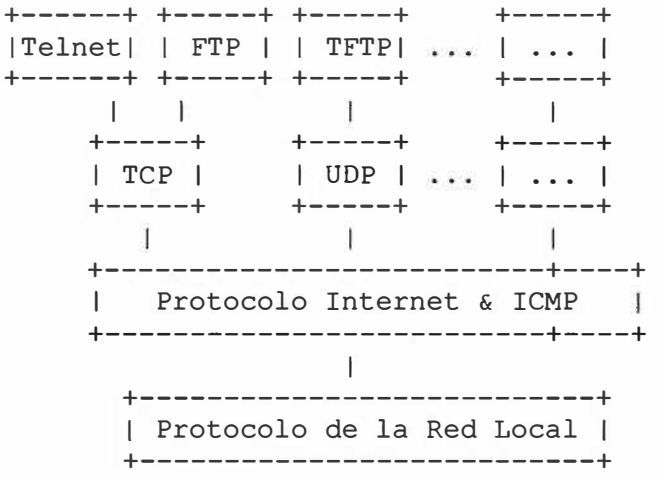
El protocolo internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo ni entre extremos ni entre saltos. No hay control de errores para los datos, sólo una suma de control de cabecera. No hay retransmisiones. No existe control de flujo.

Los errores detectados pueden ser notificados por medio del Internet Control Message Protocol (ICMP) (Protocolo de Mensajes de Control de Internet) [3] el cual está implementado en el módulo del protocolo internet.

2. PANORAMA GENERAL

2.1. Relación con Otros Protocolos

El siguiente diagrama ilustra el lugar del protocolo internet en la jerarquía de protocolos:



Relación entre Protocolos

Figura 1.

El protocolo Internet interactúa por un lado con los protocolos host-a-host de alto nivel y por otro con el protocolo de la red local. En este contexto una "red local" puede ser una pequeña red en un edificio o una gran red como ARPANET.

2.2. Modelo de Operación

El modelo de operación para transmitir un datagrama de una aplicación a otra se ilustra en el siguiente escenario:

Suponemos que esta transmisión involucra a una pasarela intermedia.

La aplicación remitente prepara sus datos y llama a su módulo internet local para enviar esos datos como un datagrama y pasa la dirección de destino y otros parámetros como argumentos de la llamada.

El módulo internet prepara una cabecera de datagrama y adjunta los datos a él. El módulo internet determina una dirección de la red de área local para esta dirección internet, que en este caso es la dirección de una pasarela.

Envía este datagrama y la dirección de red local a la interfaz de red local.

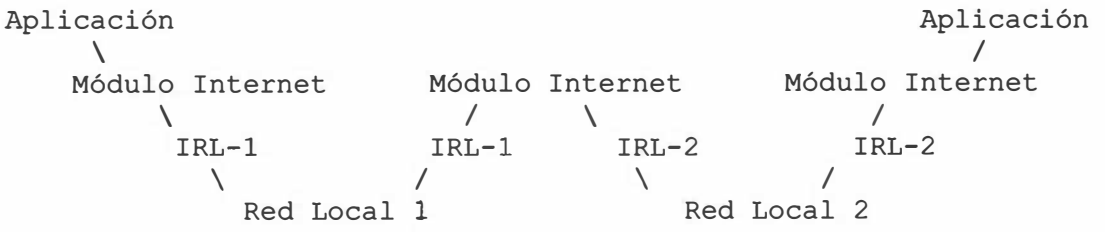
La interfaz de red local crea una cabecera de red local, le adjunta el datagrama y entonces envía el resultado a través de la red local.

El datagrama llega a un host pasarela encapsulado en la cabecera de red local, la interfaz de red local desprende esta cabecera y dirige el datagrama hacia el módulo internet. El módulo internet determina a partir de la dirección internet que el datagrama debe ser reenviado a otro host en una segunda red. El módulo internet determina una dirección de red local para el host de destino. Llama a la interfaz de red local de esa red para enviar el datagrama.

Esta interfaz de red local crea una cabecera de red local y le adjunta el datagrama enviando el resultado al host de destino.

En este host de destino la interfaz de red local le quita al datagrama la cabecera de red local y se lo pasa al módulo internet.

El módulo internet determina que el datagrama va dirigido a una aplicación en este host. Pasa los datos a la aplicación en respuesta a una llamada al sistema, pasando la dirección de origen y otros parámetros como resultado de la llamada.



Trayectoria de la transmisión

Figura 2

2.3. Descripción de Funciones

La función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas. Esto se consigue pasando los datagramas desde un módulo internet a otro hasta que se alcanza el destino. Los módulos internet residen en hosts y pasarelas en el sistema internet. Los datagramas son encaminados desde un módulo internet a otro a través de redes individuales basándose en la

interpretación de una dirección internet. Por eso, un importante mecanismo del protocolo internet es la dirección internet.

En el enrutamiento de mensajes desde un módulo internet a otro, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar ésta dificultad se proporciona un mecanismo de fragmentación en el protocolo internet.

Direccionamiento

Se establece una distinción entre nombres, direcciones y rutas [4]. Un nombre indica qué buscamos. Una dirección indica dónde está. Una ruta indica cómo llegar allí. El protocolo internet maneja principalmente direcciones. Es tarea de los protocolos de mayor nivel (es decir, protocolos host-a-host o entre aplicaciones) hacer corresponder nombres con direcciones. El módulo internet hace corresponder direcciones de internet con direcciones de red local. Es tarea de los procedimientos de menor nivel (es decir, redes locales o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de una longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección local (llamada el campo "resto"). Hay 3 formatos o clases de direcciones internet: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local.

Se debe tener cuidado al relacionar direcciones internet con direcciones de red local; un host individual físicamente hablando debe ser capaz de actuar como si fuera varios hosts distintos, hasta el punto de usar varias direcciones internet distintas. Algunos hosts tendrán también varios interfaces físicos (multi-homing).

Esto quiere decir que se debe establecer algún mecanismo que permita a un host tener varios interfaces físicos de red, cada uno de ellos con varias direcciones lógicas internet.

Se pueden encontrar ejemplos de correspondencias de direcciones en "Correspondencias de Direcciones" [5].

Fragmentación

La fragmentación de un datagrama internet es necesaria cuando éste se origina en una red local que permite un tamaño de paquete grande y debe atravesar una red local que limita los paquetes a un tamaño inferior para llegar a su destino.

Un datagrama internet puede ser marcado como "no fragmentar". Todo datagrama internet así marcado no será fragmentado entre distintas redes bajo ninguna circunstancia. Si un datagrama internet marcado como "no fragmentar" no puede ser entregado en su destino sin fragmentarlo, entonces debe ser descartado.

La fragmentación, transmisión y reensamblaje a través de una red local invisible para el módulo del protocolo internet se llama fragmentación intranet y puede ser utilizada [6].

El procedimiento de fragmentación y reensamblaje en internet tiene que ser capaz de dividir un datagrama en un número casi arbitrario de piezas que puedan ser luegos reensambladas. El receptor de los fragmentos utiliza el campo de identificación para asegurarse de que no se mezclan fragmentos de distintos datagramas. El campo posición ("offset") le indica al receptor la posición de un fragmento en el datagrama original. La posición y longitud del fragmento determinan la porción de datagrama original comprendida en este fragmento. El indicador "más-fragmentos" indica (puesto a cero) el último fragmento. Estos campos proporcionan información suficiente para reensamblar datagramas.

El campo identificador se usa para distinguir los fragmentos de un datagrama de los de otro. El módulo de protocolo de origen de un datagrama internet establece el campo identificador a un valor que debe ser único para ese protocolo y par origen-destino durante el tiempo que el datagrama estará activo en el sistema internet. El módulo de protocolo de origen de un datagrama completo pone el indicador "más-fragmentos" a cero y la posición del fragmento a cero.

Para fragmentar un datagrama internet grande, un módulo de protocolo internet (p. ej., en una pasarela) crea dos nuevos datagramas internet y copia el contenido de los campos de cabecera internet del datagrama grande en las dos cabeceras nuevas. Los datos del datagrama grande son divididos en dos trozos tomando una resolución mínima de 8 octetos (64 bits) (el segundo trozo puede no ser un múltiplo entero de 8 octetos, pero el primero sí debe serlo). Llamemos al número de bloques de 8 octetos en el primer trozo NFB (Number of Fragment Blocks: Número de Bloques del Fragmento). El primer trozo de datos es colocado en el primer nuevo datagrama internet y el campo longitud total se establece a la longitud del primer datagrama. El indicador "más fragmentos" es puesto a uno. El

segundo trozo de datos es colocado en el segundo nuevo datagrama internet y el campo longitud total se establece a la longitud del segundo datagrama. El indicador "más fragmentos" lleva el mismo valor que en el datagrama grande. El campo posición del segundo nuevo datagrama se establece al valor de ese campo en el datagrama grande más NFB.

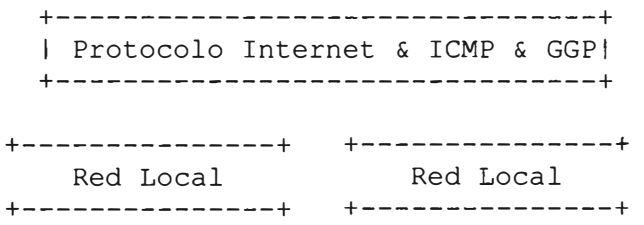
Este procedimiento puede generalizarse para una n-partición, mejor que para la división en dos partes descrita.

Para ensamblar los fragmentos de un datagrama internet, un módulo de protocolo internet (por ejemplo en un host de destino) combina todos los datagramas internet que tengan el mismo valor en los cuatro campos: identificación, origen, destino y protocolo. La combinación se realiza colocando el trozo de datos de cada fragmento en su posicıon relativa indicada por la posición del fragmento en la cabecera internet de ese fragmento. El primer fragmento tendrá posición cero, y el último fragmento tendrá el indicador "más fragmentos" puesto a cero.

2.4. Pasarelas

Las pasarelas implementan el protocolo internet para reexpedir datagramas entre redes. Las pasarelas también implementan el Protocolo Pasarela a Pasarela (Gateway to Gateway Protocol, GGP) [7] para coordinar el encaminamiento y otra información de control internet.

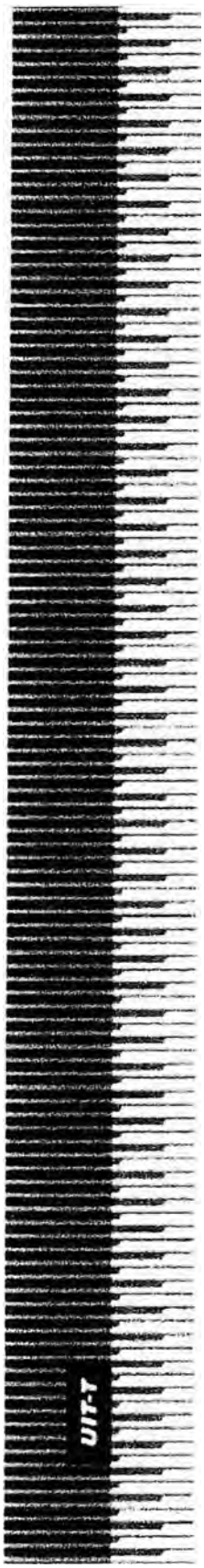
En una pasarela los protocolos de nivel superior no necesitan ser implementados y las funciones GGP son añadidas al módulo IP.



Protocolos de Pasarela

Figura 3.

ANEXO H
Protocolos H323



Unión Internacional de Telecomunicaciones

UIT-T H.225.0

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(05/2006)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIA

Infraestructura de los servicios audiovisuales – Multiplexación y sincronización en transmisión

Protocolos de señalización de llamada y paquetización de trenes de medios para sistemas de comunicación multimedia por paquetes

Recomendación UIT-T H.225.0

7.1 Utilización de mensajes Q.931

Las implementaciones seguirán la Rec. UIT-T Q.931 como se especifica en esta Recomendación. Los terminales pueden también soportar APDU H.450 opcionales en el elemento de información (IE) usuario-usuario. Los mensajes contendrán todos los elementos de información obligatorios y pueden contener cualquiera de los elementos de información opcionales definidos en la Rec. UIT-T Q.931 que se describen en esta Recomendación. Adviértase que el punto extremo H.225.0 puede, según la Rec. UIT-T Q.931, ignorar todos los mensajes opcionales que no soportan sin dañar la interoperabilidad, pero responderá a un mensaje desconocido con un mensaje de estado.

Cada punto extremo H.225.0 será capaz de recibir e identificar un mensaje de señalización de llamada H.225.0 incluso si contiene una APDU H.450 en el elemento de información usuario-usuario. Será capaz de procesar los mensajes de señalización de llamada H.225.0 obligatorios; puede ser capaz de procesar los mensajes de señalización de llamada H.225.0 opcionales. En cualquier caso, cada punto extremo H.225.0 será capaz de ignorar mensajes que le resulten desconocidos sin perturbar el funcionamiento.

Cada punto extremo H.225.0 será capaz de interpretar y generar los elementos de información que sean de su mandato en lo sucesivo para los respectivos mensajes de señalización de llamada H.225.0 y APDU H.450 en el elemento de información usuario-usuario. Podría interpretar y generar también los elementos de información opcionales definidos a continuación. Puede también interpretar otros elementos de información de Q.931 y otros protocolos de la serie Q o protocolos H.450. Los puntos extremos serán capaces de ignorar los elementos de información desconocidos contenidos en un mensaje de señalización de llamada H.225.0 o una APDU H.450 sin perturbar el funcionamiento. Los procedimientos para recibir elementos de información "se requiere comprensión" no reconocidos se aplicarán conforme a 5.8.7.1/Q.931. Los puntos extremos H.225.0 no enviarán múltiples elementos de información del mismo tipo en el mismo mensaje; por ejemplo, no enviarán múltiples elementos de información número de parte llamante según se describe en el anexo A/Q.951.3.

Los elementos de información se codificarán de acuerdo con la Rec. UIT-T Q.931, salvo aquellas partes en que se apliquen las modificaciones de la presente Recomendación. Sin embargo, se seguirá siempre el orden apropiado de los elementos de información dentro de un mensaje prescrito en la Rec. UIT-T Q.931, sin atender al orden de los elementos indicados en la presente Recomendación.

Los sistemas intermedios (pasarelas y controladores de acceso) seguirán las reglas siguientes en relación con los mensajes opcionales y elementos de información de señalización de llamada H.225.0:

1) La pasarela debe remitir y el controlador de acceso remitirá todos los elementos de información (opcionales u obligatorios) después de la modificación apropiada asociados con mensajes de señalización de llamada H.225.0 obligatorios sea desde el terminal a la pasarela/terminal o en sentido opuesto. Esto incluye elementos de información tales como información usuario-usuario y la información de visualización.

2) Una pasarela debe remitir todos los mensajes de señalización de llamada H.225.0, incluso si contienen una APDU H.450, y elementos de información en ambos sentidos.

3) Un controlador de acceso remitirá todos los mensajes de señalización de llamada H.225.0, incluso si contienen APDU H.450, y elementos de información en ambos sentidos después de la modificación apropiada. Obsérvese que es posible que el controlador de acceso actúe como un elemento de señalización que puede proporcionar características (tales como las características de los servicios suplementarios) y, por lo tanto, modificar, terminar u originar mensajes de señalización de llamada H.225.0.

Las pasarelas H.323 pueden convertir servicios suplementarios de la serie H.450 y mensajes H.225.0 a los correspondiente servicios y mensajes de ISO/CEI 11582, parte usuario de la RDSI y otras normas de señalización RCC. Los detalles están dentro del ámbito de la Rec. UIT-T H.246 y sus anexos.

Las pasarelas H.323 podrán hacer seguir mensajes de señalización de ISO/CEI 11582, la parte usuario de RDSI y otras normas de señalización, sin modificación, mediante la tunelización de señalización no H.323 en H.225.0. En el anexo M/H.323 M (véanse M.1/H.323. M.2/H.323, etc.) se presenta una información detallada.

En esta versión de esta Recomendación, todas las referencias corresponden a la versión 1998 de la Rec. UIT-T Q.931. Se siguen los procedimientos de 3.1/Q.931 para el establecimiento de conexión en modo circuito. Sin embargo, se recuerda al implementador que aunque el "portador" está siendo señalizado al efecto, no existen "canales B" efectivos del tipo RDSI en el lado red de paquetes. La "llamada" realizada con éxito da lugar a un canal fiable de extremo a extremo que soporta la mensajería H.245. Realmente, el establecimiento del "portador" se efectúa aplicando H.245. Sin embargo, la utilización de Q.931 en el lado red de paquetes permite el interfuncionamiento con Q.931 en el lado RCC así como el aprovisionamiento de un marco verificado para determinar las características generales de llamada orientadas a la conexión.

En general, se utilizan los procedimientos simétricos del anexo D/Q.931, lo cual implica que la máquina de estados Q.931 va seguida como se indica en el anexo D/Q.931 con la excepción de que el procedimiento de D.3/Q.931 (Colisión de llamadas) no se aplicará; la recuperación tras esta condición se deja a la capa de aplicación.

Los puntos extremos que no soporten juegos de códigos Q.931 con cambio a otros juegos ignorarán todos los mensajes Q.931 que utilicen dichos métodos.

El cuadro 4 muestra qué mensajes son obligatorios y opcionales para el establecimiento de la comunicación H.323 y H.225.0 utilizando Q.931 en la red de paquetes.

Cuadro 4/H.225.0 – Utilización de mensajes Q.931/Q.932 en H.225.0

	Transmisión (M, F, O, CM) (nota 1)	**Recepción y acción [M, F, O (nota 2), CM]**
Mensajes de establecimiento de la comunicación		
Aviso	M	M
Llamada en curso	O	CM (notas 3 y 6)
Conexión	M	M
Acuse de conexión	F	F
Progresión	O	CM (nota 6)
Establecimiento	M	M
Acuse de establecimiento	O	O
Mensajes de liberación de llamada		
Desconexión	F	F
Liberación	F	F
Liberación completa	M (nota 4)	M
Mensajes de la fase de información de llamada		
Reanudación	F	F
Acuse de reanudación	F	F
Rechazo de reanudación	F	F

Cuadro 4/H.225.0 – Utilización de mensajes Q.931/Q.932 en H.225.0

	Transmisión (M, F, O, CM) (nota 1)	**Recepción y acción [M, F, O (nota 2), CM]**
Suspensión	F	F
Acuse de suspensión	F	F
Rechazo de suspensión	F	F
Información de usuario	O	O
Mensajes varios		
Control de congestión	F	F
Información	O	CM (nota 6)
Notificación	O	O
Estado	M (nota 5)	M
Indagación de estado	O	M
Mensajes Q.932/H.450		
Facilidad	M	M
Retención	F	F
Acuse de retención	F	F
Rechazo de retención	F	F
Recuperación	F	F
Acuse de recuperación	F	F
Rechazo de recuperación	F	F

NOTA 1 – M: Obligatorio (*mandatory*), F: Prohibido (*forbidden*), O: Facultativo (u opcional), CM: Condicionalmente obligatorio *(conditionally mandatory)*. Un mensaje es condicionalmente obligatorio si es obligatorio cuando es soportada una opción.

NOTA 2 – Obsérvese que no se enviará el mensaje Estado en respuesta a un mensaje indicado como "O" en el presente cuadro El receptor simplemente pasará por alto el mensaje si no lo soporta.

NOTA 3 – Los terminales que han de utilizar pasarelas recibirán y actuarán al recibir Llamada en curso.

NOTA 4 – Liberación completa se necesita para cerrar el canal de señalización de llamada fiable H.225.0. No obstante, el canal de señalización de llamada se mantendrá abierto si otras llamadas que utilizan el mismo canal de señalización de llamada siguen en curso. Adicionalmente, el controlador de acceso puede fijar la bandera **maintainConnection** en VERDADERO para evitar el cierre del canal de señalización de llamada.

NOTA 5 – El punto extremo responderá a un mensaje desconocido con un mensaje Estado; es también obligatoria la respuesta a Indagación de estado. Sin embargo, un punto extremo no tiene que enviar Indagación de estado. Como un asunto práctico, el punto extremo debe ser capaz de comprender un mensaje Estado recibido en respuesta a un mensaje enviado que no es conocido para el receptor.

NOTA 6 – Los puntos extremos que soporten las características facultativas que utilizan estos mensajes (por ejemplo, la tunelización H.245, los servicios suplementarios H.450, la tunelización de los protocolos de señalización o las características que utilizan **genericData**) deberán procesar estos mensajes.

7.2 Elementos de información Q.931 comunes

7.2.1 Elementos de información de encabezamiento

Para todos los mensajes de señalización de llamada H.225.0, hay tres campos comunes que son obligatorios, además del tipo de mensaje, que se describe en esta cláusula.

7.2.1.1 Discriminador de protocolo

Se define en 4.2/Q.931.

Se pondrá a 08H – esto identifica el mensaje como mensaje usuario-red Q.931/I.451 (codificado según la figura 4-2/Q.931). Si un controlador de acceso está actuando como una red para suministrar servicios suplementarios, puede ser adecuado utilizar otro valor. Este asunto queda en estudio.

7.2.1.2 Referencia de llamada

Se define en 4.3/Q.931.

Se soportará una longitud de valor de referencia de llamada de dos octetos por cualquier punto extremo H.323.

El valor de referencia de llamada se elige en el lado que origina la llamada y tiene que ser localmente exclusivo. En una comunicación posterior, el lado llamante y el lado llamado utilizarán este valor de referencia de llamada en todos los mensajes pertenecientes a esta llamada determinada.

El valor se codifica según la figura 4-5/Q.931 para un valor de referencia de llamada de dos octetos. El octeto más significativo del valor de referencia se codifica siempre en el octeto N.° 2.

Obsérvese que el CRV es sólo exclusivo en una determinada parte de una llamada, por ejemplo, entre los terminales, o entre un terminal y un controlador de acceso. Si un determinado terminal tiene dos llamadas en la misma conferencia, cada uno tendrá el mismo ID de conferencia, pero diferentes CRV.

La bandera de referencia de llamada se fijará de acuerdo con los procedimientos descritos en la Rec. UIT-T Q.931.

Nótese que los valores CRV enviados en mensajes RAS se ajustarán a la estructura indicada en la Rec. UIT-T Q.931. Concretamente, la bandera de referencia de llamada se incluirá como el bit más significativo del valor de referencia de llamada. Esto limita el CRV real a la gama de 0 a 32 767, inclusive.

La referencia de llamada global, que se muestra en la figura 4-5/Q.931 y tiene el valor numérico 0, se utiliza para hacer referencia a todas las llamadas en el canal de señalización de llamada o en el canal RAS.

7.2.1.3 Tipo de mensaje

El tipo de mensaje se codifica según la figura 4-6/Q.931 utilizando los valores especificados en el cuadro 4-2/Q.931. Quedan en estudio las extensiones específicas de H.225.0.

7.2.2 Elementos de información específicos del mensaje

Las reglas de codificación generales para los elementos de información siguientes se definen en 4.5.1/Q.931 y en el cuadro 4-3/Q.931. Se seguirán estas reglas. El mecanismo de escape (véase la figura 4-8/Q.931) es opcional.

7.2.2.1 Capacidad portadora

Este elemento de información se codifica de acuerdo con la figura 4-11/Q.931 y el cuadro 4-6/Q.931. Si este elemento de información se recibe en una llamada de red de paquetes a red de paquetes puede ser ignorada por el receptor. Si este elemento de información aparece en un mensaje de establecimiento de la comunicación para una conexión de señalización independiente de la llamada, definida en la Rec. UIT-T H.450.1 la codificación se ajustará a 7.2.2.1.2. En todos los demás casos, la codificación deberá ajustarse a 7.2.2.1.1. Las referencias de números de octeto remiten a la figura 4-11/Q.931.

7.2.2.1.1 Codificación por defecto de la capacidad portadora

Las entidades H.323 codificarán los elementos de información de capacidad portadora como se indica a continuación, a menos que se señale otra cosa en las cláusulas subsiguientes.

Bit de extensión para el octeto N.º 3 (bit 8)

Se pondrá a "1".

Norma de codificación (octeto N.º 3, bits 6-7)

Se pondrá a "00" indicando "UIT-T".

Capacidad de transferencia de información (octeto N.º 3, bits 1-5)

Para llamadas originadas en un punto extremo de RDSI se remitirá la información indicada a la pasarela.

NOTA – Esto permite obtener alguna información adelantada sobre la naturaleza de la conexión que ha de remitirse al punto extremo H.323, por ejemplo, voz solamente *versus* datos *versus* vídeo; esto tendría repercusión en la anchura de banda requerida así como en la aptitud/voluntad de aceptar o no la llamada.

Las llamadas que se originan en un punto extremo H.323 utilizarán este campo para indicar su deseo de efectuar una llamada audiovisual. Por tanto, el campo se pondrá a "información digital sin restricciones", es decir, "01000" o a "información digital restringida" es decir "01001". Si ha de efectuarse una llamada sólo vocal, el terminal H.323 pondrá la capacidad de transferencia de información a "conversación" (es decir "00000") o a "audio a 3,1 kHz" (es decir "10000").

Bit de extensión para el octeto N.º 4 (bit 8)

Se pondrá a "0" si la velocidad de transferencia de información se pone a "multivelocidad"; se pondrá a "1" en otro caso.

Modo de transferencia (octeto N.º 4, bits 6-7)

Especificará "modo circuito", valor "00".

Velocidad de transferencia de información (octeto N.º 4, bits 1-5)

Se codificará siguiendo el cuadro 4-6/Q.931, salvo que el valor "00000" (para el modo paquete) no se permite a menos que la pasarela se conecte a una red de paquetes.

Multiplicador de velocidad (octeto N.º 4.1)

Estará presente si la velocidad de transferencia de información se pone a "multivelocidad".

El bit de extensión (bit 8) se pondrá a "1".

Los bits 1 a 7 indicarán la anchura de banda necesaria para la llamada definida a continuación (nótese que, contrariamente a la Rec. UIT-T Q.931, se permite aquí un valor de "0000001").

Para una llamada originada en un punto extremo de RDSI, la pasarela pasará simplemente la información que recibe de la RDSI.

Para una llamada entrante procedente de un punto extremo H.324, la pasarela fijará el multiplicador de velocidad a 01H.

Para una llamada entrante procedente de una RDSI-BA, es necesario efectuar cierta traducción de la Rec. UIT-T Q.2931 a la Rec. UIT-T Q.931. Este asunto queda en estudio.

Para una llamada originada en un punto extremo H.323, éste se utilizará para indicar la anchura de banda a utilizar para esta llamada. Si el sistema llamado es otro punto extremo H.323, este valor puede reflejar la anchura de banda a utilizar en la red de paquetes, pero no es necesario que el terminal de recepción siga esta información. Si interviene una pasarela,

este valor reflejará entonces el número de conexiones externas a establecer. La anchura de banda necesaria para la llamada es la anchura de banda requerida en el lado RCC y puede o no concordar con la anchura de banda permitida en la red de paquetes por los mensajes ACF/BCF.

Protocolo de capa 1 (octeto N.º 5)

El bit de extensión (bit 8) se pondrá a "1".

Los bits 6 y 7 indicarán el identificador de capa 1, es decir, "01".

Los bits 1 a 5 indicarán el protocolo de capa 1.

Los valores permitidos son G.711 (ley A "00011" y ley μ "00010") para indicar una llamada sólo voz y H.221 y H.242 ("00101") para indicar una llamada videotelefónica H.323.

Los octetos N.º 5a, 5b, 5c, 5d, 6 y 7 no estarán presentes.

7.2.2.1.2 Codificación de la capacidad portadora para conexiones de señalización H.450.1 independientes de la llamada

Las entidades H.323 codificarán el elemento de información capacidad portadora como se indica a continuación para las conexiones de señalización independientes de la llamada definidas en la Rec. UIT-T H.450.1.

Bit de extensión para el octeto N.º 3 (bit 8)

Se pondrá a "1".

Norma de codificación (octeto N.º 3, bits 6-7)

Se pondrá a "01" indicando "Otra norma internacional". Se señala que, cuando se indique esta norma de codificación, deberá aplicarse la codificación definida en la Rec. UIT-T Q.931 para los octetos 1 a 2 y el bit 8 de los octetos 3 a 4. La capacidad de transferencia de información, el modo de transferencia y la velocidad de transferencia de información se codificarán como se indica sin incluir ningún otro octeto.

Capacidad de transferencia información (octeto N.º 3, bits 1-5)

Se pondrá a "01000", indicando "Información digital sin restricciones".

Bit de extensión para el octeto N.º 4 (bit 8)

Se pondrá a "1".

Modo de transferencia (octeto N.º 4, bits 6-7)

Se pondrá a "00", indicando "Conexión de señalización independiente de la llamada".

Velocidad de transferencia de información (octeto N.º 4, bits 1-5)

Se pondrá a "00000", indicando "Capacidad de señalización independiente de la llamada".

No se incluirán los octetos 4.1 y superiores.

7.2.2.2 Identidad de la llamada

El posible uso del elemento de información identidad de llamada queda en estudio. En este estudio se debe considerar la marcación en múltiples etapas incluidas terminal-a-controlador-de-acceso-a-terminal, y terminal-a-pasarela-a-terminal y, encaminamiento de fuente flexible.

7.2.2.3 Estado de la llamada

Este elemento de información se codifica según la figura 4-13/Q.931.

Octeto N.º 3 norma de codificación (bits 8-7)

Se pone a "00" para codificación normalizada indicando UIT-T.

Valor de estado de la llamada (octeto N.º 3, bits 1-6)

Fijado como en el cuadro 4-8/Q.931, pero no se utilizan los valores globales de estado de la interfaz. Los valores se interpretan como estado de usuario tal como se usa en el anexo D/Q.931. Adviértase que la mayoría de los códigos enumerados no serán generados por un terminal H.323.

7.2.2.4 Número de la parte llamada

Este elemento de información se codifica según la figura 4-14/Q.931 y el cuadro 4-9/Q.931.

Octeto N.º 3 extensión (bit 8)

Puesto a "1".

Tipo de número (octeto N.º 3, bits 5-7)

Codificado según los valores y reglas del cuadro 4-9/Q.931.

Identificación del plan de numeración (octeto N.º 3, bits 1-4)

Codificado según los valores y reglas del cuadro 4-9/Q.931. Un número en forma de una cadena de dígitos marcada debe codificarse como "0000" (desconocido). Si está puesto a "1001" (plan de numeración privado) en una llamada originada en una red de paquetes, esto indica que:

1) la cadena de dígitos marcada no está presente en Establecimiento; y
2) la llamada se encaminará mediante una dirección de alias en la información usuario-usuario.

Tipo de número (octeto N.º 3, bits 5-7)

Codificado según los valores y reglas del cuadro 4-9/Q.931. Un número con la identificación de plan de numeración codificada como "0000" (desconocido) se codificará como "000" (desconocido). Un número con la identificación de plan de numeración codificada como "0001" (plan de numeración RDSI/telefonía, Rec. UIT-T E.164) con el tipo de número codificado como "000" (desconocido) puede utilizarse para compatibilidad hacia atrás.

"Dígitos" de número

Cualquier número de caracteres IA5, según los formatos especificados en el plan de numeración/marcación apropiado.

NOTA – Un número E.164 estará formado solamente por los caracteres IA5 "0", "1", "2", "3", "4", "5", "6", "7", "8" y "9".

7.2.2.5 Subdirección de la parte llamada

Se utiliza como en la Rec. UIT-T Q.931.

7.2.2.6 Número de la parte llamante

Este elemento de información se codifica según la figura 4-16/Q.931 y el cuadro 4-11/Q.931.

Tipo de número (octeto N.º 3, bits 5-7)

Codificado según los valores y reglas del cuadro 4-11/Q.931. Un número con la identificación de plan de numeración codificada como "0000" (desconocido) se codificará como "000" (desconocido). Un número con la identificación de plan de numeración codificada como "0001" (plan de numeración RDSI/telefonía, Rec. UIT-T E.164) con el

tipo de número codificado como "000" (desconocido) puede utilizarse para compatibilidad hacia atrás.

Identificación del plan de numeración (octeto N.º 3, bits 1-4)

Codificada según los valores y reglas del cuadro 4-11/Q.931. Un número en forma de una cadena de dígitos marcada debe codificarse como "0000" (desconocido). Si está puesto a "1001" (plan de numeración privado) en una llamada originada en una red de paquetes, esto indica que:

1) la cadena de dígitos marcada no está presente en Establecimiento; y
2) la llamada se encaminará mediante una dirección de alias en la información usuario-usuario.

Octeto N.º 3a

Codificado según los valores y reglas del cuadro 4-11/Q.931.

"Dígitos" de número

Cualquier número de caracteres IA5, según los formatos especificados en el plan de numeración/marcación apropiado.

NOTA – Un número E.164 estará formado solamente por los caracteres IA5 "0", "1", "2", "3", "4", "5", "6", "7", "8" y "9".

Los puntos extremos H.323 no enviarán múltiples elementos de información número de la parte llamante en el mismo mensaje. Las pasarelas pueden facilitar el interfuncionamiento con los mensajes ESTABLECIMIENTO Q.931 que contienen múltiples elementos de información número de la parte llamante. Las pasarelas que faciliten ese soporte deberán establecer la correspondencia entre el primer elemento de información número de la parte llamante Q.931 y el elemento información número de la parte llamante del mensaje Establecimiento H.225.0, así como las correspondencias subsiguientes entre los elementos de información número de la parte llamante Q.931 y el campo **additionalSourceAddresses** del mensaje Establecimiento H.225.0. Los controladores de acceso que encaminan mensajes de establecimiento iniciados en un punto extremo H.323 pueden incluir un número en el campo **additionalSourceAddresses** antes de reenviar el mensaje al siguiente destinatario.

7.2.2.7 Subdirección de la parte llamante

Se utiliza como en la Rec. UIT-T Q.931.

7.2.2.8 Causa

Si se recibe, se aplican las reglas definidas en la Rec. UIT-T Q.850. Obsérvese que, o bien Causa o **ReleaseCompleteReason** es obligatorio para Liberación completa; el IE Causa es facultativo en cualquier otra parte. El IE Causa y el **ReleaseCompleteReason** (**motivo de liberación completa**) (una parte del mensaje Liberación completa) se excluyen mutuamente. Las pasarelas establecerán una correspondencia de **ReleaseCompleteReason** al IE Causa cuando se envíe un mensaje Liberación completa del lado red con conmutación de paquetes al lado red con conmutación de circuitos (véase el cuadro 5). (No se requiere la correspondencia inversa ya que las entidades de red de paquetes tienen que decodificar el IE Causa.)

Asimismo, las pasarelas establecerán una correspondencia de **AdmissionRejectReason** y **LocationRejectReason** al IE Causa cuando se envíe un mensaje Liberación completa al lado red con conmutación de circuitos tras haber recibido un **AdmissionReject** o un **LocationReject** (cuadro 6).

Cuadro 5/H.225.0 – Correspondencia de ReleaseCompleteReason al IE Causa

Código ReleaseCompleteReason	Valor de causa Q.931/Q.850 correspondiente
noBandwidth	34 – No hay circuito/canal disponible
gatekeeperResources	47 – Recurso no disponible, no especificado
unreachableDestination	3 – No hay ruta hacia el destino
destinationRejection	16 – Liberación normal de la llamada
invalidRevision	88 – Destino incompatible
noPermission	127 – Interfuncionamiento, no especificado
unreachableGatekeeper	38 – Red fuera de servicio
gatewayResources	42 – Congestión en el equipo de conmutación
badFormatAddress	28 – Formato de número no válido (dirección incompleta)
adaptiveBusy	41 – Fallo temporal
inConf	17 – Usuario ocupado
undefinedReason	31 – Normal, no especificado
facilityCallDeflection	16 – Liberación normal de la llamada
securityDenied	31 – Normal, no especificado
securityWrongSyncTime	31 – Normal, no especificado
securityReplay	31 – Normal, no especificado
securityWrongGeneralID	31 – Normal, no especificado
securityWrongSendersID	31 – Normal, no especificado
securityMessageIntegrityFailed	31 – Normal, no especificado
securityWrongOID	31 – Normal, no especificado
securityDHmismatch	31 – Normal, no especificado
securityCertificateExpired	31 – Normal, no especificado
securityCertificateDateInvalid	31 – Normal, no especificado
securityCertificateRevoked	31 – Normal, no especificado
securityCertificateNotReadable	31 – Normal, no especificado
securityCertificateSignatureInvalid	31 – Normal, no especificado
securityCertificateMissing	31 – Normal, no especificado
securityCertificateIncomplete	31 – Normal, no especificado
securityUnsupportedCertificateAlgOID	31 – Normal, no especificado
securityUnknownCA	31 – Normal, no especificado
calledPartyNotRegistered	20 – Abonado ausente
callerNotRegistered	31 – Normal, no especificado
newConnectionNeeded	47 – Recurso no disponible, no especificado
nonStandardReason	127 – Interfuncionamiento, no especificado
replaceWithConferenceInvite	31 – Normal, no especificado
genericDataReason	31 – Normal, no especificado
neededFeatureNotSupported	31 – Normal, no especificado
tunnelledSignallingRejected	127 – Interfuncionamiento, no especificado
InvalidCID	3 – No hay ruta hacia el destino
hopCountExceeded	3 – No hay ruta hacia el destino

Cuadro 6/H.225.0 – Correspondencia de AdmissionRejectReason/ LocationRejectReason al IE Causa

Código AdmissionRejectReason o LocationRejectReason	Valor de causa Q.931/Q.850 correspondiente
calledPartyNotRegistered	20 – Abonado ausente
invalidPermission	127 – Interfuncionamiento, no especificado
requestDenied	31 – Normal, no especificado
undefinedReason	31 – Normal, no especificado
callerNotRegistered	31 – Normal, no especificado
routeCallToGatekeeper	No aplicable
invalidEndpointIdentifier	127 – Interfuncionamiento, no especificado
resourceUnavailable	47 – Recurso no disponible, no especificado
securityDenial	31 – Normal, no especificado
qosControlNotSupported	63 – Servicio u opción no disponible, no especificado
incompleteAddress	28 – Formato de número no válido (dirección incompleta)
aliasesInconsistent	31 – Normal, no especificado
routeCallToSCN	3 – No hay ruta hacia el destino
exceedsCallCapacity	41 – Fallo temporal
collectDestination	31 – Normal, no especificado
collectPIN	31 – Normal, no especificado
genericDataReason	31 – Normal, no especificado
neededFeatureNotSupported	31 – Normal, no especificado
securityWrongSyncTime	31 – Normal, no especificado
securityReplay	31 – Normal, no especificado
securityWrongGeneralID	31 – Normal, no especificado
securityWrongSendersID	31 – Normal, no especificado
securityIntegrityFailed	31 – Normal, no especificado
securityWrongOID	31 – Normal, no especificado
secuirtyDHMismatch	31 – Normal, no especificado
noRouteToDestination	3 – No hay ruta hacia el destino
unallocatedNumber	1 – Número no atribuido (no asignado)
noBandwidthAvailable	34 – No hay ningún circuito o canal disponible

7.2.2.9 Identificación de canal

La utilización queda en estudio; puede utilizarse para proporcionar una reacción a múltiples intentos de llamada.

7.2.2.10 Número conectado

Codificado conforme a 5.4.1/Q.951.

7.2.2.11 Subdirección conectada

Codificada conforme a 5.4.2/Q.951.

7.2.2.12 Nivel de congestión

No se utilizará.

7.2.2.13 Fecha/hora

Codificado según la figura 4-21/Q.931.

7.2.2.14 Visualización

Codificado según la figura 4-22/Q.931. La longitud máxima del elemento de información completo es 82 octetos.

7.2.2.15 Elemento de información Facilidad ampliada

Cualquier IE Facilidad ampliada utilizado para indicar una semántica sin modificaciones, tal como se define en las Recomendaciones de la serie Q.95.x, se codificará de acuerdo con 8.2.4/Q.932. En este caso, las ADU de servicio se formarán de acuerdo con ROSE (utiliza la Rec. UIT-T X.680 (Especificación de la ASN.1) y la Rec. UIT-T X.690 (Especificación de las reglas de codificación básica de la ASN.1)) como se define en la Rec. UIT-T X.229.

7.2.2.16 Facilidad

Para señalizar la redirección de llamada específica de los procedimientos H.323 (reenvío de llamada, redireccionamiento de una llamada al MC, o reencaminamiento forzado de una llamada hacia el controlador de acceso) o, en el caso de servicios suplementarios, señalización según la Rec. UIT-T H.450, se utiliza el elemento de información usuario-usuario del mensaje facilidad. Este caso particular se indicará codificando un IE Facilidad de longitud cero; es decir, el elemento de información Facilidad constará exactamente de 2 octetos, como sigue:

- Octeto N.º 1 (identificador del elemento de información) se pondrá a "00011100" ("1C'H) para indicar el IE Facilidad.

  Octeto N.º 2 (longitud del elemento de información) se pondrá a "0" para indicar que no siguen más octetos pertenecientes a este elemento de información.

Para indicar el reenvío de llamada, el IE Facilidad estará vacío y en el **UUIE Facilidad** se indicará en **dirección alternativa (alternativeAddress)** o **dirección alias alternativa (alternativeAliasAddress)** el terminal al que será redirigida la llamada. En este caso, **motivo de la facilidad (facilityReason)** se fijará en **llamada reenviada (callForwarded)**.

Para ordenar a un punto extremo que llame a un punto extremo diferente porque el punto extremo llamante desea incorporarse a una conferencia y el punto extremo llamado no tiene el MC, el IE Facilidad se podría también dejar vacío. El **ID de conferencia** indicará la conferencia a la que se ha de incorporar y el motivo en el **UUIE Facilidad** será **encaminar llamada a MC**.

Además, para ordenar al punto extremo llamante que señalice al punto extremo llamado a través del controlador de acceso del punto extremo llamado, el IE Facilidad se deja vacío. El **ID de conferencia** en el **UUIE Facilidad** indicará la conferencia a la que se ha de incorporar y el motivo en el **UUIE Facilidad** será **encaminar llamada a controlador de acceso**.

Cualquier IE Facilidad ampliada utilizado para indicar una semántica sin modificaciones, tal como se define en las Recomendaciones de la serie Q.95.x, se codificará de acuerdo a 8.2.3/Q.932. En este caso, las ADU de servicio se formarán de acuerdo con ROSE (utiliza la Rec. UIT-T X.680 (Especificación de la ASN.1) y la Rec. UIT-T X.690 (Especificación de las reglas básicas de codificación de la ASN.1)) como se define en la Rec. UIT-T X.229.

7.2.2.17 Compatibilidad de capa alta

Queda en estudio.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.235

(02/98)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIOS

Infraestructura de los servicios audiovisuales – Aspectos de los sistemas

Seguridad y criptado para terminales multimedios de la serie H (basados en las Recomendaciones H.323 y H.245)

Recomendación UIT-T H.235

(Anteriormente Recomendación del CCITT)

abreviaturas de tres letras (**ARQ**); los nombres de mensajes Q.931 están formados por una o dos palabras cuya letra inicial aparece en mayúsculas [**Llamada en curso (Call Proceeding)**].

6 Presentación del sistema

6.1 Resumen

1) El canal de señalización de llamada se puede asegurar utilizando TLS [**TLS**] o IPSEC [**13/IPSEC**] en un puerto conocido seguro (H.225.0).

2) Los usuarios pueden ser autenticados durante la conexión de llamada inicial, en el proceso de asegurar el canal H.245 y/o intercambiando certificados por el canal H.245.

3) Las capacidades de criptación de un canal de medios son determinadas por extensiones del mecanismo de negociación de capacidades existente.

4) La distribución inicial de material de claves del terminal director se efectúa mediante mensajes **Apertura canal lógico (OpenLogicalChannel)** o **Acuse apertura canal lógico (OpenLogicalChannelAck)**.

5) El recifrado se puede realizar mediante las instrucciones H.245: **Petición actualización criptación (EncryptionUpdateRequest)** y **Actualización criptación (EncryptionUpdate)**.

6) La distribución de material de claves se protege haciendo funcionar el canal H.245 como un canal privado o protegiendo específicamente el material de claves mediante el uso de certificados intercambiados seleccionados.

7) Los protocolos de seguridad presentados se conforman con las normas publicadas de la ISO o con las normas propuestas de IETF.

6.2 Autenticación

El proceso de autenticación verifica que los respondedores son, de hecho, quienes dicen ser. La autenticación se puede realizar junto con el intercambio de certificados basados en claves públicas. Se puede efectuar también por un intercambio que utiliza un secreto compartido entre las entidades participantes. Éste puede ser una contraseña estática o alguna otra pieza previa de información.

La presente Recomendación describe el protocolo para intercambiar los certificados, pero no especifica los criterios por los cuales éstos son verificados y aceptados mutuamente. En general, los certificados dan cierta seguridad al verificador de que el presentador del certificado es quien dice ser. La intención del intercambio de certificados es autenticar al *usuario* del punto extremo, no simplemente al punto extremo físico. Cuando se utilizan certificados digitales, un protocolo de autenticación prueba que los respondedores poseen las claves privadas correspondientes a las claves públicas contenidas en los certificados. Esta autenticación protege contra ataques intermedios, pero no prueba automáticamente quiénes son los respondedores. Para esto se requiere normalmente que haya alguna política relativa a otro contenido de los certificados. Por ejemplo, para los certificados de autorización, el certificado contendría normalmente la identificación del proveedor de servicio junto con alguna forma de identificación de cuenta de usuario prescrita por el proveedor de servicio.

El marco de autenticación de la presente Recomendación no prescribe el contenido de los certificados (es decir, no especifica una política de certificado) además de lo requerido por el protocolo de autenticación, sin embargo, una aplicación que utiliza este marco puede imponer requisitos de política de alto nivel tales como presentar el certificado al usuario para aprobación. Esta política de alto nivel puede ser automatizada dentro de la aplicación o requerir la interacción humana.

Para la autenticación que no utiliza certificados digitales, la presente Recomendación proporciona la señalización para completar distintos casos de pregunta/respuesta. Este método de autenticación requiere la coordinación previa por las entidades comunicantes de modo que se pueda obtener un secreto compartido. Un ejemplo de este método sería un cliente de un servicio basado en abono.

Como una tercera opción, la autenticación puede ser completada dentro del contexto de un protocolo de seguridad distinto, tal como TLS [**TLS**] o IPSEC [**13/IPSEC**].

La autenticación bidireccional y unidireccional puede ser admitida por entidades pares. Esta autenticación se puede producir en algunos o en todos los canales de comunicación.

Todos los mecanismos de autenticación específicos descritos en la presente Recomendación son idénticos a los algoritmos desarrollados por la ISO o derivados de éstos, como se especifica en las Partes 2 a 3 de ISO/CEI 9798 o están basados en protocolos IETF.

6.2.1 Certificados

La normalización de certificados, incluida su generación, administración y distribución, está fuera del alcance de la presente Recomendación. Los certificados utilizados para establecer canales seguros (señalización de llamada y/o control de llamada) se conformarán a los prescritos por cualquier protocolo que haya sido negociado para asegurar el canal.

Cabe señalar que para la autenticación que utiliza certificados de clave pública, los puntos extremos tienen que proporcionar firmas digitales utilizando el valor de clave privada asociado. El intercambio de certificados de clave pública por sí solo no protege contra ataques intermedios. Los protocolos H.235 cumplen este requisito.

6.3 Seguridad de establecimiento de la llamada

Hay por lo menos dos razones para motivar la seguridad del canal de establecimiento de llamada (por ejemplo, H.323 que utiliza Q.931). La primera es la autenticación simple, antes de aceptar la llamada. La segunda razón es tener en cuenta la autorización de la llamada. Si esta funcionalidad se desea en el terminal de la serie H, se debe utilizar un modo seguro de comunicación (tal como TLS/IPSEC para H.323) antes del intercambio de mensajes de conexión de la llamada. Como otra posibilidad, la autorización se puede proporcionar sobre la base de una autenticación específica del servicio. Las constricciones de una política de autorización específica del servicio están fuera del alcance de la presente Recomendación.

6.4 Seguridad de control de la llamada (H.245)

El canal de control de llamada (H.245) debe estar asegurado también de alguna manera para proporcionar privacidad de los medios subsiguientes. El canal H.245 se asegurará utilizando cualquier mecanismo de privacidad negociado (esto incluye la opción "ninguno"). Los mensajes H.245 se utilizan para señalizar algoritmos de criptación y claves de criptación utilizados en los canales de medios privados compartidos. La capacidad de hacer esto, canal lógico por canal lógico, permite que diferentes canales de medios sean encriptados por diferentes mecanismos. Por ejemplo, en conferencias multipunto centralizadas, es posible utilizar diferentes claves para los trenes a cada punto extremo. Esto puede permitir que los trenes de medios sean privados para cada punto extremo en la conferencia. Para utilizar los mensajes H.245 de una manera segura, todo el canal H.245 (canal lógico 0) se debe abrir de una manera segura negociada.

El mecanismo por el cual el canal H.245 es seguro depende de los terminales de la serie H participantes. El único requisito en todos los sistemas que utilizan esta estructura de seguridad es que cada uno tenga alguna manera de negociar y/o señalizar que el canal H.245 ha de funcionar de una

manera particularmente segura antes de que sea iniciado realmente. Por ejemplo, H.323 utilizará los mensajes de señalización de conexión H.225.0 para realizar esto.

6.5 Privacidad de trenes de medios

La presente Recomendación describe la privacidad de medios para trenes de medios enviados por transportes basados en paquetes. Estos canales pueden ser unidireccionales con respecto a las caracterizaciones de canal lógico H.245. Los canales no tienen que ser unidireccionales en un nivel físico o de transporte.

Un primer paso para obtener la privacidad de los medios debe ser la provisión de un canal de control privado por el cual establecer material de claves criptográficas y/o establecer los canales lógicos que transportarán los trenes de medios criptados. Para esto, cuando se funciona en una conferencia segura, cualesquiera puntos extremos participantes pueden utilizar un canal H.245 criptado. De esta manera, la selección del algoritmo criptográfico y las claves de criptación transferidas en la instrucción **Apertura canal lógico** H.245 están protegidas.

El canal seguro H.245 puede funcionar con diferentes características de los canales de medios privados mientras proporcione un nivel de privacidad mutuamente aceptable. Esto prevé mecanismos que protegen los trenes de medios y los canales de control para funcionar de una manera completamente independiente, proporcionando niveles totalmente diferentes de robustez y complejidad.

Si se requiere que el canal H.245 funcione de una manera no criptada, las claves de criptación de medios específicos pueden ser criptadas separadamente de la manera señalizada y acordadas por las partes participantes. Se puede utilizar un canal lógico del tipo **Control h235** para proporcionar el material que ha de proteger las claves de criptación de medios. Este canal lógico puede funcionar en un modo negociado adecuadamente.

La privacidad (criptación) de los datos transportados por canales lógicos tendrá la forma especificada por la **Apertura canal lógico**. La información de encabezamiento específica de transporte no será criptada. La privacidad de datos se ha de basar en la criptación de extremo a extremo.

6.6 Elementos de confianza

La base para la autenticación (confianza) y la privacidad es definida por los terminales del canal de comunicación. Para un canal de establecimiento de conexión, ésta puede estar entre el llamante y un componente de la red anfitriona. Por ejemplo, un teléfono "confía" en que el conmutador de red lo conectará con el teléfono cuyo número ha marcado. Por este motivo, toda entidad que termina un canal de control H.245 criptada o cualesquiera canales lógicos del tipo **datos criptados (encryptedData)** serán considerados un elemento de confianza de la conexión; esto incluye las unidades de control multipunto y las cabeceras. El resultado de confiar en un elemento es la confianza para revelar el mecanismo de privacidad (algoritmo y clave) a ese elemento.

Dado lo anterior, corresponde a los participantes en el trayecto de comunicación autenticar cualquiera y todos los elementos "de confianza". Esto se hará normalmente mediante el intercambio de certificados como se haría para la autenticación de extremo a extremo "normalizada". La presente Recomendación no requiere ningún nivel específico de autenticación, sino que aconseja que dicho nivel sea aceptable para todas las entidades que utilizan el elemento de confianza. Los detalles de un modelo de confianza y de una política de certificados quedan en estudio.

La privacidad se puede asegurar entre dos puntos extremos solamente si las conexiones entre elementos de confianza han demostrado estar protegidas contra ataques "intermedios".

6.6.1 Depósito de claves

Aunque no se requiere específicamente para el funcionamiento, la presente Recomendación contiene disposiciones para que las entidades que utilizan el protocolo H.235 admitan una técnica de recuperación de claves dentro de los elementos de señalización.

Se debe admitir la posibilidad de recuperar las claves de criptación de medios perdidas en aquellas instalaciones en las que esta funcionalidad es deseada o requerida.

El depósito de claves es una facilidad a menudo denominada tercero de confianza (TTP, *trusted third party*). Esta facilidad seguirá siendo objeto de estudio.

6.7 No repudio

Queda en estudio.

7 Procedimientos de establecimiento de la conexión

7.1 Introducción

Como se indica en la introducción del sistema, el canal de conexión de la llamada (H.225.0 para la serie H.323) y el canal de control de llamada (H.245) funcionarán en el modo seguro o inseguro negociado a partir del primer intercambio. Para el canal de conexión de la llamada, esto se hace previamente [para H.323 un TSAP seguro de TLS (puerto 1300) será utilizado para los mensajes Q.931]. Para el canal de control de llamada, el modo de seguridad es determinado por la información transferida en el protocolo de establecimiento de conexión inicial en uso por el terminal de la serie H.

Cuando no hay capacidades de seguridad superpuestas, el terminal llamado puede rechazar la conexión. El error devuelto no debe transferir información sobre cualquier discordancia de seguridad y el terminal llamante tendrá que determinar el problema por otros medios. Cuando el terminal llamante recibe un mensaje de ACUSE DE CONEXIÓN sin capacidades de seguridad suficientes, terminará la llamada.

Si los terminales llamante y llamado tienen capacidades de seguridad compatibles, ambos lados supondrán que el canal H.245 funcionará en el modo seguro negociado. La imposibilidad de establecer el canal H.245 en el modo seguro determinado debe considerarse un error de protocolo y la conexión será terminada.

8 Señalización y procedimientos H.245

En general, los aspectos de privacidad de los canales de medio son controlados de la misma manera que cualquier otro parámetro de codificación; cada terminal indica sus capacidades, la fuente de los datos selecciona un formato que ha de utilizar y el receptor acepta o rechaza el modo. Todos los aspectos del mecanismo independientes del transporte, tales como selección de algoritmo, se indican en elementos de canal lógico genéricos. Los elementos específicos de transporte, tales como la sincronización de algoritmos de clave/criptación son transferidos en estructuras específicas de transporte.

8.1 Funcionamiento seguro del canal H.245

Suponiendo que los procedimientos de conexión mencionados en la cláusula anterior indiquen un modo de funcionamiento seguro, se llevará a cabo la toma de contacto y la autenticación negociadas para el canal lógico H.245 antes de que se intercambie cualquier mensaje H.245. Si se ha negociado,

cualquier intercambio de certificados se producirá utilizando este mecanismo apropiado para los terminales de la serie H. Después de completar la seguridad del canal H.245, los terminales utilizarán el protocolo H.245 de la misma manera que si funcionasen en un modo inseguro.

8.2 Funcionamiento inseguro del canal H.245

Como otra posibilidad, el canal H.245 puede funcionar de una manera insegura y las dos entidades abren un canal lógico seguro con el cual efectuar la autenticación y/o la derivación de secreto compartido. Por ejemplo, se puede utilizar TLS o IPSEC abriendo un canal lógico con el **tipo de datos** que contiene un valor para **datos de criptación (encryptionData)**. Este canal se utilizaría para derivar un secreto compartido que protege cualesquiera clave de sesión de medios o para transportar la **sincronización de criptación (encryptionSync)**.

8.3 Intercambio de capacidades

De acuerdo con los procedimientos de 8.3/H.245 (Procedimientos de intercambio de capacidades) y las Recomendaciones apropiadas relativas a sistemas de la serie H, los puntos extremos intercambian capacidades utilizando mensajes H.245. Estos conjuntos de capacidades pueden contener definiciones que indiquen parámetros de seguridad y criptación. Por ejemplo, un punto extremo pudiera proporcionar capacidades para enviar y recibir vídeo H.261. Puede señalizar también la posibilidad de enviar y recibir vídeo H.261 criptado.

Cada algoritmo de criptación que se utilice junto con un códec de medios determinado, supone una nueva definición de capacidad. Como con cualquier otra capacidad, los puntos extremos pueden suministrar códecs codificados independientes y dependientes en su intercambio. Esto permitirá a los puntos extremos ampliar sus capacidades de seguridad basadas en la tara y recursos disponibles.

Una vez completado el intercambio de capacidades, los puntos extremos pueden abrir canales lógicos seguros para los medios, de la misma manera que lo harían en un modo inseguro.

8.4 Cometido de terminal director

La determinación de terminal director-subordinado de H.245 se utiliza para establecer la entidad directora a los efectos del funcionamiento de canales bidireccionales y la resolución de otros conflictos. Este cometido de director se utiliza también en los métodos de seguridad. Aunque los modos de seguridad de un tren de medios son fijados por la fuente (en deferencia a las capacidades del receptor), el director es el punto extremo que genera la clave de criptación. Esta generación de la clave de criptación se hace con independencia de si el director es el receptor o la fuente de los medios criptados. Para efectuar el funcionamiento de canales multidistribución con claves compartidas, el controlador multipunto (también el director) debe generar las claves.

8.5 Señalización de canal lógico

Los puntos extremos abren canales lógicos de medios seguros de la misma manera que abren canales lógicos de medios inseguros. Cada canal puede funcionar de una manera completamente independiente con respecto a los otros canales, en particular cuando esto incumbe a la seguridad. El modo particular será definido en el campo **tipo datos (dataType)** de **apertura canal lógico**. La clave de criptación inicial se transferirá en **Apertura de canal lógico** o **Acuse apertura canal lógico** dependiendo de la relación director/subordinado del originador de **Apertura canal lógico**.

El **Acuse apertura canal lógico** actuará como una confirmación del modo de criptación. Si **apertura canal lógico** no es aceptable al recibiente, se devolverá **tipo datos no admitido (dataTypeNotSupported)** o **tipo datos no disponible (dataTypeNotAvailable)** (condición transitoria) en el campo de causa de **Rechazo apertura canal lógico (OpenLogicalCbannelReject)**.

Durante el intercambio de protocolos que establece el canal lógico, la clave de criptación será transferida del terminal director al subordinado (con independencia de quién inició **Apertura canal lógico**). Para los canales de medios abiertos por un punto extremo (que no sea el director), el director devolverá la clave de criptación inicial y el punto de sincronización inicial en **Acuse apertura canal lógico** (en el campo **sincronización de criptación**). Para los canales de medios abiertos por el director, **Apertura canal lógico** incluirá la clave de criptación inicial y el punto de sincronización en el campo **sincronización de criptación**.

9 Procedimientos multipunto

9.1 Autenticación

La autenticación se producirá entre un punto extremo y la MC(U) de la misma manera que se haría en una conferencia punto a punto. La MC(U) fijará la política relativa al nivel y rigor de autenticación. Como se indica en 6.6, se confía en la MC(U); los puntos extremos existentes en una conferencia pueden estar limitados por el nivel de autenticación empleado por la MC(U). Las nuevas instrucciones **petición conferencia/respuesta conferencia** permiten que los puntos extremos obtengan de la MC(U) los certificados de otros participantes en la conferencia. Como se indica en los procedimientos H.245, los puntos extremos en una conferencia multipunto pueden solicitar cualquier otro certificado de punto extremo por medio del MC, pero no pueden realizar la autenticación criptográfica directa dentro del canal H.245.

9.2 Privacidad

La MC(U) ganará todos los intercambios director/subordinado y como tal suministrará las claves de criptación a los participantes en una conferencia multipunto. La privacidad para cada fuente dentro de una sesión común (suponiendo multidistribución) se puede lograr con claves individuales o comunes. Estos dos modos pueden ser elegidos arbitrariamente por la MC(U) y no serán controlables desde ningún punto extremo particular, salvo en modos permitidos por la política de la MC(U). En otras palabras, se puede utilizar una clave común a través de múltiples canales lógicos abiertos por diferentes fuentes.

10 Señalización y procedimientos de autenticación

10.1 Introducción

Se puede utilizar dos tipos de autenticación. El primer tipo se basa en criptación simétrica que no requiere un contacto previo entre las entidades comunicantes. El segundo tipo se basa en la capacidad de tener algún secreto compartido previo (denominado "abono"). Se proporcionan dos formas de autenticación basada en abono: contraseña y certificado.

10.2 Intercambio Diffie-Hellman con autenticación facultativa

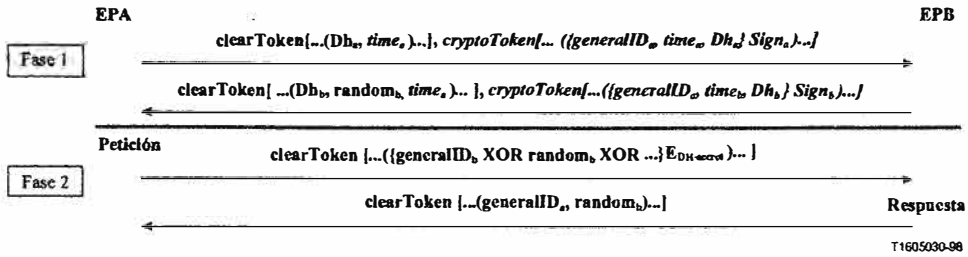
El propósito no es proporcionar autenticación absoluta a nivel de usuario. Este método proporciona la señalización para generar un secreto compartido entre dos entidades que pueden manipular material para comunicaciones privadas.

Al final de este intercambio ambas entidades poseerán una clave secreta compartida junto con un algoritmo elegido con el cual utilizar esta clave. Esta clave secreta compartida se puede utilizar en cualquier intercambio de petición/respuesta subsiguiente. Cabe señalar que, en casos muy raros, el intercambio Diffie-Hellman puede generar claves *débiles* conocidas para determinados algoritmos.

Cuando es así, cada entidad debe desconectar y reconectar para establecer un nuevo conjunto de claves.

La primera fase de la figura 1 siguiente muestra los datos intercambiados durante la negociación Diffie-Hellman. La segunda fase prevé que los mensajes de petición específicos de la aplicación o del protocolo sean autenticados por el respondedor. Obsérvese que se puede devolver un nuevo valor aleatorio con cada respuesta.

NOTA – Se puede proporcionar también un elemento de firma facultativo, que se ilustra a continuación en ***cursivas***.



[... ...] indica una secuencia de testigos

() indica un testigo determinado, que contiene múltiples elementos

{}$E_{DH\text{-}Secret}$ indica que los valores contenidos han sido criptados utilizando el secreto Diffie-Hellman

El punto extremo B (EPB) sabe qué clave secreta compartida ha de utilizar para descifrar el identificador **ID$_b$ general** asociándolo con el **ID$_a$ general** que debe ser transferido también en el mensaje. Obsérvese que el valor criptado en la fase 2 es transferido en el campo **ID general** de un **testigo claro** para simplificar la codificación.

Figura 1/H.235

10.3 Autenticación basada en abono

10.3.1 Introducción

Aunque los procedimientos esbozados aquí (y los algoritmos de la ISO de los cuales se derivan) son bidireccionales, pueden ser utilizados solamente en un sentido si la autenticación se necesita solamente en ese sentido. Estos intercambios suponen que cada extremo posee algún identificador bien conocido (como un identificador textual) que lo identifica inequívocamente. Otra hipótesis es que hay una referencia de tiempo mutuamente aceptable (de la cual derivar sellos de hora). La diferencia de hora que es aceptable es un asunto de la implementación local.

Hay tres variaciones diferentes que se pueden aplicar dependiendo de las necesidades:

1) Contraseña con criptación simétrica.

2) Contraseña con troceado.

3) Certificado con firma.

En todos los casos, el testigo contendrá la información descrita en las subcláusulas siguientes según la variación elegida. Obsérvese que en todos los casos el **ID general** puede ser conocido a través de la configuración o del directorio, en vez de en el intercambio de protocolos dentro de banda.

generará nuevas claves en respuesta a esta instrucción y puede decidir también asíncronamente distribuir nuevas claves y, si lo hace así, utilizará el mensaje **actualización criptación**.

Después de recibir una **petición actualización criptación**, el terminal director enviará **actualización criptación**. Si se trata de una conferencia multipunto, el MC (también el director) distribuirá la nueva clave a todos los receptores antes de dar esta clave al transmisor. El transmisor de los datos por el canal lógico utilizará la nueva clave tan pronto sea posible después de recibir el mensaje.

Un transmisor (que se supone no es el director) puede solicitar también una nueva clave. Si el transmisor forma parte de una conferencia multipunto, el procedimiento será el siguiente:

El transmisor enviará **petición actualización criptación** al MC (director).

El MC debe generar una nueva clave y enviar un mensajes **actualización criptación** a todos los participantes en la conferencia, salvo al transmisor.

Después de distribuir las nuevas claves a todos los participantes, el MC enviará **actualización criptación** al transmisor que utilizará entonces la nueva clave.

12 Recuperación tras error de seguridad

Esta Recomendación no especifica ni recomienda métodos por los cuales los puntos extremos puedan supervisar su privacidad absoluta. Sin embargo, sí recomienda acciones que se han de ejecutar cuando se detecta la pérdida de privacidad.

Si cualquiera de los dos puntos extremos detecta una brecha en la seguridad del canal de conexión de la llamada (por ejemplo, H.225.0 para H.323), debe cerrar inmediatamente la conexión aplicando los procedimientos de protocolo apropiados al punto extremo en cuestión [8.5/H.323 con la excepción del paso 5)].

Si cualquiera de los dos puntos extremos detecta una brecha en la seguridad del canal H.245 o del canal lógico **(control h235)** de datos seguro, debe cerrar inmediatamente la conexión aplicando los procedimientos de protocolo apropiados al punto extremo en cuestión [8.5/H.323 con la excepción del paso 5)].

Si cualquier punto extremo detecta una pérdida de privacidad en uno de los canales lógicos, debe solicitar inmediatamente una nueva clave **(petición actualización criptación)** y/o cerrar el canal lógico. A discreción de la MC(U) una pérdida de privacidad en el canal lógico puede provocar el cierre de todos los otros canales lógicos y/o la creación de nuevas claves a discreción de la MC(U). La MC(U) enviará **petición actualización criptación, actualización criptación** a cualquier y a todos lo puntos extremos afectados.

A discreción de la MC(U), hubo un error de seguridad en un canal puede provocar el cierre de las conexiones en todos los puntos extremo de la conferencia, terminándola así.

ANEXO A

ASN.1 del protocolo H.235

```
H235-SECURITY-MESSAGES DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

-- EXPORTS All

ChallengeString   ::= OCTET STRING (SIZE(8..128))
TimeStamp         ::= INTEGER(1..4294967295) -- seconds since 00:00 1/1/1970 UTC
RandomVal         ::= INTEGER
```

```
Password                ::= BMPString (SIZE (1..128))
Identifier              ::= BMPString (SIZE (1..128))
KeyMaterial             ::= BIT STRING(SIZE(1..2048))

NonStandardParameter ::= SEQUENCE
{
        nonStandardIdentifier     OBJECT IDENTIFIER,
        data                      OCTET STRING
}

-- if local octet representations of these bit strings are used they shall
-- utilize standard Network Octet ordering (e.g. Big Endian)
DHset ::= SEQUENCE
{
        halfkey                 BIT STRING (SIZE(0..2048)), -- = g^x mod n
        modSize                 BIT STRING (SIZE(0..2048)), -- n
        generator               BIT STRING (SIZE(0..2048)), -- g
        ...
}

TypedCertificate ::= SEQUENCE
{
        type                    OBJECT IDENTIFIER,
        certificate             OCTET STRING,
        ...
}

AuthenticationMechanism ::=CHOICE
{
        dhExch                  NULL, -- Diffe-Hellman
        pwdSymEnc               NULL, -- password with symmetric encryption
        pwdHash                 NULL, -- password with hashing
        certSign                NULL, -- Certificate with signature
        ipsec                   NULL, -- IPSEC based connection
        tls                     NULL,
        nonStandard             NonStandardParameter, -- something else.
        ...
}

ClearToken          ::= SEQUENCE  -- a "token" may contain multiple value types.
{
        timeStamp               TimeStamp OPTIONAL,
        password                Password OPTIONAL,
        dhkey                   DHset OPTIONAL,
        challenge               ChallengeString OPTIONAL,
        random                  RandomVal OPTIONAL,
        certificate             TypedCertificate OPTIONAL,
        generalID               Identifier OPTIONAL,
        nonStandard             NonStandardParameter OPTIONAL,
        ...
}

--
-- Start all the cryptographic parameterized types here...
--


SIGNED { ToBeSigned } ::= SEQUENCE {
  toBeSigned        ToBeSigned,
  algorithmOID      OBJECT IDENTIFIER,
  paramS            Params,       -- any "runtime" parameters
```

```
  signature          BIT STRING
} ( CONSTRAINED BY { -- Verify or Sign Certificate -- } )


ENCRYPTED { ToBeEncrypted } ::= SEQUENCE {
  algorithmOID          OBJECT IDENTIFIER,
  paramS                Params,      -- any "runtime" parameters
  encryptedData         OCTET STRING
} ( CONSTRAINED BY { -- Encrypt or Decrypt -- ToBeEncrypted } )

HASHED { ToBeHashed } ::= SEQUENCE {
  algorithmOID          OBJECT IDENTIFIER,
  paramS                Params,      -- any "runtime" parameters
  hash                  BIT STRING
} ( CONSTRAINED BY { -- Hash -- ToBeHashed } )

IV8 ::= OCTET STRING (SIZE(8))

-- signing algorithm used must select one of these types of parameters
-- needed by receiving end of signature.

Params ::= SEQUENCE {
      ranInt        INTEGER OPTIONAL, -- some integer value
      iv8           IV8 OPTIONAL,   -- 8 octet initialization vector


EncodedGeneralToken ::= TYPE-IDENTIFIER.&Type (ClearToken -- general usage token
PwdCertToken ::= ClearToken (WITH COMPONENTS {..., timeStampPRESENT, generalIDPRESENT})
EncodedPwdCertToken ::= TYPE-IDENTIFIER.&Type (PwdCertToken)

CryptoToken::= CHOICE
{

      cryptoEncryptedToken SEQUENCE -- General purpose/application specific token
      {
            tokenOID    OBJECT IDENTIFIER,
            token       ENCRYPTED { EncodedGeneralToken }
      },
      cryptoSignedToken  SEQUENCE -- General purpose/application specific token
      {
            tokenOID    OBJECT IDENTIFIER,
            token       SIGNED { EncodedGeneralToken }
      },
      cryptoHashedToken SEQUENCE -- General purpose/application specific token
      {
            tokenOID          OBJECT IDENTIFIER,
            hashedVals        ClearToken,
            token HASHED { EncodedGeneralToken }
      },
      cryptoPwdEncr     ENCRYPTED { EncodedPwdCertToken },


-- These allow the passing of session keys within the H.245 OLC structure.
-- They are encoded as standalone ASN.1 and based as an OCTET STRING within H.245
H235Key     ::=CHOICE  -- this is used with the H.245 "h235Key" field
{
      secureChannel     KeyMaterial,
      sharedSecret      ENCRYPTED {EncodedKeySyncMaterial},
      certProtectedKey        SIGNED { EncodedKeySignedMaterial },
```

```
KeySignedMaterial ::= SEQUENCE {
        generalId           Identifier, -- slave's alias
        mrandom     RandomVal, -- master's random value
        srandom     RandomVal OPTIONAL, -- slave's random value
        timeStamp           TimeStamp OPTIONAL, -- master's timestamp for unsolicited EU
        encrptval           ENCRYPTED {EncodedKeySyncMaterial }
}
EncodedKeySignedMaterial ::= TYPE-IDENTIFIER.&Type (KeySignedMaterial)

H235CertificateSignature ::=SEQUENCE
{
        certificate             TypedCertificate,
        responseRandom          RandomVal,
        requesterRandom         RandomVal OPTIONAL,
        signature               SIGNED { EncodedReturnSig },
        ...
}

ReturnSig ::= SEQUENCE {
        generalId               Identifier, -- slave's alias
        responseRandom          RandomVal,
        requestRandom           RandomVal OPTIONAL,
        certificate             TypedCertificate OPTIONAL -- requested certificate
}

EncodedReturnSig ::= TYPE-IDENTIFIER.&Type (ReturnSig)
KeySyncMaterial   ::=SEQUENCE
{
        generalID           Identifier,
        keyMaterial         KeyMaterial,
        ...
}
EncodedKeySyncMaterial ::=TYPE-INDENTIFIER.&Type (KeySyncMaterial)


END  -- End of H235-SECURITY-MESSAGES DEFINITIONS
```

ANEXO B

Aspectos específicos del protocolo H.323

B.1 Antecedentes

En la figura B.1 se muestra un diagrama con una visión general del alcance de protocolo H.235 en el marco de la Recomendación H.323.

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

H.245

(05/2006)

SERIE H: SISTEMAS AUDIOVISUALES Y MULTIMEDIA

Infraestructura de los servicios audiovisuales – Procedimientos de comunicación

Protocolo de control para comunicación multimedia

Recomendación UIT-T H.245

HDLC	Control de enlace de datos de alto nivel (*high-level data link control*)
HRD	Decodificador hipotético de referencia (*hypothetical reference decoder*) (véanse las Recs. UIT-T H.261 y H.263)
IV	Vector de inicialización (*initialization vector*) (utilizado para criptación: véanse las Recs. UIT-T H.233 y H.234)
LAPM	Protocolo de acceso al enlace para módems (*link access protocol for modems*)
LCSE	Entidad de señalización de canal lógico (*logical channel signalling entity*)
MC	Entidad de control multipunto H.323 (*H.323 multipoint control entity*)
MCU	Unidad de control multipunto (*multipoint control unit*)
MLSE	Entidad de señalización del bucle de mantenimiento (*maintenance loop signalling entity*)
MPI	Intervalo de imagen mínimo (*minimum picture interval*)
MRSE	Entidad de señalización de petición de modo (*mode request signalling entity*)
MSDSE	Entidad de señalización de determinación principal-subordinado (*master-slave determination signalling entity*)
MTSE	Entidad de señalización de tabla múltiplex (*multiplex table signalling entity*)
PCR	Referencia de reloj de programa (*program clock reference*) (véase la Rec. UIT-T H.222.0 | ISO/CEI 13818-1)
PID	Identificador de paquete (*packet identifier*) (véase la Rec. UIT-T H.222.0 | ISO/CEI 13818-1)
QCIF	Cuarto de CIF (*quarter CIF*)
RMESE	Entidad de señalización de petición de entrada múltiplex (*request multiplex entry signalling entity*)
RTCP	Protocolo de control de transporte en tiempo real (*real-time transport control protocol*)
RTDSE	Entidad de señalización de retardo de ida y vuelta (*round-trip delay signalling entity*)
RTGC	Red telefónica general conmutada
RTP	Protocolo de transporte en tiempo real (*real-time transport protocol*)
SDL	Lenguaje de especificación y descripción (*specification and description language*)
SDU	Unidad de datos de servicio (*service data unit*)
SE	Mensaje de intercambio de sesión (*session exchange message*) (utilizado para criptación: véanse las Recs. UIT-T H.233 y H.234)
SQCIF	Sub QCIF (*sub QCIF*)
STD	Decodificador-objetivo de sistema (*system target decoder*) (véase la Rec. UIT-T H.222.0 | ISO/CEI 13818-1)
VC	Canal virtual de ATM (*ATM virtual channel*)

5 Presentación general

Esta Recomendación proporciona diversos servicios diferentes, alguno de los cuales se espera que sean aplicables a todos los terminales que los utilizan, siendo otros más específicos de terminales concretos. Se definen procedimientos para permitir el intercambio de capacidad audiovisuales y de datos; para solicitar la transmisión de un modo audiovisual y de datos determinado; para gestionar

los canales lógicos utilizados para transportar la información audiovisual y de datos; para establecer qué terminal es el terminal principal y cuál el subordinado con fines de gestión de los canales lógicos bidireccionales; para transportar distintas señales de control e indicación; para controlar la velocidad de bits de los canales lógicos individuales y de la totalidad del múltiplex; y para medir el retardo de ida y vuelta entre un par de terminales. Estos procedimientos se explican con más detalle en lo que sigue.

Continuando con esta introducción general, hay cláusulas donde se detalla la sintaxis y la semántica de los mensajes, así como los procedimientos correspondientes. Se ha definido la sintaxis empleando la notación ASN.1 [40] y la semántica define el significado de los elementos sintácticos y proporciona asimismo las limitaciones de sintaxis no especificadas en ASN.1. La cláusula de procedimientos define los protocolos que utilizan los mensajes definidos en las demás cláusulas.

Aunque no todos los mensajes y procedimientos definidos en esta Recomendación se aplicarán a la totalidad de los terminales, no se indican aquí tales restricciones, las cuales competen a las recomendaciones que hagan uso de esta Recomendación.

Se ha definido esta Recomendación de forma que sea independiente del mecanismo de transporte subyacente, aunque se ha previsto su empleo con una capa de transporte fiable, es decir, aquella que proporcione una entrega garantizada de datos correctos.

5.1 Determinación principal-subordinado

Se presentan conflictos cuando dos terminales que intervienen en una llamada inician simultáneamente eventos similares y sólo uno de esos eventos es posible o deseado, por ejemplo, cuando los recursos están disponibles solamente para una aparición del evento. Para resolver esas situaciones, un terminal actuará como terminal principal y el otro actuará como terminal subordinado. Las reglas especificarán el comportamiento del terminal principal y del terminal subordinado en caso de conflicto.

El procedimiento de determinación principal-subordinado permite a los terminales en una llamada determinar cuál es el principal y cuál es el subordinado. La categoría del terminal se puede determinar de nuevo en cualquier momento durante una llamada; sin embargo, un terminal sólo puede iniciar el proceso de determinación principal-subordinado si no está activo localmente ningún procedimiento que dependa de su resultado.

5.2 Intercambio de capacidades

Los procedimientos de intercambio de capacidades tienen por finalidad asegurar que únicamente las señales multimedia que deben transmitirse son aquellas que el terminal de recepción puede recibir y manejar adecuadamente. Esto exige que las capacidades de cada terminal para recibir y decodificar sean conocidas por el otro terminal. No es necesario que un terminal comprenda o almacene todas las capacidades entrantes; podrán ignorarse capacidades no comprendidas o no utilizadas, sin que esto implique la consideración de que existen errores. Cuando se reciba una capacidad que contenga extensiones no comprendidas por el terminal, la capacidad será aceptada como si se contuviera las extensiones.

Mediante la transmisión de su juego de capacidades, se pone en conocimiento de un terminal la capacidad total de otro terminal para recibir y decodificar diversas señales.

Las capacidades de recepción describen la aptitud del terminal para recibir y procesar los trenes de información entrantes. Los transmisores deberán limitar el contenido de la información transmitida al valor que el receptor haya indicado que es capaz de recibir. La ausencia de una capacidad de recepción indica que el terminal es incapaz de recibir información (se trata de un transmisor únicamente).

Las capacidades de transmisión describen la aptitud del terminal para la transmisión de trenes de información. Estas capacidades permiten ofrecer a los receptores la posibilidad de elección entre distintos modos de funcionamiento, de forma que el receptor pueda solicitar el modo en el que prefiere efectuar la recepción. La ausencia de una capacidad de transmisión indica que el terminal no ofrecerá al receptor la elección de modos preferidos (pero puede sin embargo transmitir alguna información compatible con la capacidad del receptor).

Estos conjuntos de capacidades permiten la transmisión simultánea de más de un tren de un tipo de medio determinado. Por ejemplo, un terminal puede declarar su aptitud para recibir (o enviar) simultáneamente dos flujos de vídeo H.262 independientes y dos trenes de audio G.722 independientes. Se han definido los mensajes de capacidad para permitir que un terminal indique que no posee capacidades fijas, sino que dependen de los demás modos que se estén utilizando simultáneamente. Por ejemplo, es posible indicar que puede decodificarse una señal vídeo de elevada resolución cuando se utiliza un algoritmo de audio más simple o que pueden decodificarse cualquiera de dos secuencias de vídeo de baja resolución o una sola de alta resolución. Es posible también expresar compromisos entre la capacidad de transmisión y la capacidad de recepción.

Pueden emitirse capacidades y mensajes de control no normalizados utilizando la estructura NonStandardParameter. Debe observarse que aunque el significado de los mensajes no normalizados lo definen organizaciones individuales, los equipos construidos por cualquier fabricante pueden señalizar cualquier mensaje no normalizado si conocen su significado.

Los terminales pueden volver a enviar conjuntos de capacidades en cualquier momento.

5.3 Procedimientos de señalización de canal lógico

Se define un protocolo de acuse de recibo para la apertura y el cierre de canales lógicos que transportan información audiovisual y de datos. La finalidad de estos procedimientos es garantizar que un terminal es capaz de recibir y decodificar los datos que se transmitirán por un canal lógico en el momento en que se abra tal canal, en vez de en el momento en que se transmita el primer dato por él y para asegurar que el terminal de recepción está preparado para recibir y decodificar los datos que se transmitirán por el canal lógico antes del comienzo de la transmisión. El mensaje de apertura del canal lógico incluye una descripción de los datos que se transportarán, por ejemplo H.262 MP@ML a 6 Mbit/s. Los canales lógicos únicamente se abrirán cuando exista capacidad suficiente para recibir datos sobre todos los canales lógicos abiertos simultáneamente.

Una parte de este protocolo se aplica a la apertura de canales bidireccionales. Para evitar problemas de temporización, se define un terminal como terminal principal y el otro como terminal subordinado. Únicamente el terminal principal puede iniciar la apertura de canales bidireccionales: sin embargo, el terminal subordinado puede solicitar al terminal principal que realice esa apertura. Se ha definido un protocolo para establecer qué terminal será el principal y cuál el subordinado. Sin embargo, los sistemas que hagan uso de esta Recomendación deberán especificar otros modos de determinar qué terminal es el principal y cuál el subordinado.

5.4 Petición de cierre de canal lógico por el terminal receptor

Un canal lógico se abre y cierra desde el lado transmisor. Se define un mecanismo que permite a un terminal receptor solicitar el cierre de un canal lógico entrante. El terminal transmisor puede aceptar o rechazar la petición de cierre del canal lógico. Un terminal puede, por ejemplo, utilizar estos procedimientos para solicitar el cierre de un canal lógico entrante que, por una razón cualquiera, no puede decodificarse. Estos procedimientos pueden utilizarse también para solicitar el cierre de un canal lógico bidireccional, por el terminal que no abrió el canal.

5.5 Modificación de entrada en la tabla múltiplex H.223

La tabla múltiplex H.223 asocia cada octeto dentro de un mensaje MUX H.223 con un determinado número de canal lógico. La tabla múltiplex H.223 puede tener hasta 15 entradas. Se proporciona un mecanismo que permite al terminal transmisor especificar e informar al receptor sobre las nuevas entradas en la tabla múltiplex H.223. Un terminal receptor puede también solicitar la retransmisión de una entrada en la tabla múltiplex.

5.6 Petición de modo audiovisual y de modo datos

Cuando el protocolo de intercambio de capacidad ha concluido, ambos terminales tendrán conocimiento de la capacidad del otro para transmitir y recibir como se especifica en los descriptores de capacidad que han sido intercambiados. Un terminal no está obligado a declarar todas sus capacidades; sólo necesita declarar aquellas que desea utilizar.

Un terminal puede indicar sus capacidades para transmitir. Un terminal que recibe capacidades de transmisión del terminal distante puede pedir que se le transmitan en un determinado modo. Un terminal indica que no desea que su modo de transmisión sea controlado por el terminal distante no enviando capacidades de transmisión.

5.7 Determinación del retardo de ida y vuelta

En algunas aplicaciones puede ser conveniente tener conocimiento del retardo de ida y vuelta entre un terminal transmisor y un terminal receptor. Se proporciona un mecanismo para medir este tiempo de ida y vuelta. Este mecanismo puede ser también útil como un medio para detectar si el terminal distante está funcionando todavía.

5.8 Bucles de mantenimiento

Se especifican procedimientos para establecer bucles de mantenimiento. Es posible especificar el bucle de un canal lógico individual como un bucle digital o como un bucle decodificado y el bucle del múltiplex completo.

5.9 Instrucciones e indicaciones

Se proporcionan instrucciones e indicaciones para diversas finalidades: señales de vídeo/audio activo/inactivo para informar al usuario; petición de actualización rápida para conmutación en la fuente, en aplicaciones multipunto, son algunos ejemplos. Ni las instrucciones ni las indicaciones provocan mensajes de respuesta del terminal distante. Las instrucciones fuerzan la ejecución de una acción en el terminal distante, mientras que las indicaciones se limitan a proporcionar información y no fuerzan a ejecutar ninguna acción.

Una instrucción, por definición, permite que la velocidad binaria de los canales lógicos y de la totalidad del múltiplex sean controladas desde el terminal distante. Esto tiene varias finalidades: interfuncionamiento con terminales que utilizan múltiplex en los cuales sólo hay un número finito de velocidades binarias disponibles; aplicaciones multipunto en que las velocidades de las diferentes fuentes deben ser adaptadas; y control de flujo en redes congestionadas.

Apéndice II

Ejemplos de procedimientos H.245

II.1 Introducción

Este apéndice ilustra ejemplos de los procedimientos definidos en el anexo C. La figura II.1-1 muestra los símbolos gráficos utilizados en los diagramas de este apéndice.

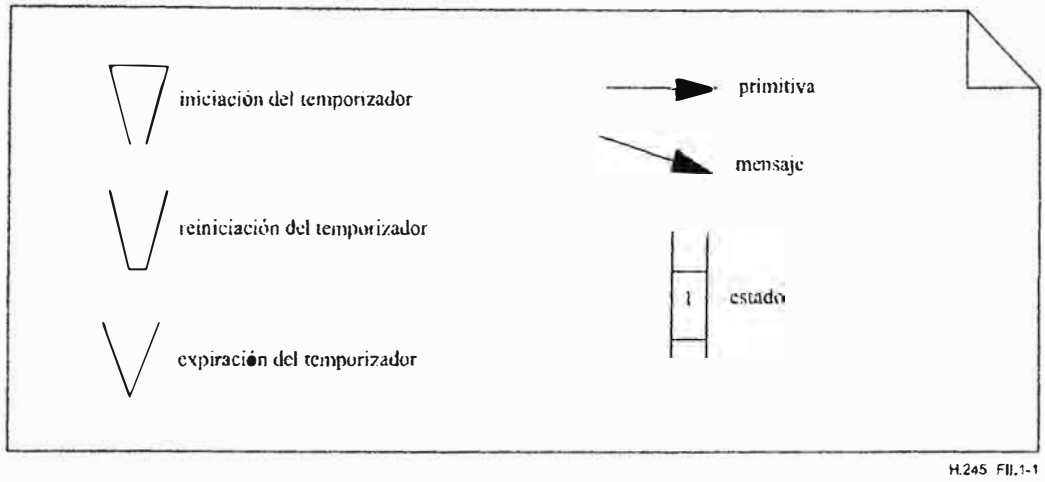


Figura II.1-1/H.245 – Clave de las figuras

II.2 Entidad de señalización de determinación principal-subordinado

En las figuras II.2-1 a II.2-10 los mensajes se representan por los nombres abreviados indicados en el cuadro II.2-1.

Cuadro II.2-1/H.245 – Nombres abreviados de determinación principal-subordinado

Mensaje	Nombre en los ejemplos
MasterSlaveDetermination	MSD
MasterSlaveDeterminationAck	MSDAck
MasterSlaveDeterminationReject	MSDReject
MasterSlaveDeterminationRelease	MSDRelease

En las figuras II.2-1 a II.2-10, REPOSO, ESPERA DE RESPUESTA DE SALIDA y ESPERA DE RESPUESTA DE ENTRADA se designan por "0", "1" y "2", respectivamente.

En las figuras siguientes el valor de parámetro asociado con las primitivas DETERMINACIÓN.indicación y DETERMINACIÓN.confirmación es la del parámetro TIPO. El valor de campo asociado con el mensaje MasterSlaveDeterminationAck es el del campo de decisión.

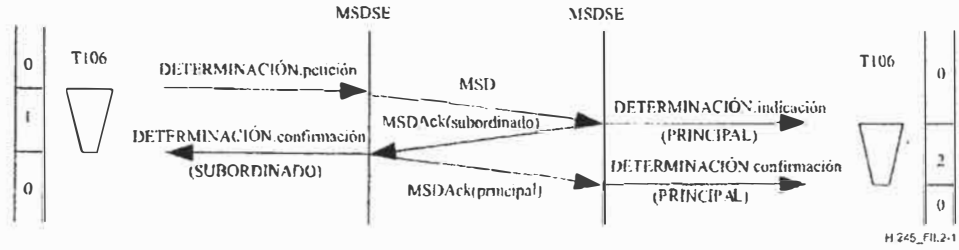


Figura II.2-1/H.245 – Determinación principal-subordinado – Principal en la MSDSE distante

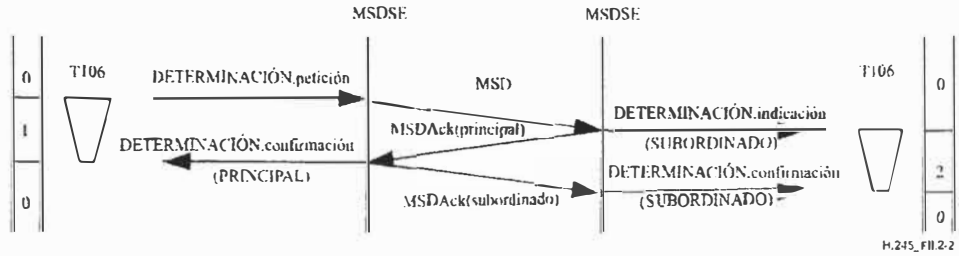


Figura II.2-2/H.245 – Determinación principal-subordinado – Subordinado en la MSDSE distante

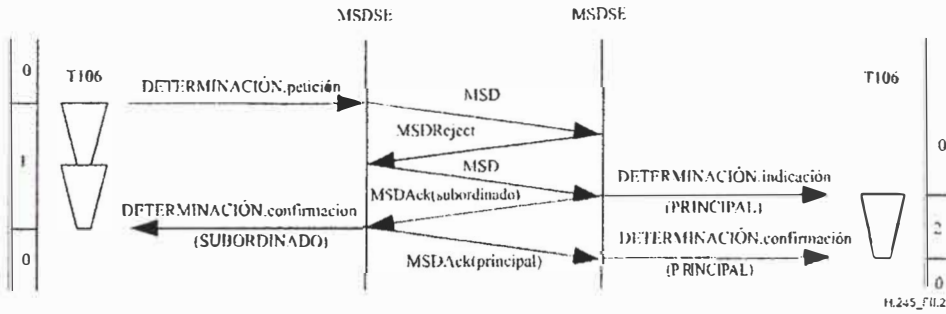


Figura II.2-3/H.245 – Determinación principal-subordinado – El primer intento produjo un resultado indeterminado. El segundo intento tuvo éxito

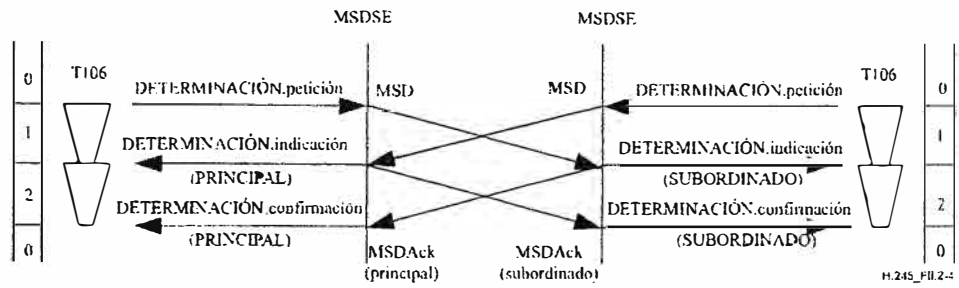


Figura II.2-4/H.245 – Determinación principal-subordinado – Determinación simultánea

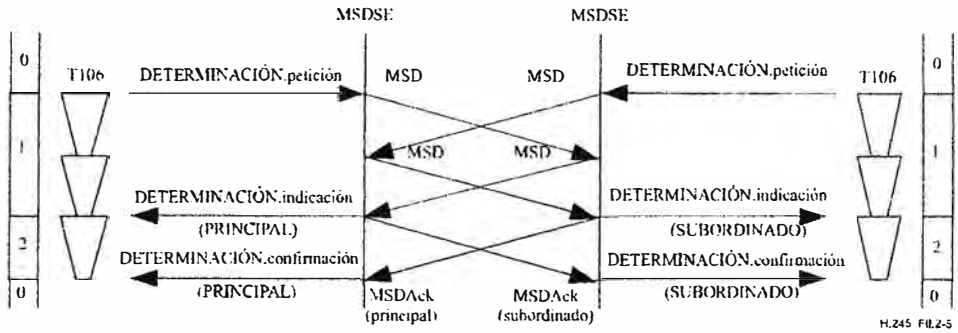


Figura II.2-5/H.245 – Determinación principal-subordinado – Determinación simultánea, pero el primer intento produce un resultado indeterminado

En la figura II.2-6, ha expirado el temporizador local T106. Sólo el terminal de la derecha conoce su categoría. El terminal de la derecha es capaz de recibir nuevas instrucciones pero no puede solicitar nada del otro terminal que se base en el conocimiento del resultado de la determinación de categoría. El terminal de la izquierda no puede ni aceptar ni iniciar nuevos procedimientos. Debe iniciarse un segundo procedimiento de determinación de categoría.

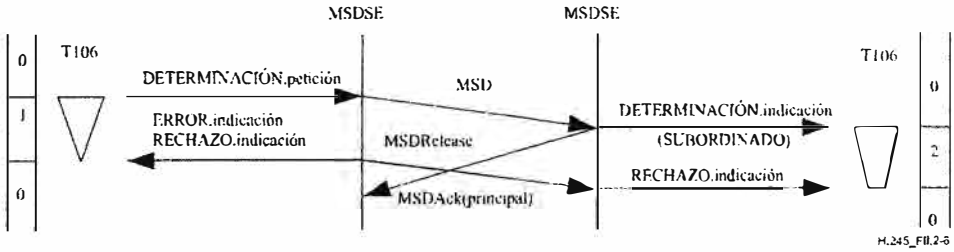


Figura II.2-6/H.245 – Determinación principal-subordinado – Expiración del temporizador local T106 con subordinado en el extremo distante

En la figura II.2-7, ha expirado el temporizador distante T106 durante el estado ESPERA DE ACUSE DE RECIBO EN ENTRADA. Ambos terminales conocen su categoría. El terminal de la izquierda puede recibir y emitir instrucciones. Sin embargo, el terminal distante no sabe si el terminal local está listo para recibir y no puede emitir instrucciones que se basen en el conocimiento del resultado de la determinación de categoría. Debe iniciarse un segundo procedimiento de determinación de categoría.

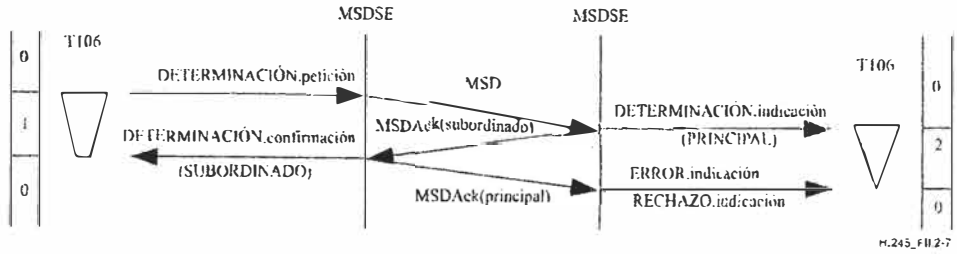


Figura II.2-7/H.245 – Determinación principal-subordinado – Expiración del temporizador distante T106 con director en el extremo distante

En la figura II.2-8 ha expirado el temporizador distante T106 durante el estado ESPERA DE ACUSE DE RECIBO EN SALIDA durante un procedimiento de determinación simultánea. Ambos terminales conocen su categoría. El terminal de la derecha puede recibir y emitir instrucciones. Sin embargo, el terminal de la izquierda no sabe si el otro terminal está listo para recibir y no puede emitir instrucciones que se basen en el conocimiento del resultado de la determinación de categoría. Puede recibir tales instrucciones. Debe iniciarse un segundo procedimiento de determinación de categoría.

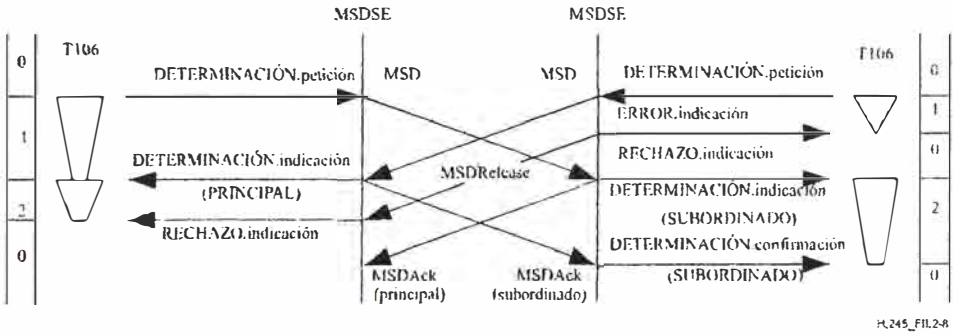


Figura II.2-8/H.245 – Determinación principal-subordinado – Procedimientos de determinación simultánea con expiración del temporizador T106 en el subordinado

En la figura II.2-9, ha expirado el temporizador distante T106 durante una estado ESPERA DE ACUSE DE RECIBO EN ENTRADA, durante un procedimiento de determinación simultánea. Ambos terminales conocen su categoría. El terminal de la izquierda puede recibir y emitir instrucciones. Sin embargo, el terminal de la derecha no sabe si el otro terminal está listo para recibir y no puede emitir instrucciones que se basen en el conocimiento del resultado de la

determinación de categoría. Puede recibir tales instrucciones. Debe iniciarse un segundo procedimiento de determinación de categoría.

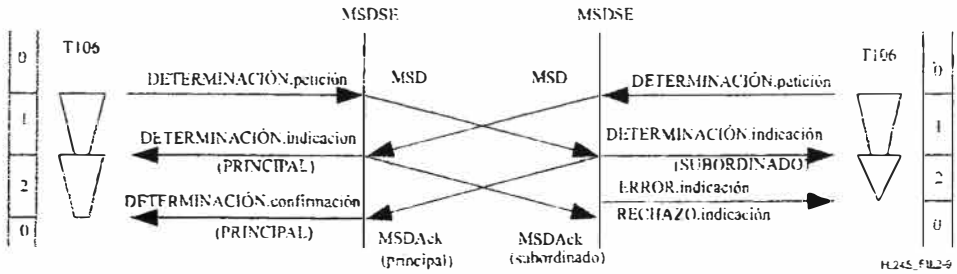


Figura II.2-9/H.245 – Determinación principal-subordinado – Procedimientos de determinación simultánea con expiración del temporizador T106 durante el estado ESPERA DE ACUSE DE RECIBO EN ENTRADA

En la figura II.2-10 se obtuvo un resultado indeterminado N100 veces. En este caso, N100 = 3.

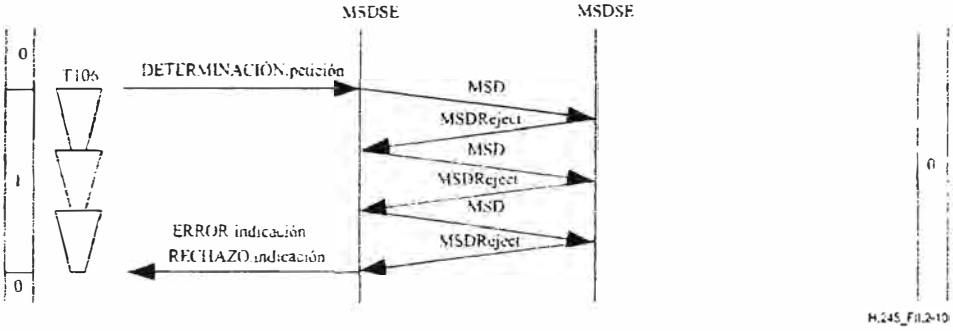


Figura II.2-10/H.245 – Determinación principal-subordinado – Resultado indeterminado con N100 = 3

II.3 Entidad de señalización de intercambio de capacidad

Las figuras II.3-1 a II.3-4 ilustran los procedimientos de la CESE. Los estados REPOSO y ESPERA DE RESPUESTA se designan por "0" y "1", respectivamente.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T H.261

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/93)

TRANSMISIÓN EN LÍNEA DE SEÑALES NO TELEFÓNICAS

CÓDEC VÍDEO PARA SERVICIOS AUDIOVISUALES A $p \times 64$ kbit/s

Recomendación UIT-T H.261

(Anteriormente «Recomendación del CCITT»)

Recomendación H.261

CÓDEC VÍDEO PARA SERVICIOS AUDIOVISUALES A $p \times 64$ kbit/s

(Ginebra, 1990, revisada en Helsinki, 1993)

El CCITT,

considerando

(a) que existe una demanda significativa de servicios videofónico, de videoconferencia, y otros servicios audiovisuales;

(b) que mediante la transmisión digital a las velocidades de los canales H_0, B o sus múltiplos, hasta la velocidad primaria, o a las de los canales H_{11}/H_{12}, pueden proporcionarse los circuitos necesarios para satisfacer esta demanda;

(c) que algunos países podrían disponer de RDSI que proporcionen un servicio de transmisión conmutada a la velocidad de los canales B, H_0 o H_{11}/H_{12};

(d) que la existencia de diferentes jerarquías digitales y diferentes normas de televisión en diferentes partes del mundo complica los problemas relativos a la especificación de las normas de transmisión y codificación para conexiones internacionales;

(e) que es probable que aparezcan varios servicios audiovisuales que utilicen los accesos RDSI básico y de velocidad primaria y que debe ser posible la intercomunicación de sus terminales;

(f) que el códec vídeo constituye un elemento esencial de la infraestructura de los servicios audiovisuales, permitiendo dicha intercomunicación en el marco de la Recomendación H.200;

(g) que la Recomendación H.120 sobre la videoconferencia con transmisión en grupo digital primario fue la primera de una serie de Recomendaciones en vías de elaboración,

observando

que los adelantos en la investigación y el desarrollo de técnicas de codificación vídeo y de reducción de la velocidad binaria llevan a la utilización de velocidades binarias inferiores, hasta 64 kbit/s, de forma que ésta puede considerarse como la segunda de la serie de Recomendaciones en vías de elaboración,

y advirtiendo

que el objetivo básico del CCITT es el de recomendar soluciones únicas para las conexiones internacionales,

recomienda

que, además de codecs conformes a la Recomendación H.120, en los servicios audiovisuales internacionales, se utilicen codecs que posean las características de codificación de transmisión y de procesamiento de señales descritas a continuación.

NOTAS

1 Los codecs de este tipo también son adecuados para algunos servicios de televisión en los que no se necesita la calidad de la difusión de señales de televisión.

2 Quedan en estudio los equipos para transcodificar desde y hacia los codecs conformes a la Recomendación H.120.

1 Objeto

Esta Recomendación describe los métodos de codificación y decodificación vídeo del componente de imagen en movimiento de los servicios audiovisuales a las velocidades de $p \times 64$ kbit/s, donde p está comprendido entre 1 y 30.

2 Breve especificación

En la Figura 1 aparece un diagrama de bloques resumido del códec.

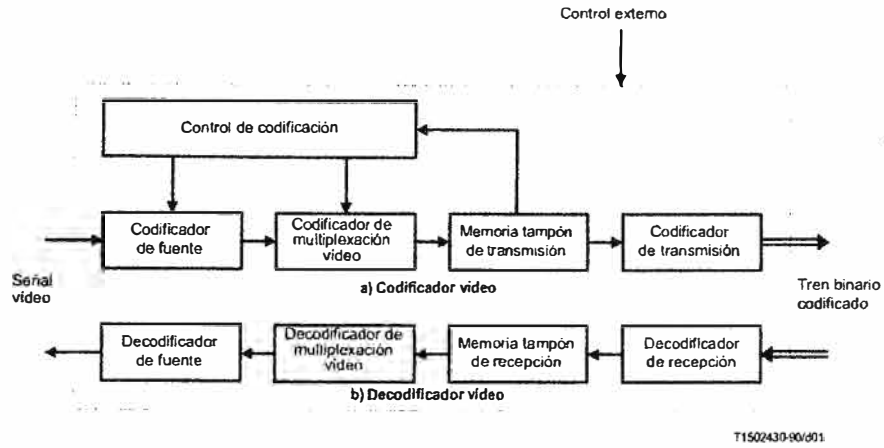


FIGURA 1/H.261

Diagrama de bloques resumido del códec vídeo

2.1 Entrada y salida vídeo

Para poder abarcar con una sola Recomendación la utilización en regiones que emplean normas de televisión de 625 y 525 líneas, y entre dichas regiones, el codificador fuente actúa sobre imágenes basadas en un formato intermedio común (CIF, *common intermediate format*). Las normas de las señales de televisión de entrada y salida, que pueden, por ejemplo, ser compuestas o de componentes analógicas o digitales, no son objeto de Recomendaciones, como tampoco lo son los métodos de realizar cualquier conversión necesaria de y hacia el formato de codificación de fuente.

2.2 Entrada y salida digital

El codificador vídeo proporciona un tren binario digital autocontenido que puede combinarse con otras señales multifacilidades (tal como se define en la Recomendación H.221, por ejemplo). El decodificador vídeo efectúa el proceso inverso.

2.3 Frecuencia de muestreo

Las imágenes se muestrean a un múltiplo entero de la frecuencia de línea vídeo. Este reloj de muestreo y el reloj de red digital son asíncronos.

2.4 Algoritmo de codificación de fuente

Se adopta una combinación de predicción interimágenes para utilizar redundancia temporal y codificación de la transformada de la señal restante para reducir la redundancia espacial. El decodificador tiene la capacidad de compensación de movimiento, permitiendo la incorporación facultativa de esta técnica en el codificador.

2.5 Velocidad binaria

Esta Recomendación está orientada fundamentalmente hacia la utilización de velocidades binarias vídeo entre unos 40 kbit/s y 2 Mbit/s.

2.6 Simetría de transmisión

El códec puede utilizarse para la comunicación visual bidireccional o unidireccional.

2.7 Tratamiento de los errores

El tren de bits transmitido contiene un código BCH (*Bose, Chaudhuri Hocquengham*) (511,493) de corrección de errores sin canal de retorno. Su utilización en el decodificador es facultativa.

2.8 Funcionamiento multipunto

Se incluyen las características necesarias para el funcionamiento multipunto conmutado.

3 Codificador de fuente

3.1 Formato de fuente

El codificador de fuente trabaja con imágenes no entrelazadas que aparecen 30 000/1001 (aproximadamente 29,97) veces por segundo. La tolerancia de la frecuencia de imagen es de ± 50 ppm.

Las imágenes se codifican para obtener la componente de luminancia y las dos componentes diferencia de color (Y, C_R y C_B). Estas componentes y los códigos que representan sus valores muestreados son los que define la Recomendación 601 del CCIR.

Negro = 16

Blanco = 235

Diferencia de color nula = 128

Diferencia de color máxima = 16 y 240.

Estos valores son nominales y el algoritmo de codificación funciona con valores de entrada comprendidos entre 1 y 254.

Se especifican dos formatos de exploración de imagen.

En el primer formato (CIF), la estructura de muestreo de la luminancia es de 352 elementos de imagen por línea, 288 líneas por imagen, en una disposición ortogonal. El muestreo de cada una de las dos componentes de diferencia de color es de 176 elementos de imagen por línea, 144 líneas por imagen, ortogonal. Las muestras de diferencia de color se sitúan de manera que sus límites de bloque coincidan con los límites de bloque de luminancia, como se muestra en la Figura 2. La zona de imagen cubierta por estos números de elementos de imagen y líneas tiene una relación de aspecto de 4:3 y corresponde a la porción activa de la entrada vídeo de norma local.

NOTA – El número de elementos de imagen por línea es compatible con el muestreo de las porciones activas de las señales de luminancia y diferencia de color de fuentes de 525 ó 625 líneas a 6,75 y 3,375 MHz respectivamente. Estas frecuencias tienen una relación simple con las de la Recomendación 601 del CCIR.

El segundo formato, de un cuarto de CIF (QCIF, *quarter-CIF*), tiene la mitad de elementos de imagen y de líneas que el formato anterior. Todos los codecs deben poder funcionar con QCIF. Algunos codecs pueden también funcionar con CIF.

Deben preverse los medios necesarios para limitar el máximo periodo de transmisión de imagen de los codificadores, dejando de transmitir al menos 0, 1, 2 ó 3 imágenes entre las imágenes transmitidas. La selección de este número mínimo y de CIF o QCIF se hará por medios externos (por ejemplo, mediante la Recomendación H.221).

3.2 Algoritmo de codificación de fuente vídeo

El codificador de fuente se muestra en forma generalizada en la Figura 3. Los principales elementos son la predicción, la transformación de bloques y la cuantificación.

El error de predicción (modo INTER) o la imagen de entrada (modo INTRA) se subdividen en bloques de 8 elementos de imagen por 8 líneas que se segmentan como transmitidos o no transmitidos. Además, cuatro bloques de luminancia y los dos bloques de diferencia de color correspondientes espacialmente se combinan para formar un macrobloque, como se muestra en la Figura 10.

FIGURA 2/H.261

Posición de las muestras de luminancia y crominancia

Los criterios de elección del modo y la transmisión de un bloque no son objeto de recomendación y pueden variar dinámicamente como parte de la estrategia de control de la codificación. Los bloques transmitidos se transforman y los coeficientes resultantes se cuantifican y se codifican con longitud variable.

3.2.1 Predicción

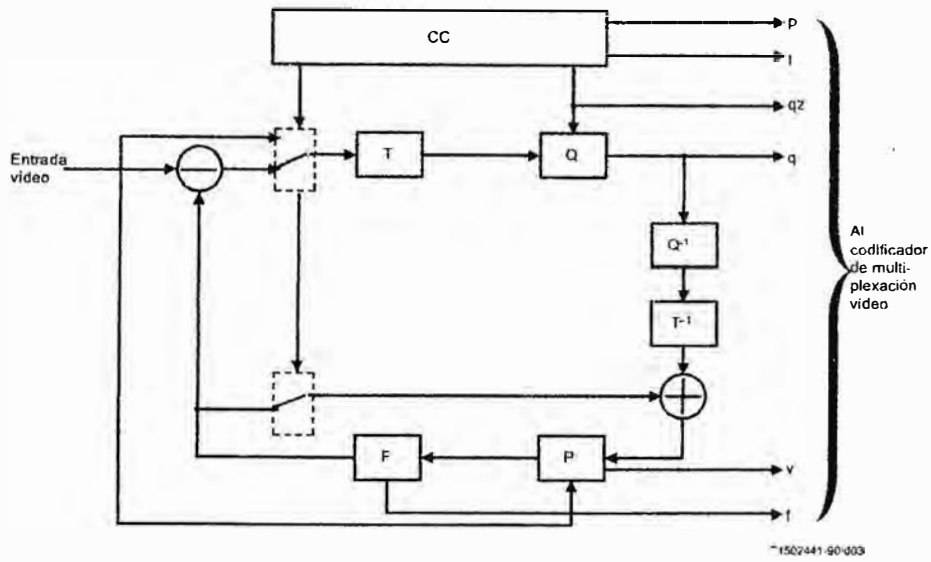
La predicción es interimágenes y puede aumentarse por compensación del movimiento (véase 3.2.2) y mediante un filtro espacial (véase 3.2.3).

3.2.2 Compensación del movimiento

La compensación del movimiento (MC, *motion compensation*) es facultativa en el codificador. El decodificador aceptará un vector por cada macrobloque. Las componentes horizontal y vertical de estos vectores de movimiento tienen valores enteros que no pasan de ± 15. El vector se utiliza para los cuatro bloques de luminancia del macrobloque. El vector de movimiento para ambos bloques de diferencia de color se obtiene dividiendo por dos los valores de las componentes del vector de macrobloque y haciendo un truncamiento a cero de las partes de magnitud para producir componentes enteros.

Un valor positivo de las componentes horizontal o vertical del vector de movimiento significa que la predicción se ha realizado a partir de elementos de imagen de la imagen anterior situados espacialmente a la derecha o debajo de los elementos de imagen objeto de predicción.

Los vectores de movimiento están limitados de manera que todos los elementos de imagen por ellos referenciados estén dentro de la zona de imagen codificada.



T Transformada
Q Cuantificador
P Memoria de imagen con retardo variable y compensación del movimiento
F Filtro de bucle
CC Control de codificación
p Bandera de INTRA/INTER
t Bandera de transmitido o no transmitido
qz Indicación de cuantificador
q Índice de cuantificación para los coeficientes de la transformada
v Vector de movimiento
f Activación/desactivación de filtro de bucle

FIGURA 3/H.261
Codificador fuente

3.2.3 Filtro de bucle

El proceso de predicción puede modificarse mediante un filtro espacial bidimensional (FIL) que actúa sobre los elementos de imagen de un bloque predicho de ocho por ocho.

El filtro es separable en funciones unidimensionales horizontal y vertical. Ambas son no recursivas con coeficientes de 1/4, 1/2, 1/4 excepto en los bordes del bloque, donde uno de los puntos de toma caería fuera del bloque. En tales casos se modifica el filtro unidimensional para que tenga coeficientes 0, 1, 0. La precisión aritmética se conserva totalmente redondeando a valores enteros de ocho bits en la salida del filtro bidimensional. Los valores cuya parte fraccionaria es un medio se redondean al valor superior.

El filtro se activa/desactiva para los seis bloques de un macrobloque según el tipo de macrobloque (véase MTYPE en 4.2.3).

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T G.729

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(03/96)

ASPECTOS GENERALES DE LOS SISTEMAS DE TRANSMISIÓN DIGITAL

CODIFICACIÓN DE LA VOZ A 8 kbit/s MEDIANTE PREDICCIÓN LINEAL CON EXCITACIÓN POR CÓDIGO ALGEBRAICO DE ESTRUCTURA CONJUGADA

Recomendación UIT-T G.729

(Anteriormente «Recomendación del CCITT»)

Recomendación G.729

CODIFICACIÓN DE LA VOZ A 8 kbit/s MEDIANTE PREDICCIÓN LINEAL CON EXCITACIÓN POR CÓDIGO ALGEBRAICO DE ESTRUCTURA CONJUGADA

(Ginebra, 1996)

1 Introducción

En la presente Recomendación se describe un algoritmo para la codificación de la voz a 8 kbit/s mediante predicción lineal con excitación por código algebraico con estructura conjugada (CS-ACELP, *conjugate-structure algebraic-code-excited linear-prediction*).

El códec en cuestión está diseñado para operar con una señal digital obtenida tras efectuar, primero un filtrado con la anchura de banda telefónica (Recomendación G.712) de la señal analógica de entrada, seguido de su muestreo a 8000 Hz y su conversión a una modulación por impulsos codificados (MIC) lineal de 16 bits, para entrar en el codificador. La salida del decodificador deberá reconvertirse a una señal analógica siguiendo un método similar. Otras características de entrada/salida, como las que se especifican en la Recomendación G.711 para datos MIC de 64 kbit/s, deberán convertirse a MIC lineal de 16 bits antes de codificar, o de MIC lineal de 16 bits al formato apropiado después de decodificar. El tren de bits del codificador al decodificador se define dentro de esta norma.

La Recomendación está estructurada como sigue: la cláusula 2 presenta un resumen general del algoritmo CS-ACELP. En las cláusulas 3 y 4 se exponen, respectivamente, los principios del codificador y del decodificador CS-ACELP. La cláusula 5 describe el soporte lógico que define dicho códec en una aritmética de coma fija de 16 bits.

2 Descripción general del codificador/decodificador (códec)

El códec CS-ACELP se basa en el modelo de codificación mediante la predicción lineal con excitación por código (CELP). Opera con tramas vocales de 10 ms correspondientes a 80 muestras a una velocidad de muestreo de 8000 muestras por segundo. En cada trama de 10 ms se analiza la señal vocal para extraer los parámetros del modelo CELP (coeficientes de filtros de predicción lineal, ganancias e índices de las tablas de códigos adaptativos y fijos). Los parámetros en cuestión se codifican y se transmiten. El Cuadro 1 ilustra la asignación de bits para los parámetros del códec. En el decodificador, dichos parámetros se utilizan para recuperar los parámetros de excitación y del filtro de síntesis. La voz se reconstruye filtrando la excitación a través del filtro de síntesis de corto plazo, como se ve en la Figura 1. El filtro de síntesis de corto plazo se basa en un filtro de predicción lineal (PL) de décimo orden. El filtro de síntesis de largo plazo o de tono se aplica mediante el método de la llamada tabla de códigos adaptativos. Tras calcular la señal vocal reconstruida, ésta se mejora con un postfiltrado.

CUADRO 1/G.729

Asignación de bit de algoritmos CS-ACELP a 8 kbit/s por segundo (trama de 10 ms)

Parámetro	Palabra de código	Subtrama 1	Subtrama 2	Total por trama
Pares del espectro lineal (LSP)	*L0, L1, L2, L3*			18
Retardo de la tabla de códigos adaptativos	*P1, P2*	8	5	13
Paridad del retardo de tono	*P0*	1		1
Índice de tabla de códigos fijos	*C1, C2*	13	13	26
Signo de tabla de códigos fijos	*S1, S2*	4	4	8
Ganancias de tabla de códigos (fase 1)	*GA1, GA2*	3	3	6
Ganancias de tabla de códigos (fase 2)	*GB1, GB2*	4	4	8
Total				80

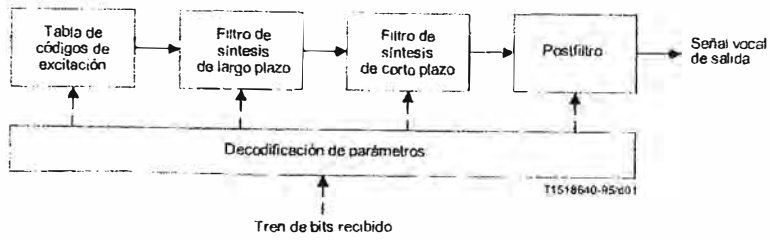


FIGURA I/G.729

Diagrama funcional del modelo conceptual de síntesis (CELP)

2.1 Codificador

El principio de codificación puede observarse en la Figura 2. La señal de entrada pasa por un filtro de paso alto y se pone a escala en el bloque de preprocesamiento. La señal preprocesada actúa como señal de entrada para todo el análisis ulterior. Se efectúa un análisis de predicción lineal (LP) para cada trama de 10 ms con el fin de calcular los coeficientes de filtro LP. Éstos se convierten en pares del espectro lineal (LSP, *line spectrum pairs*), cuantificándose mediante una cuantificación vectorial (VQ) predictiva en dos etapas de 18 bits. La señal de excitación se selecciona utilizando un procedimiento de búsqueda basado en el análisis por síntesis, según el cual la diferencia entre la señal original y la reconstruida se reduce al mínimo de acuerdo con una medida de la distorsión ponderada perceptualmente. Esto se logra pasando la señal de error por un filtro de ponderación perceptual, cuyos coeficientes se derivan del filtro LP sin cuantificar. El valor de la ponderación perceptual se hace adaptativa, con el fin de mejorar la calidad para señales de entrada con una respuesta de frecuencia plana.

Los parámetros de excitación (parámetros de tabla de códigos fijos y adaptativos) se determinan para cada subtrama de 5 ms (40 muestras). Los coeficientes cuantificados y no cuantificados del filtro LP se aplican a la segunda subtrama, mientras que para la primera subtrama se utilizan coeficientes del filtro LP interpolados (cuantificados o no). Se estima un retardo de tono en buele abierto por cada trama de 10 ms, en base a señal vocal ponderada perceptualmente. Luego se efectúan, para cada subtrama por separado, las siguientes operaciones. Se calcula la señal objetivo $x(n)$ pasando el LP residual por el filtro de síntesis ponderado $W(z)/\hat{A}(z)$. Los estados iniciales de estos filtros se actualizan filtrando la diferencia que se produce entre el residuo LP y la excitación. Ello equivale al método corriente de sustraer de la señal vocal ponderada la respuesta de entrada cero del filtro de síntesis ponderado. Se calcula la respuesta de impulso $h(n)$ del filtro de síntesis ponderado. Seguidamente se analiza el tono en buele cerrado (para determinar el retardo y ganancia de la tabla de códigos adaptativos) mediante la respuesta objetivo $x(n)$ y la respuesta a los impulsos $h(n)$, indagando en torno al valor del retardo de tono de buele abierto. Se utiliza un retardo de tono fraccionario de 1/3 de definición. El retardo de tono se codifica con 8 bits para la primera subtrama y diferencialmente con 5 bits para la segunda. La señal objetivo $x(n)$ se actualiza sustrayendo la contribución (filtrada) de la tabla de códigos adaptativos y se aplica este nuevo objetivo, $x'(n)$, para la búsqueda de la tabla de códigos fijos, con el fin de obtener la excitación óptima. Para la excitación de la tabla de códigos fijos se aplica una tabla de códigos algebraicos de 17 bits. Las ganancias de las contribuciones de las tablas de códigos adaptativos y fijos se cuantifican vectorialmente con 7 bits (con una predicción de media móvil aplicada a la ganancia de la tabla de códigos fijos). Finalmente, se actualizan las memorias de los filtros mediante la señal de excitación así determinada.

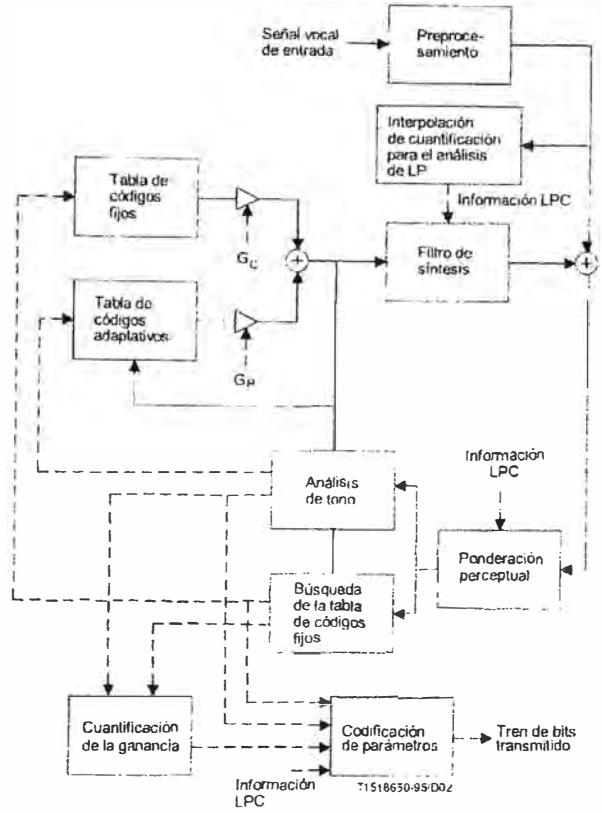


FIGURA 2/G.729

Principio de codificación del codificador CS-ACELP

2.2 Decodificador

El principio del decodificador aparece en la Figura 3. Primero se extraen los índices de los parámetros a partir del tren de bits recibido. Los índices se decodifican para obtener los parámetros del códec correspondientes a una trama de voz de 10 ms. Estos parámetros son los coeficientes LSP, los dos retardos de tono fraccionarios, los dos vectores de la tabla de códigos fijos y ambos conjuntos de ganancias de las tablas de códigos adaptativos y fijos. Los coeficientes LSP se interpolan y se convierten en coeficientes del filtro LP de cada subtrama. A continuación, para cada subtrama de 5 ms se aplican los siguientes pasos:

- se construye la excitación sumando los vectores de las tablas de los códigos adaptativos y fijos, puestos a escala por sus respectivas ganancias;
- se reconstruye la señal vocal filtrando la excitación por el filtro de síntesis LP;
- se hace pasar la señal vocal reconstruida a través de una fase de postprocesamiento, que incluye un postfiltro adaptativo basado en filtros de síntesis de largo y corto plazo, seguido de un filtro de paso alto y un escalamiento.

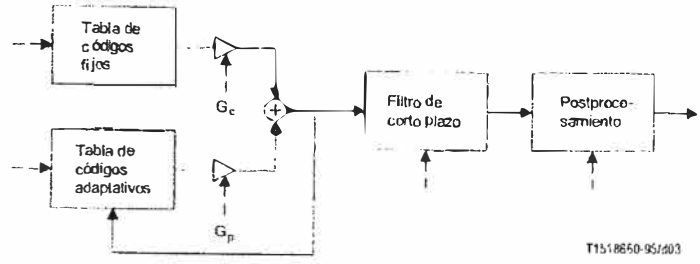


FIGURA 3/G.729

Principio del decodificador CS-ACELP

2.3 Retardo

El códec codifica la voz y otras señales de audio con tramas de 10 ms. Se produce además un preanálisis de 5 ms, por lo que el retardo algorítmico total es de 15 ms. Los demás retardos producidos por la aplicación práctica de este códec tienen por causa:

- el tiempo de procesamiento necesario para las operaciones de codificación y decodificación;
- el tiempo de transmisión en el enlace de comunicación;
- el retardo de multiplexación por la combinación de datos de señales vocales y otros.

2.4 Descripción del códec de señales vocales

La descripción del algoritmo de codificación/decodificación de la voz en la presente Recomendación se hace en términos de operaciones matemáticas de coma fija y exactitud de bits. El código C de ANSI, indicado en la cláusula 5 y que es parte integrante de esta Recomendación, refleja este método descriptivo de coma fija y exactitud de bit. Las descripciones matemáticas del codificador (véase la cláusula 3) y del decodificador (véase la cláusula 4) pueden aplicarse también de varias otras maneras, dando lugar, quizás, a aplicaciones del códec que no satisfacen los términos de esta Recomendación. Por este motivo, la descripción del algoritmo del código C de ANSI que figura en la cláusula 5 prevalecerá en caso de discrepancia con cualquier otra descripción matemática contenida en las cláusulas 3 y 4. Sin llegar a ser exhaustivo, puede obtenerse de la UIT un juego de señales de prueba utilizables al aplicar el código C de ANSI.

2.5 Convenciones de notación

En todo este documento se ha procurado seguir las siguientes convenciones de notación:

- Las tablas de códigos se destacan por medio de caracteres caligráficos (por ejemplo $\mathcal{C}$).
- Las señales de tiempo se destacan mediante su símbolo seguido de un índice de muestra entre paréntesis [por ejemplo $s(n)$]. El símbolo n se utiliza como índice de muestra.
- Los superíndices entre paréntesis (por ejemplo $g^{(m)}$) se utilizan para indicar la dependencia en el tiempo de las variables. La variable m corresponde, según el contexto, a un índice de trama o de subtrama, mientras que la variable n corresponde a un índice de muestra.
- Los índices de recursión se identifican mediante un superíndice entre corchetes (por ejemplo $E^{[k]}$).
- Los subíndices identifican un elemento particular de una matriz de coeficientes.
- El símbolo $\hat{}$ identifica la versión cuantificada de un parámetro (por ejemplo $\hat{g}_c$).
- Entre corchetes se expresan los intervalos de los parámetros, incluyendo sus límites (por ejemplo [0.6, 0.9]).

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T **G.711**

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

ASPECTOS GENERALES DE LOS SISTEMAS DE TRANSMISIÓN DIGITAL

EQUIPOS TERMINALES

MODULACIÓN POR IMPULSOS CODIFICADOS (MIC) DE FRECUENCIAS VOCALES

Recomendación UIT-T G.711

(Extracto del *Libro Azul*)

Recomendación G.711

MODULACIÓN POR IMPULSOS CODIFICADOS (MIC) DE FRECUENCIAS VOCALES

(Ginebra, 1972; modificada posteriormente)

Consideraciones generales

Se recomienda el empleo de las siguientes características para la codificación de señales de frecuencias vocales.

2 Velocidad de muestreo

El valor nominal recomendado es de 8000 muestras por segundo con una tolerancia de ± 50 partes por millón (ppm).

3 Ley de codificación

3.1 Para los circuitos internacionales deben utilizarse ocho dígitos binarios por muestra.

3.2 Se recomiendan dos leyes de codificación, designadas ley A y ley μ. Las definiciones de estas leyes se encuentran en los cuadros 1a/G.711 y 1b/G.711, y en los cuadros 2a/G.711 y 2b/G.711, respectivamente.

Si se utiliza la ley μ en redes que requieran la supresión de la señal de carácter "todos 0", la señal de carácter correspondiente a valores de entrada negativos comprendidos entre valores de decisión 127 y 128, será 00000010, y el valor a la salida del decodificador será −7519. Al valor de salida del decodificador corresponde el número 125.

3.3 El número de valores cuantificados viene dado por la ley de codificación.

3.4 Los trayectos digitales entre países que hayan adoptado leyes de codificación diferentes deberán efectuar la transmisión con señales codificadas según la ley A. Cuando los dos países hayan adoptado la misma ley, deberá utilizarse esa ley en los trayectos digitales entre los mismos. Incumbirá a los países que utilicen la ley μ efectuar toda conversión necesaria.

3.5 Las reglas para la conversión se dan en los cuadros 3/G.711 y 4/G.711.

3.6 *Conversión a MIC uniforme y a partir de ella*

Cada "valor de decisión" y "valor cuantificado" de ley A (o μ) debe asociarse a un "valor MIC uniforme". (Véase la definición de "valor de decisión" y "valor cuantificado" en la Recomendación G.701 y en particular en la figura 2/G.701.) Esto requiere la aplicación de un código MIC uniforme con 13 (14) bits. En los cuadros 1/G.711 y 2/G.711 se indica la transformación del MIC de ley A y del MIC de ley μ, respectivamente, a MIC uniforme. La conversación de los valores de ley A o ley μ a partir de los valores de MIC uniforme correspondientes a los valores de decisión figurará en las especificaciones de cada equipo. En el § 4.2.8 de la Recomendación G.721, subbloque COMPRESS, se describe una opción.

4 Transmisión de señales de carácter

Cuando se transmiten en serie las señales de carácter, esto es, consecutivamente en un medio físico, el bit 1 (bit de polaridad) se transmite en primer lugar y el bit 8 (el bit menos significativo) en último lugar.

5 Relación entre las leyes de codificación y el nivel de la señal de frecuencias vocales

La relación entre las leyes de codificación de los cuadros 1/G.711 y 2/G.711 y el nivel de la señal de frecuencias vocales se define como sigue:

En una salida de frecuencias vocales cualquiera del multiplexor MIC debe haber una señal sinusoidal de 1 kHz con un nivel nominal de 0 dBm0 al aplicarse a la entrada del decodificador la secuencia periódica de señales de carácter del cuadro 5/G.711 para la ley A y del cuadro 6/G.711 para la ley μ.

El nivel de sobrecarga teórica resultante ($U_{máx.}$) es de +3,14 dBm0 para la ley A y de +3,17 dBm0 para la ley μ.

CUADRO 1a/G.711

Ley A: valores de entrada positivos

1	2	3	4	5	6	7	8
Número de los segmentos	Número de intervalos × dimensión de los intervalos	Valor en los extremos de los segmentos	Número de los valores de decisión n	Valor de decisión x_n (véase la nota 1)	Señal de carácter antes de la inversión de los bits pares Número de los bits 1 2 3 4 5 6 7 8	Valor cuantificado (valor a la salida del decodificador) y_n	Número de los valores a la salida del decodificador
		4096	(128)	(4096)	- - - - - - - -		
			127	3968	1 1 1 1 1 1 1 1	4032	128
7	16 × 128				(véase la nota 2)		
			113	2176			
		2048	112	2048	1 1 1 1 0 0 0 0	2112	113
6	16 × 64				(véase la nota 2)		
			97	1088			
		1024	96	1024	1 1 1 0 0 0 0 0	1056	97
5	16 × 32				(véase la nota 2)		
			81	544			
		512	80	512	1 1 0 1 0 0 0 0	528	81
4	16 × 16				(véase la nota 2)		
			65	272			
		256	64	256	1 1 0 0 0 0 0 0	264	65
3	16 × 8				(véase la nota 2)		
			49	136			
		128	48	128	1 0 1 1 0 0 0 0	132	49
2	16 × 4				(véase la nota 2)		
			33	68			
		64	32	64	1 0 1 0 0 0 0 0	66	33
1	32 × 2				(véase la nota 2)		
↓			1	2			
					1 0 0 0 0 0 0 0	1	1
			0	0			

Nota 1 – 4096 unidades de valor normalizado corresponden a $T_{máx}$ = 3,14 dBm0.

Nota 2 – Las señales de carácter se obtienen invirtiendo los bits pares de las señales de la columna 6. Antes de esta inversión, la señal de carácter correspondiente a los valores de entrada positivos comprendidos entre dos valores de decisión sucesivos n y $n+1$ (véase la columna 4) es $(128+n)$ expresado como un número binario.

Nota 3 – El valor a la salida del decodificador es $y_n = \frac{x_{n-1} + x_n}{2}$ para $n = 1, \ldots 127, 128$

Nota 4 – x_{128} es un valor virtual de decisión

Nota 5 – En los cuadros 1/G.711 y 2/G.711, los valores de la codificación uniforme figuran en las columnas 3, 5 y 7.

CUADRO 1b / G.711

Ley A: valores de entrada negativos

1	2	3	4	5	6	7	8
Número de los segmentos	Número de intervalos × dimensión de los intervalos	Valor en los extremos de los segmentos	Número de los valores de decisión n	Valor de decisión x_n (véase la nota 1)	Señal de carácter antes de la inversión de los bits pares Número de los bits 1 2 3 4 5 6 7 8	Valor cuantificado (valor a la salida del decodificador) y_n	Número de los valores a la salida del decodificador
			0	0			
				−2	0 0 0 0 0 0 0 0	−1	1
1	32 × 2				(véase la nota 2)		
		−64	32	−64			
					0 0 1 0 0 0 0 0	−66	33
2	16 × 4		33	−68	(véase la nota 2)		
		−128	48	−128			
					0 0 1 1 0 0 0 0	−132	49
3	16 × 8		49	−136	(véase la nota 2)		
		−256	64	−256			
					0 1 0 0 0 0 0 0	−264	65
4	16 × 16		65	−272	(véase la nota 2)		
		−512	80	−512			
					0 1 0 1 0 0 0 0	−528	81
5	16 × 32		81	−544	(véase la nota 2)		
		−1024	96	−1024			
					0 1 1 0 0 0 0 0	−1056	97
6	16 × 64		97	−1088	(véase la nota 2)		
		−2048	112	−2048			
					0 1 1 1 0 0 0 0	−2112	113
			113	−2176			
7	16 × 128				(véase la nota 2)		
			127	−3968			
					0 1 1 1 1 1 1 1	−4032	128
		−4096	128	(−4096)			

Nota 1 – 4096 unidades de valor normalizado corresponden a T máx. = 3,14 dBm0.

Nota 2 – Las señales de carácter se obtienen invirtiendo los bits pares de las señales de la columna 6. Antes de esta inversión, la señal de carácter correspondiente a los valores de entrada negativos comprendidos entre dos valores de decisión sucesivos n y $n+1$ (véase la columna 4) es n expresado como un número binario.

Nota 3 – El valor a la salida del decodificador es $y_n = \frac{x_{n-1} + x_n}{2}$ para n = 1, ..., 127, 128.

Nota 4 – x_{128} es un valor virtual de decisión.

Nota 5 – En los cuadros 1/G.711 y 2/G.711, los valores de la codificación uniforme figuran en las columnas 3, 5 y 7.

CUADRO 2a / G.711

Ley μ: valores de entrada positivos

1	2	3	4	5	6	7	8
Número de los segmentos	Número de intervalos × dimensión de los intervalos	Valor en los extremos de los segmentos	Número de los valores de decisión n	Valor de decisión x_n (véase la nota 1)	Señal de carácter Número de los bits 1 2 3 4 5 6 7 8	Valor cuantificado (valor a la salida del decodificador) y_n	Número de los valores a la salida del decodificador
		8159	(128)	(8159)			
			127	7903	1 0 0 0 0 0 0 0	8031	127
8	16 × 256				(véase la nota 2)		
			113	4319			
		4063	112	4063	1 0 0 0 1 1 1 1	4191	112
7	16 × 128				(véase la nota 2)		
			97	2143			
					1 0 0 1 1 1 1	2079	96
		2015	96	2015			
6	16 × 64				(véase la nota 2)		
			81	1055			
					1 0 1 0 1 1 1 1	1023	80
		991	80	991			
5	16 × 32				(véase la nota 2)		
			65	511			
					1 0 1 1 1 1 1 1	495	64
		479	64	479			
4	16 × 16				(véase la nota 2)		
			49	239			
					1 1 0 0 1 1 1 1	231	48
		223	48	223			
3	16 × 8				(véase la nota 2)		
			33	103			
					1 1 0 1 1 1 1 1	99	32
		95	32	95			
2	16 × 4				(véase la nota 2)		
			17	35			
					1 1 1 0 1 1 1 1	33	16
		31	16	31			
	15 × 2				(véase la nota 2)		
			2	3			
					1 1 1 1 1 1 1 0	2	1
1			1	1			
					1 1 1 1 1 1 1 1	0	0
▼	1 × 1		0	0			

Nota 1 – 8159 unidades de valor normalizado corresponden a $T_{máx}$ = 3,17 dBm0.

Nota 2 – La señal de carácter correspondiente a los valores de entrada positivos comprendidos entre dos valores de decisión sucesivos n y $n+1$ (véase la columna 4) es (255 – n) expresado como un número binario.

Nota 3 – El valor a la salida del decodificador es $y_0 = x_0 = 0$ para $n = 0$ e $y_n = \frac{x_n + x_{n-1}}{2}$ para $n = 1, 2, \ldots 127$.

Nota 4 – x_{128} es un valor virtual de decisión.

Nota 5 – En los cuadros 1/G.711 y 2/G.711, los valores de la codificación uniforme figuran en las columnas 3, 5 y 7.

CUADRO 2b/ G.711

Ley μ: valores de entrada negativos

1	2	3	4	5	6	7	8
Número de los segmentos	Número de intervalos × dimensión de los intervalos	Valor en los extremos de los segmentos	Número de los valores de decisión n	Valor de decisión v_n (véase la nota 1)	Señal de carácter Número de los bits 1 2 3 4 5 6 7 8	Valor cuantificado (valor a la salida del decodificador) y_n	Número de los valores a la salida del decodificador
▲	1 × 1		0	0	0 1 1 1 1 1 1 1	0	0
			1	−1			
1			2	−3	0 1 1 1 1 1 1 0	−2	1
	15 × 2				(véase la nota 2)		
		−31	16	−31			
			17	−35	0 1 1 0 1 1 1 1	−33	16
2	16 × 4				(véase la nota 2)		
		−95	32	−95			
			33	−103	0 1 0 1 1 1 1 1	99	32
3	16 × 8				(véase la nota 2)		
		−223	48	−223			
			49	−239	0 1 0 0 1 1 1 1	−231	48
4	16 × 16				(véase la nota 2)		
		−479	64	−479			
			65	511	0 0 1 1 1 1 1 1	−495	64
5	16 × 32				(véase la nota 2)		
		−991	80	−991			
			81	−1055	0 0 1 0 1 1 1 1	−1023	80
6	16 × 64				(véase la nota 2)		
		−2015	96	−2015			
			97	−2143	0 0 0 1 1 1 1 1	−2079	96
7	16 × 128				(véase la nota 2)		
		−4063	112	−4063			
			113	−4319	0 0 0 0 1 1 1 1	−4191	112
8	16 × 256				(véase la nota 2)		
			126	−7647			
			127	−7903	0 0 0 0 0 0 0 1	−7775	126
		−8159	(128)	(−8159)	0 0 0 0 0 0 0 0	−8031	127

Nota 1 – 8159 unidades de valor normalizado corresponden a T_{max} = 3,17 dBm0.

Nota 2 – La señal de carácter correspondiente a los valores de entrada negativos comprendidos entre dos valores de decisión sucesivos n y $n+1$ (véase la columna 4) es $(127 - n)$ expresado como un número binario, para $n = 1, 2, \ldots 127$.

Nota 3 – El valor a la salida del decodificador es $y_0 = v_0 = 0$ para $n = 0$ e $y_n = \frac{v_n + v_{n+1}}{2}$ para $n = 1, 2, \ldots 127$.

Nota 4 – v_{128} es un valor virtual de decisión.

Nota 5 – En los cuadros 1/G.711 y 2/G.711, los valores de la codificación uniforme figuran en las columnas 3, 5 y 7.

Network Working Group
Request for Comments: 3550
Obsoletes: 1889
Category: Standards Track

H. Schulzrinne
Columbia University
S. Casner
Packet Design
R. Frederick
Blue Coat Systems Inc.
V. Jacobson
Packet Design
July 2003

RTP: A Transport Protocol for Real-Time Applications

Status of this Memo

Copyright Notice

Abstract

This memorandum describes RTP, the real-time transport protocol. RTP provides end-to-end network transport functions suitable for applications transmitting real-time data, such as audio, video or simulation data, over multicast or unicast network services. RTP does not address resource reservation and does not guarantee quality-of-service for real-time services. The data transport is augmented by a control protocol (RTCP) to allow monitoring of the data delivery in a manner scalable to large multicast networks, and to provide minimal control and identification functionality. RTP and RTCP are designed to be independent of the underlying transport and network layers. The protocol supports the use of RTP-level translators and mixers.

Most of the text in this memorandum is identical to RFC 1889 which it obsoletes. There are no changes in the packet formats on the wire, only changes to the rules and algorithms governing how the protocol is used. The biggest change is an enhancement to the scalable timer algorithm for calculating when to send RTCP packets in order to minimize transmission in excess of the intended rate when many participants join a session simultaneously.

1. Introduction

This memorandum specifies the real-time transport protocol (RTP), which provides end-to-end delivery services for data with real-time characteristics, such as interactive audio and video. Those services include payload type identification, sequence numbering, timestamping and delivery monitoring. Applications typically run RTP on top of UDP to make use of its multiplexing and checksum services; both protocols contribute parts of the transport protocol functionality. However, RTP may be used with other suitable underlying network or transport protocols (see Section 11). RTP supports data transfer to multiple destinations using multicast distribution if provided by the underlying network.

Note that RTP itself does not provide any mechanism to ensure timely delivery or provide other quality-of-service guarantees, but relies on lower-layer services to do so. It does not guarantee delivery or prevent out-of-order delivery, nor does it assume that the underlying network is reliable and delivers packets in sequence. The sequence numbers included in RTP allow the receiver to reconstruct the sender's packet sequence, but sequence numbers might also be used to determine the proper location of a packet, for example in video decoding, without necessarily decoding packets in sequence.

While RTP is primarily designed to satisfy the needs of multi-participant multimedia conferences, it is not limited to that particular application. Storage of continuous data, interactive distributed simulation, active badge, and control and measurement applications may also find RTP applicable.

This document defines RTP, consisting of two closely-linked parts:

- the real-time transport protocol (RTP), to carry data that has real-time properties.

- the RTP control protocol (RTCP), to monitor the quality of service and to convey information about the participants in an on-going session. The latter aspect of RTCP may be sufficient for "loosely controlled" sessions, i.e., where there is no explicit membership control and set-up, but it is not necessarily intended to support all of an application's control communication requirements. This functionality may be fully or partially subsumed by a separate session control protocol, which is beyond the scope of this document.

RTP represents a new style of protocol following the principles of application level framing and integrated layer processing proposed by Clark and Tennenhouse [10]. That is, RTP is intended to be malleable

to provide the information required by a particular application and will often be integrated into the application processing rather than being implemented as a separate layer. RTP is a protocol framework that is deliberately not complete. This document specifies those functions expected to be common across all the applications for which RTP would be appropriate. Unlike conventional protocols in which additional functions might be accommodated by making the protocol more general or by adding an option mechanism that would require parsing, RTP is intended to be tailored through modifications and/or additions to the headers as needed. Examples are given in Sections 5.3 and 6.4.3.

Therefore, in addition to this document, a complete specification of RTP for a particular application will require one or more companion documents (see Section 13):

- a profile specification document, which defines a set of payload type codes and their mapping to payload formats (e.g., media encodings). A profile may also define extensions or modifications to RTP that are specific to a particular class of applications. Typically an application will operate under only one profile. A profile for audio and video data may be found in the companion RFC 3551 [1].

- payload format specification documents, which define how a particular payload, such as an audio or video encoding, is to be carried in RTP.

A discussion of real-time services and algorithms for their implementation as well as background discussion on some of the RTP design decisions can be found in [11].

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [2] and indicate requirement levels for compliant RTP implementations.

2. RTP Use Scenarios

The following sections describe some aspects of the use of RTP. The examples were chosen to illustrate the basic operation of applications using RTP, not to limit what RTP may be used for. In these examples, RTP is carried on top of IP and UDP, and follows the conventions established by the profile for audio and video specified in the companion RFC 3551.

2.1 Simple Multicast Audio Conference

A working group of the IETF meets to discuss the latest protocol document, using the IP multicast services of the Internet for voice communications. Through some allocation mechanism the working group chair obtains a multicast group address and pair of ports. One port is used for audio data, and the other is used for control (RTCP) packets. This address and port information is distributed to the intended participants. If privacy is desired, the data and control packets may be encrypted as specified in Section 9.1, in which case an encryption key must also be generated and distributed. The exact details of these allocation and distribution mechanisms are beyond the scope of RTP.

The audio conferencing application used by each conference participant sends audio data in small chunks of, say, 20 ms duration. Each chunk of audio data is preceded by an RTP header; RTP header and data are in turn contained in a UDP packet. The RTP header indicates what type of audio encoding (such as PCM, ADPCM or LPC) is contained in each packet so that senders can change the encoding during a conference, for example, to accommodate a new participant that is connected through a low-bandwidth link or react to indications of network congestion.

The Internet, like other packet networks, occasionally loses and reorders packets and delays them by variable amounts of time. To cope with these impairments, the RTP header contains timing information and a sequence number that allow the receivers to reconstruct the timing produced by the source, so that in this example, chunks of audio are contiguously played out the speaker every 20 ms. This timing reconstruction is performed separately for each source of RTP packets in the conference. The sequence number can also be used by the receiver to estimate how many packets are being lost.

Since members of the working group join and leave during the conference, it is useful to know who is participating at any moment and how well they are receiving the audio data. For that purpose, each instance of the audio application in the conference periodically multicasts a reception report plus the name of its user on the RTCP (control) port. The reception report indicates how well the current speaker is being received and may be used to control adaptive encodings. In addition to the user name, other identifying information may also be included subject to control bandwidth limits. A site sends the RTCP BYE packet (Section 6.6) when it leaves the conference.

2.2 Audio and Video Conference

If both audio and video media are used in a conference, they are transmitted as separate RTP sessions. That is, separate RTP and RTCP packets are transmitted for each medium using two different UDP port pairs and/or multicast addresses. There is no direct coupling at the RTP level between the audio and video sessions, except that a user participating in both sessions should use the same distinguished (canonical) name in the RTCP packets for both so that the sessions can be associated.

One motivation for this separation is to allow some participants in the conference to receive only one medium if they choose. Further explanation is given in Section 5.2. Despite the separation, synchronized playback of a source's audio and video can be achieved using timing information carried in the RTCP packets for both sessions.

2.3 Mixers and Translators

So far, we have assumed that all sites want to receive media data in the same format. However, this may not always be appropriate. Consider the case where participants in one area are connected through a low-speed link to the majority of the conference participants who enjoy high-speed network access. Instead of forcing everyone to use a lower-bandwidth, reduced-quality audio encoding, an RTP-level relay called a mixer may be placed near the low-bandwidth area. This mixer resynchronizes incoming audio packets to reconstruct the constant 20 ms spacing generated by the sender, mixes these reconstructed audio streams into a single stream, translates the audio encoding to a lower-bandwidth one and forwards the lower-bandwidth packet stream across the low-speed link. These packets might be unicast to a single recipient or multicast on a different address to multiple recipients. The RTP header includes a means for mixers to identify the sources that contributed to a mixed packet so that correct talker indication can be provided at the receivers.

Some of the intended participants in the audio conference may be connected with high bandwidth links but might not be directly reachable via IP multicast. For example, they might be behind an application-level firewall that will not let any IP packets pass. For these sites, mixing may not be necessary, in which case another type of RTP-level relay called a translator may be used. Two translators are installed, one on either side of the firewall, with the outside one funneling all multicast packets received through a secure connection to the translator inside the firewall. The translator inside the firewall sends them again as multicast packets to a multicast group restricted to the site's internal network.

Mixers and translators may be designed for a variety of purposes. An example is a video mixer that scales the images of individual people in separate video streams and composites them into one video stream to simulate a group scene. Other examples of translation include the connection of a group of hosts speaking only IP/UDP to a group of hosts that understand only ST-II, or the packet-by-packet encoding translation of video streams from individual sources without resynchronization or mixing. Details of the operation of mixers and translators are given in Section 7.

2.4 Layered Encodings

Multimedia applications should be able to adjust the transmission rate to match the capacity of the receiver or to adapt to network congestion. Many implementations place the responsibility of rate-adaptivity at the source. This does not work well with multicast transmission because of the conflicting bandwidth requirements of heterogeneous receivers. The result is often a least-common denominator scenario, where the smallest pipe in the network mesh dictates the quality and fidelity of the overall live multimedia "broadcast".

Instead, responsibility for rate-adaptation can be placed at the receivers by combining a layered encoding with a layered transmission system. In the context of RTP over IP multicast, the source can stripe the progressive layers of a hierarchically represented signal across multiple RTP sessions each carried on its own multicast group. Receivers can then adapt to network heterogeneity and control their reception bandwidth by joining only the appropriate subset of the multicast groups.

Details of the use of RTP with layered encodings are given in Sections 6.3.9, 8.3 and 11.

3. Definitions

RTP payload: The data transported by RTP in a packet, for example audio samples or compressed video data. The payload format and interpretation are beyond the scope of this document.

RTP packet: A data packet consisting of the fixed RTP header, a possibly empty list of contributing sources (see below), and the payload data. Some underlying protocols may require an encapsulation of the RTP packet to be defined. Typically one packet of the underlying protocol contains a single RTP packet, but several RTP packets MAY be contained if permitted by the encapsulation method (see Section 11).

RTCP packet: A control packet consisting of a fixed header part similar to that of RTP data packets, followed by structured elements that vary depending upon the RTCP packet type. The formats are defined in Section 6. Typically, multiple RTCP packets are sent together as a compound RTCP packet in a single packet of the underlying protocol; this is enabled by the length field in the fixed header of each RTCP packet.

Port: The "abstraction that transport protocols use to distinguish among multiple destinations within a given host computer. TCP/IP protocols identify ports using small positive integers." [12] The transport selectors (TSEL) used by the OSI transport layer are equivalent to ports. RTP depends upon the lower-layer protocol to provide some mechanism such as ports to multiplex the RTP and RTCP packets of a session.

Transport address: The combination of a network address and port that identifies a transport-level endpoint, for example an IP address and a UDP port. Packets are transmitted from a source transport address to a destination transport address.

RTP media type: An RTP media type is the collection of payload types which can be carried within a single RTP session. The RTP Profile assigns RTP media types to RTP payload types.

Multimedia session: A set of concurrent RTP sessions among a common group of participants. For example, a videoconference (which is a multimedia session) may contain an audio RTP session and a video RTP session.

RTP session: An association among a set of participants communicating with RTP. A participant may be involved in multiple RTP sessions at the same time. In a multimedia session, each medium is typically carried in a separate RTP session with its own RTCP packets unless the the encoding itself multiplexes multiple media into a single data stream. A participant distinguishes multiple RTP sessions by reception of different sessions using different pairs of destination transport addresses, where a pair of transport addresses comprises one network address plus a pair of ports for RTP and RTCP. All participants in an RTP session may share a common destination transport address pair, as in the case of IP multicast, or the pairs may be different for each participant, as in the case of individual unicast network addresses and port pairs. In the unicast case, a participant may receive from all other participants in the session using the same pair of ports, or may use a distinct pair of ports for each.

The distinguishing feature of an RTP session is that each maintains a full, separate space of SSRC identifiers (defined next). The set of participants included in one RTP session consists of those that can receive an SSRC identifier transmitted by any one of the participants either in RTP as the SSRC or a CSRC (also defined below) or in RTCP. For example, consider a three-party conference implemented using unicast UDP with each participant receiving from the other two on separate port pairs. If each participant sends RTCP feedback about data received from one other participant only back to that participant, then the conference is composed of three separate point-to-point RTP sessions. If each participant provides RTCP feedback about its reception of one other participant to both of the other participants, then the conference is composed of one multi-party RTP session. The latter case simulates the behavior that would occur with IP multicast communication among the three participants.

The RTP framework allows the variations defined here, but a particular control protocol or application design will usually impose constraints on these variations.

Synchronization source (SSRC): The source of a stream of RTP packets, identified by a 32-bit numeric SSRC identifier carried in the RTP header so as not to be dependent upon the network address. All packets from a synchronization source form part of the same timing and sequence number space, so a receiver groups packets by synchronization source for playback. Examples of synchronization sources include the sender of a stream of packets derived from a signal source such as a microphone or a camera, or an RTP mixer (see below). A synchronization source may change its data format, e.g., audio encoding, over time. The SSRC identifier is a randomly chosen value meant to be globally unique within a particular RTP session (see Section 8). A participant need not use the same SSRC identifier for all the RTP sessions in a multimedia session; the binding of the SSRC identifiers is provided through RTCP (see Section 6.5.1). If a participant generates multiple streams in one RTP session, for example from separate video cameras, each MUST be identified as a different SSRC.

Contributing source (CSRC): A source of a stream of RTP packets that has contributed to the combined stream produced by an RTP mixer (see below). The mixer inserts a list of the SSRC identifiers of the sources that contributed to the generation of a particular packet into the RTP header of that packet. This list is called the CSRC list. An example application is audio conferencing where a mixer indicates all the talkers whose speech

was combined to produce the outgoing packet, allowing the receiver to indicate the current talker, even though all the audio packets contain the same SSRC identifier (that of the mixer).

End system: An application that generates the content to be sent in RTP packets and/or consumes the content of received RTP packets. An end system can act as one or more synchronization sources in a particular RTP session, but typically only one.

Mixer: An intermediate system that receives RTP packets from one or more sources, possibly changes the data format, combines the packets in some manner and then forwards a new RTP packet. Since the timing among multiple input sources will not generally be synchronized, the mixer will make timing adjustments among the streams and generate its own timing for the combined stream. Thus, all data packets originating from a mixer will be identified as having the mixer as their synchronization source.

Translator: An intermediate system that forwards RTP packets with their synchronization source identifier intact. Examples of translators include devices that convert encodings without mixing, replicators from multicast to unicast, and application-level filters in firewalls.

Monitor: An application that receives RTCP packets sent by participants in an RTP session, in particular the reception reports, and estimates the current quality of service for distribution monitoring, fault diagnosis and long-term statistics. The monitor function is likely to be built into the application(s) participating in the session, but may also be a separate application that does not otherwise participate and does not send or receive the RTP data packets (since they are on a separate port). These are called third-party monitors. It is also acceptable for a third-party monitor to receive the RTP data packets but not send RTCP packets or otherwise be counted in the session.

Non-RTP means: Protocols and mechanisms that may be needed in addition to RTP to provide a usable service. In particular, for multimedia conferences, a control protocol may distribute multicast addresses and keys for encryption, negotiate the encryption algorithm to be used, and define dynamic mappings between RTP payload type values and the payload formats they represent for formats that do not have a predefined payload type value. Examples of such protocols include the Session Initiation Protocol (SIP) (RFC 3261 [13]), ITU Recommendation H.323 [14] and applications using SDP (RFC 2327 [15]), such as RTSP (RFC 2326 [16]). For simple

applications, electronic mail or a conference database may also be used. The specification of such protocols and mechanisms is outside the scope of this document.

4. Byte Order, Alignment, and Time Format

All integer fields are carried in network byte order, that is, most significant byte (octet) first. This byte order is commonly known as big-endian. The transmission order is described in detail in [3]. Unless otherwise noted, numeric constants are in decimal (base 10).

All header data is aligned to its natural length, i.e., 16-bit fields are aligned on even offsets, 32-bit fields are aligned at offsets divisible by four, etc. Octets designated as padding have the value zero.

Wallclock time (absolute date and time) is represented using the timestamp format of the Network Time Protocol (NTP), which is in seconds relative to 0h UTC on 1 January 1900 [4]. The full resolution NTP timestamp is a 64-bit unsigned fixed-point number with the integer part in the first 32 bits and the fractional part in the last 32 bits. In some fields where a more compact representation is appropriate, only the middle 32 bits are used; that is, the low 16 bits of the integer part and the high 16 bits of the fractional part. The high 16 bits of the integer part must be determined independently.

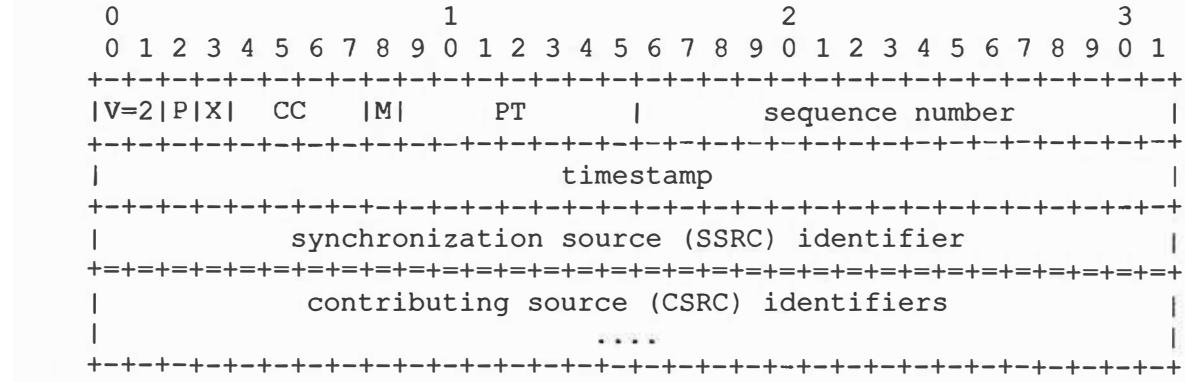
An implementation is not required to run the Network Time Protocol in order to use RTP. Other time sources, or none at all, may be used (see the description of the NTP timestamp field in Section 6.4.1). However, running NTP may be useful for synchronizing streams transmitted from separate hosts.

The NTP timestamp will wrap around to zero some time in the year 2036, but for RTP purposes, only differences between pairs of NTP timestamps are used. So long as the pairs of timestamps can be assumed to be within 68 years of each other, using modular arithmetic for subtractions and comparisons makes the wraparound irrelevant.

5. RTP Data Transfer Protocol

5.1 RTP Fixed Header Fields

The RTP header has the following format:



The first twelve octets are present in every RTP packet, while the list of CSRC identifiers is present only when inserted by a mixer. The fields have the following meaning:

version (V): 2 bits
: This field identifies the version of RTP. The version defined by this specification is two (2). (The value 1 is used by the first draft version of RTP and the value 0 is used by the protocol initially implemented in the "vat" audio tool.)

padding (P): 1 bit
: If the padding bit is set, the packet contains one or more additional padding octets at the end which are not part of the payload. The last octet of the padding contains a count of how many padding octets should be ignored, including itself. Padding may be needed by some encryption algorithms with fixed block sizes or for carrying several RTP packets in a lower-layer protocol data unit.

extension (X): 1 bit
: If the extension bit is set, the fixed header MUST be followed by exactly one header extension, with a format defined in Section 5.3.1.

CSRC count (CC): 4 bits
: The CSRC count contains the number of CSRC identifiers that follow the fixed header.

marker (M): 1 bit
The interpretation of the marker is defined by a profile. It is intended to allow significant events such as frame boundaries to be marked in the packet stream. A profile MAY define additional marker bits or specify that there is no marker bit by changing the number of bits in the payload type field (see Section 5.3).

payload type (PT): 7 bits
This field identifies the format of the RTP payload and determines its interpretation by the application. A profile MAY specify a default static mapping of payload type codes to payload formats. Additional payload type codes MAY be defined dynamically through non-RTP means (see Section 3). A set of default mappings for audio and video is specified in the companion RFC 3551 [1]. An RTP source MAY change the payload type during a session, but this field SHOULD NOT be used for multiplexing separate media streams (see Section 5.2).

A receiver MUST ignore packets with payload types that it does not understand.

sequence number: 16 bits
The sequence number increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence. The initial value of the sequence number SHOULD be random (unpredictable) to make known-plaintext attacks on encryption more difficult, even if the source itself does not encrypt according to the method in Section 9.1, because the packets may flow through a translator that does. Techniques for choosing unpredictable numbers are discussed in [17].

timestamp: 32 bits
The timestamp reflects the sampling instant of the first octet in the RTP data packet. The sampling instant MUST be derived from a clock that increments monotonically and linearly in time to allow synchronization and jitter calculations (see Section 6.4.1). The resolution of the clock MUST be sufficient for the desired synchronization accuracy and for measuring packet arrival jitter (one tick per video frame is typically not sufficient). The clock frequency is dependent on the format of data carried as payload and is specified statically in the profile or payload format specification that defines the format, or MAY be specified dynamically for payload formats defined through non-RTP means. If RTP packets are generated periodically, the nominal sampling instant as determined from the sampling clock is to be used, not a reading of the system clock. As an example, for fixed-rate audio the timestamp clock would likely increment by one for each sampling period. If an audio application reads blocks covering

160 sampling periods from the input device, the timestamp would be increased by 160 for each such block, regardless of whether the block is transmitted in a packet or dropped as silent.

The initial value of the timestamp SHOULD be random, as for the sequence number. Several consecutive RTP packets will have equal timestamps if they are (logically) generated at once, e.g., belong to the same video frame. Consecutive RTP packets MAY contain timestamps that are not monotonic if the data is not transmitted in the order it was sampled, as in the case of MPEG interpolated video frames. (The sequence numbers of the packets as transmitted will still be monotonic.)

RTP timestamps from different media streams may advance at different rates and usually have independent, random offsets. Therefore, although these timestamps are sufficient to reconstruct the timing of a single stream, directly comparing RTP timestamps from different media is not effective for synchronization. Instead, for each medium the RTP timestamp is related to the sampling instant by pairing it with a timestamp from a reference clock (wallclock) that represents the time when the data corresponding to the RTP timestamp was sampled. The reference clock is shared by all media to be synchronized. The timestamp pairs are not transmitted in every data packet, but at a lower rate in RTCP SR packets as described in Section 6.4.

The sampling instant is chosen as the point of reference for the RTP timestamp because it is known to the transmitting endpoint and has a common definition for all media, independent of encoding delays or other processing. The purpose is to allow synchronized presentation of all media sampled at the same time.

Applications transmitting stored data rather than data sampled in real time typically use a virtual presentation timeline derived from wallclock time to determine when the next frame or other unit of each medium in the stored data should be presented. In this case, the RTP timestamp would reflect the presentation time for each unit. That is, the RTP timestamp for each unit would be related to the wallclock time at which the unit becomes current on the virtual presentation timeline. Actual presentation occurs some time later as determined by the receiver.

An example describing live audio narration of prerecorded video illustrates the significance of choosing the sampling instant as the reference point. In this scenario, the video would be presented locally for the narrator to view and would be simultaneously transmitted using RTP. The "sampling instant" of a video frame transmitted in RTP would be established by referencing

its timestamp to the wallclock time when that video frame was presented to the narrator. The sampling instant for the audio RTP packets containing the narrator's speech would be established by referencing the same wallclock time when the audio was sampled. The audio and video may even be transmitted by different hosts if the reference clocks on the two hosts are synchronized by some means such as NTP. A receiver can then synchronize presentation of the audio and video packets by relating their RTP timestamps using the timestamp pairs in RTCP SR packets.

SSRC: 32 bits
The SSRC field identifies the synchronization source. This identifier SHOULD be chosen randomly, with the intent that no two synchronization sources within the same RTP session will have the same SSRC identifier. An example algorithm for generating a random identifier is presented in Appendix A.6. Although the probability of multiple sources choosing the same identifier is low, all RTP implementations must be prepared to detect and resolve collisions. Section 8 describes the probability of collision along with a mechanism for resolving collisions and detecting RTP-level forwarding loops based on the uniqueness of the SSRC identifier. If a source changes its source transport address, it must also choose a new SSRC identifier to avoid being interpreted as a looped source (see Section 8.2).

CSRC list: 0 to 15 items, 32 bits each
The CSRC list identifies the contributing sources for the payload contained in this packet. The number of identifiers is given by the CC field. If there are more than 15 contributing sources, only 15 can be identified. CSRC identifiers are inserted by mixers (see Section 7.1), using the SSRC identifiers of contributing sources. For example, for audio packets the SSRC identifiers of all sources that were mixed together to create a packet are listed, allowing correct talker indication at the receiver.

5.2 Multiplexing RTP Sessions

For efficient protocol processing, the number of multiplexing points should be minimized, as described in the integrated layer processing design principle [10]. In RTP, multiplexing is provided by the destination transport address (network address and port number) which is different for each RTP session. For example, in a teleconference composed of audio and video media encoded separately, each medium SHOULD be carried in a separate RTP session with its own destination transport address.

Separate audio and video streams SHOULD NOT be carried in a single RTP session and demultiplexed based on the payload type or SSRC fields. Interleaving packets with different RTP media types but using the same SSRC would introduce several problems:

1. If, say, two audio streams shared the same RTP session and the same SSRC value, and one were to change encodings and thus acquire a different RTP payload type, there would be no general way of identifying which stream had changed encodings.

2. An SSRC is defined to identify a single timing and sequence number space. Interleaving multiple payload types would require different timing spaces if the media clock rates differ and would require different sequence number spaces to tell which payload type suffered packet loss.

3. The RTCP sender and receiver reports (see Section 6.4) can only describe one timing and sequence number space per SSRC and do not carry a payload type field.

4. An RTP mixer would not be able to combine interleaved streams of incompatible media into one stream.

5. Carrying multiple media in one RTP session precludes: the use of different network paths or network resource allocations if appropriate; reception of a subset of the media if desired, for example just audio if video would exceed the available bandwidth; and receiver implementations that use separate processes for the different media, whereas using separate RTP sessions permits either single- or multiple-process implementations.

Using a different SSRC for each medium but sending them in the same RTP session would avoid the first three problems but not the last two.

On the other hand, multiplexing multiple related sources of the same medium in one RTP session using different SSRC values is the norm for multicast sessions. The problems listed above don't apply: an RTP mixer can combine multiple audio sources, for example, and the same treatment is applicable for all of them. It may also be appropriate to multiplex streams of the same medium using different SSRC values in other scenarios where the last two problems do not apply.

5.3 Profile-Specific Modifications to the RTP Header

The existing RTP data packet header is believed to be complete for the set of functions required in common across all the application classes that RTP might support. However, in keeping with the ALF design principle, the header MAY be tailored through modifications or additions defined in a profile specification while still allowing profile-independent monitoring and recording tools to function.

- The marker bit and payload type field carry profile-specific information, but they are allocated in the fixed header since many applications are expected to need them and might otherwise have to add another 32-bit word just to hold them. The octet containing these fields MAY be redefined by a profile to suit different requirements, for example with more or fewer marker bits. If there are any marker bits, one SHOULD be located in the most significant bit of the octet since profile-independent monitors may be able to observe a correlation between packet loss patterns and the marker bit.

- Additional information that is required for a particular payload format, such as a video encoding, SHOULD be carried in the payload section of the packet. This might be in a header that is always present at the start of the payload section, or might be indicated by a reserved value in the data pattern.

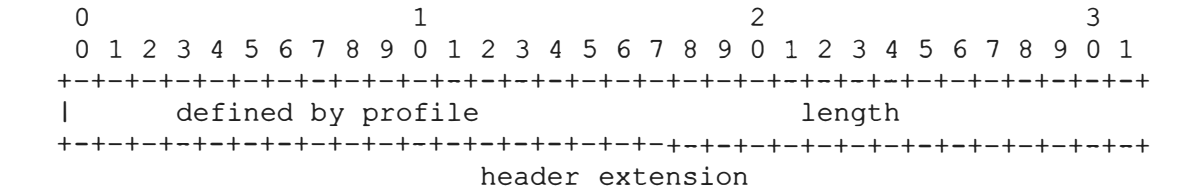
- If a particular class of applications needs additional functionality independent of payload format, the profile under which those applications operate SHOULD define additional fixed fields to follow immediately after the SSRC field of the existing fixed header. Those applications will be able to quickly and directly access the additional fields while profile-independent monitors or recorders can still process the RTP packets by interpreting only the first twelve octets.

If it turns out that additional functionality is needed in common across all profiles, then a new version of RTP should be defined to make a permanent change to the fixed header.

5.3.1 RTP Header Extension

An extension mechanism is provided to allow individual implementations to experiment with new payload-format-independent functions that require additional information to be carried in the RTP data packet header. This mechanism is designed so that the header extension may be ignored by other interoperating implementations that have not been extended.

Note that this header extension is intended only for limited use. Most potential uses of this mechanism would be better done another way, using the methods described in the previous section. For example, a profile-specific extension to the fixed header is less expensive to process because it is not conditional nor in a variable location. Additional information required for a particular payload format SHOULD NOT use this header extension, but SHOULD be carried in the payload section of the packet.



If the X bit in the RTP header is one, a variable-length header extension MUST be appended to the RTP header, following the CSRC list if present. The header extension contains a 16-bit length field that counts the number of 32-bit words in the extension, excluding the four-octet extension header (therefore zero is a valid length). Only a single extension can be appended to the RTP data header. To allow multiple interoperating implementations to each experiment independently with different header extensions, or to allow a particular implementation to experiment with more than one type of header extension, the first 16 bits of the header extension are left open for distinguishing identifiers or parameters. The format of these 16 bits is to be defined by the profile specification under which the implementations are operating. This RTP specification does not define any header extensions itself.

6. RTP Control Protocol -- RTCP

The RTP control protocol (RTCP) is based on the periodic transmission of control packets to all participants in the session, using the same distribution mechanism as the data packets. The underlying protocol MUST provide multiplexing of the data and control packets, for example using separate port numbers with UDP. RTCP performs four functions:

1. The primary function is to provide feedback on the quality of the data distribution. This is an integral part of the RTP's role as a transport protocol and is related to the flow and congestion control functions of other transport protocols (see Section 10 on the requirement for congestion control). The feedback may be directly useful for control of adaptive encodings [18,19], but experiments with IP multicasting have shown that it is also

critical to get feedback from the receivers to diagnose faults in the distribution. Sending reception feedback reports to all participants allows one who is observing problems to evaluate whether those problems are local or global. With a distribution mechanism like IP multicast, it is also possible for an entity such as a network service provider who is not otherwise involved in the session to receive the feedback information and act as a third-party monitor to diagnose network problems. This feedback function is performed by the RTCP sender and receiver reports, described below in Section 6.4.

2. RTCP carries a persistent transport-level identifier for an RTP source called the canonical name or CNAME, Section 6.5.1. Since the SSRC identifier may change if a conflict is discovered or a program is restarted, receivers require the CNAME to keep track of each participant. Receivers may also require the CNAME to associate multiple data streams from a given participant in a set of related RTP sessions, for example to synchronize audio and video. Inter-media synchronization also requires the NTP and RTP timestamps included in RTCP packets by data senders.

3. The first two functions require that all participants send RTCP packets, therefore the rate must be controlled in order for RTP to scale up to a large number of participants. By having each participant send its control packets to all the others, each can independently observe the number of participants. This number is used to calculate the rate at which the packets are sent, as explained in Section 6.2.

4. A fourth, OPTIONAL function is to convey minimal session control information, for example participant identification to be displayed in the user interface. This is most likely to be useful in "loosely controlled" sessions where participants enter and leave without membership control or parameter negotiation. RTCP serves as a convenient channel to reach all the participants, but it is not necessarily expected to support all the control communication requirements of an application. A higher-level session control protocol, which is beyond the scope of this document, may be needed.

Functions 1-3 SHOULD be used in all environments, but particularly in the IP multicast environment. RTP application designers SHOULD avoid mechanisms that can only work in unicast mode and will not scale to larger numbers. Transmission of RTCP MAY be controlled separately for senders and receivers, as described in Section 6.2, for cases such as unidirectional links where feedback from receivers is not possible.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

T.120
(07/96)

SERIE T: EQUIPOS TERMINALES Y PROTOCOLOS
PARA LOS SERVICIOS DE TELEMÁTICA

Protocolo de datos para conferencias multimedia

Recomendación UIT-T T.120

(Anteriormente Recomendación del CCITT)

Recomendación T.120

PROTOCOLO DE DATOS PARA CONFERENCIAS MULTIMEDIA

(Ginebra, 1996)

Alcance

Esta Recomendación introduce una sucesión de normas, colectivamente denominadas serie T.120.

Esta Recomendación describe el modelo de sistema T.120, que proporciona una arquitectura para comunicación de datos multipunto en un entorno de conferencias multimedia. Contiene una introducción y una descripción funcional de las Recomendaciones que van a componer la infraestructura de la serie T.120. Además, hace una sinopsis de otras Recomendaciones de la serie que proporcionan funcionalidad de protocolo de aplicación.

Esta Recomendación define los criterios para la conformidad cuando los protocolos de datos T.120 se utilizan en un entorno de conferencia o de trabajo en grupo.

Esta Recomendación sólo comprende los trabajos concluidos contenidos en Recomendaciones aprobadas. Cuando se aprueben nuevas Recomendaciones, se generará texto de apoyo para su inclusión en esta Recomendación en la siguiente fecha de publicación.

2 Referencias normativas

Las Recomendaciones y demás referencias siguientes contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y demás referencias son objeto de revisiones, por lo que se preconiza que todos los usuarios de la presente Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y demás referencias citadas a continuación. Se publica regularmente una lista de las Recomendaciones UIT-T actualmente vigentes.

Recomendación UIT-T T.121 (1996), *Plantilla de aplicación genérica.*

Recomendación UIT-T T.122 (1993), *Servicio de comunicación multipunto para la definición de los servicios de conferencia audiográfica y de conferencia audiovisual.*

Recomendación UIT-T T.123 (1994), *Pilas de protocolos para aplicaciones de teleconferencias audiográficas y audiovisuales.*

Recomendación UIT-T T.124 (1995), *Control genérico de conferencia.*

Recomendación UIT-T T.125 (1994), *Especificación de protocolo del servicio de comunicación multipunto.*

Recomendación UIT-T T.126 (1995), *Protocolo para imágenes fijas y anotaciones multipunto.*

Recomendación UIT-T T.127 (1995), *Protocolo de transferencia multipunto de ficheros binarios.*

3 Símbolos y abreviaturas

A los efectos de esta Recomendación, se utilizan las abreviaturas siguientes.

ASE Elemento de servicio de aplicación (*application service element*)

ARM Gestor de recursos de aplicación (*application resource manager*)

APE Entidad de protocolo de aplicación (*application protocolo entity*)

GAT Plantilla de aplicación genérica (*generic application template*)

GCC Control de conferencia genérico (*generic conference control*)

LAN Red de área local (*local area network*)

MBFT Transferencia binaria de ficheros multipunto (*multipoint binary file transfer*)

MCS Servicio de comunicación multipunto (*multipoint communication service*)

MCU Unidad de control multipunto (*multipoint control unit*)

MSIA Imagen fija multipunto y anotación (*multipoint still image and annotation*)

PDU Unidad de datos de protocolo (*protocol data unit*)

QOS Calidad de servicio (*quality of service*)

RDCC Red de datos con conmutación de circuitos

RDCP Red digital con conmutación de paquetes

RDSI Red digital de servicios integrados

RDSI-BA Red digital de servicios integrados de banda ancha

RTPC Red telefónica pública conmutada

SI Imagen fija (si se emplea usualmente como abreviatura de MSIA) (*still image*)

4 Sinopsis

Las Recomendaciones de la serie T.120 definen colectivamente un servicio de comunicación multipunto para uso en entornos de conferencias multimedia. El objetivo de esta de Recomendación es proporcionar una introducción y una guía a las Recomendaciones de la serie T.120, que muestren las interrelaciones entre las Recomendaciones constituyentes, y definir los requisitos de conformidad con la Recomendación T.120 para conferencia.

Esta Recomendación proporciona facilidades para establecer y gestionar comunicaciones interactivas (conferencias) en las que intervengan dos o más participantes en una variedad de redes diferentes, o entre éstas. Proporciona un amplio servicio de comunicación de datos para esos participantes, que es independiente de la red subyacente. Dentro de una conferencia permite el establecimiento de comunicaciones entre cualquier combinación de participantes en una conferencia. La serie T.120 también proporciona soporte para aplicaciones y sus protocolos asociados, definiendo mecanismos de arranque y procedimientos de intercambio de capacidades, etc.

La presente Recomendación introduce disposiciones para asegurar la interoperabilidad de la funcionalidad comúnmente requerida, tal como transferencia de ficheros, intercambio de imágenes fijas y pizarras compartidas mediante la definición de protocolos de aplicación normalizados.

Los protocolos T.120 proporcionan un medio de telecomunicar muchas formas de información de datos/telemática entre dos o más terminales multimedia y de gestionar dicha comunicación.

Proporcionan un servicio de comunicación de datos multipunto que tiene una aplicación determinada en conferencias multimedia.

Los protocolos T.120 son adecuados para su uso en muchos tipos de redes: RTPC, RDSI, RDCC, RDCP, RDSI-BA, LAN. Proporcionan la capacidad de un interfuncionamiento sin fisuras de aplicaciones entre terminales conectados a diferentes redes.

Los protocolos T.120 proporcionan:

soporte para el establecimiento de conferencia entre un grupo de nodos de red (como son los terminales de conferencia y las MCU);

mecanismos para identificar los nodos participantes y una lista general y un mecanismo de intercambio de capacidades;

gestión flexible de comunicación entre cualquier combinación de estos elementos.

Los protocolos T.120 pueden manejar una o más conferencias simultáneas. Un terminal puede participar en más de una si está autorizado a hacerlo. El *convocador* de una conferencia puede controlar la participación en la misma y la información que circula por ella.

En una conferencia que admite dirección, el convocador puede delegar parte o la totalidad de la autoridad en el director. Si una conferencia entra en el modo dirigido, los protocolos de aplicación que saben que existe un director modifican su comportamiento, como especifica su protocolo para este modo de operación.

Esta Recomendación impone pocas constricciones específicas a la configuración de las conexiones entre nodos de conferencia (terminales y MCU): pero deben disponerse en una jerarquía, con un nodo único en la cima de un árbol. Los nodos pueden todos conectarse a un punto estrella, o conectarse uno a otros dos de una cadena, o a una cadena de puntos estrella, y así sucesivamente, en la medida en que esté claro, para cada conexión, qué sentido es el ascendente, y que no haya bucles. El nodo superior debe estar presente desde el comienzo de una conferencia, ya que cualquier cambio en la cumbre puede ser disruptivo.

No se impone ninguna constricción a la velocidad o al volumen de información transmitida dentro de los diversos medios; los protocolos T.120 tienen la capacidad de organizar diferentes velocidades de flujo de información, dentro de las constricciones impuestas por el tipo de red y las conexiones establecidas en la misma. Permiten que las aplicaciones establezcan prioridades relativas utilizando los protocolos T.120.

La estructura de los protocolos T.120 se describe en la cláusula 6. No todas las disposiciones de protocolos T.120 son obligatorias: T.123, T.122/125 y T.124 son obligatorias para entornos de conferencia y de trabajo en grupo. El resto son condicionales: cuando se proporciona la funcionalidad tratada por las normas, deben implementarse los protocolos normalizados de la serie T.120 (véanse en la cláusula 9 los requisitos de conformidad T.120). Esto asegura que siempre es posible obtener un nivel básico de interfuncionamiento, y no prohíbe las mejoras personalizadas y la negociación de modos propietarios, únicamente si todos los elementos participantes son capaces de soportar tales modos.

5 Introducción a la comunicación multimedia multipunto

Tradicionalmente los servicios de telefonía han tenido que utilizar el modo de funcionamiento punto a punto. Para las actividades de grupo, tales como reuniones, conferencias, etc., en las que intervienen participantes físicamente separados, es necesario conectar más de dos lugares. El término comunicación multipunto describe simplemente la interconexión de múltiples terminales. Normalmente, para proveer esta función se necesita un elemento de red especial, denominado unidad de control multipunto (MCU), o más simplemente un puente.

Se designa por conferencia un grupo de nodos geográficamente dispersos que se ponen en relación electrónicamente y que pueden intercambiar información audiográfica y audiovisual a través de diversas redes de comunicación.

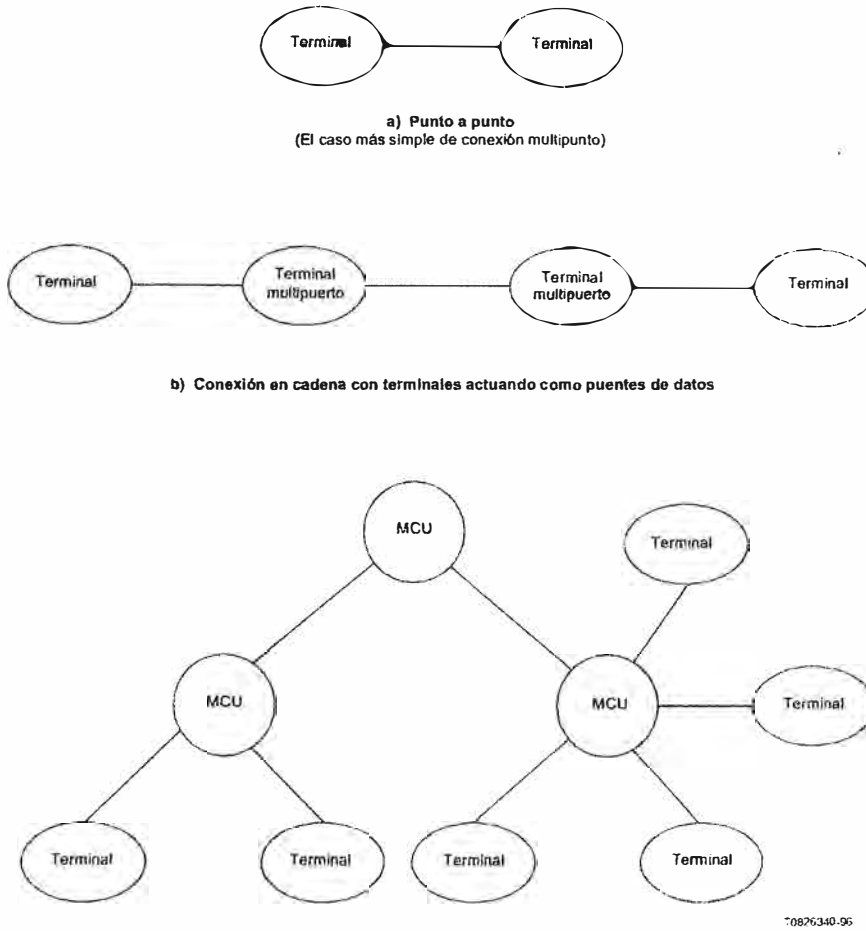
Los participantes en una conferencia pueden tener acceso a capacidades de tratamiento de diversos tipos de medios, tales como audio solamente (telefonía), audio y datos, audio y vídeo, o audio, vídeo y datos.

La serie de Recomendaciones T.120 define el componente que se utiliza para proporcionar un servicio de comunicaciones de datos, y también un servicio de gestión para cualesquiera otros medios presentes.

Los protocolos T.120 proveen la infraestructura necesaria para proporcionar servicios de datos a muchos tipos de conferencias y de trabajo en grupo, haciéndola adecuada para una variada gama de áreas de aplicación. Se espera que encontrarán aplicación en videotelefonía y en la conferencia audiográfica, así como en otras formas de comunicación multimedia multipunto.

Esta Recomendación considera las conexiones punto a punto como la forma más simple (un caso degenerado) de una conexión multipunto. Ambas formas de conexión son soportadas por los protocolos T.120. Los terminales con múltiples puertos de comunicación (cada uno con una pila de transporte T.120 apropiada) pueden actuar como puentes de datos T.120 y permitir que se establezcan conexiones multipunto en las que intervengan tres o más nodos. La Figura 1 b) muestra una conferencia en la que intervienen cuatro lugares con terminales multipuerto que actúan como puentes de datos.

Las MCU son nodos que, normalmente, no soportan la funcionalidad de terminal. Actúan como nodos de interconexión, uniendo trenes de datos y de otros medios, presentes en las conexiones. La Figura 1 c) muestra un ejemplo de cómo pueden conectarse tres MCU para servir de puente a un grupo de terminales.



a) Punto a punto
(El caso más simple de conexión multipunto)

b) Conexión en cadena con terminales actuando como puentes de datos

c) Topología multipunto
3 MCU proporcionan conexiones para permitir a multiples terminales participar en una conferencia

FIGURA 1/T.120

Ejemplos de configuraciones de conferencia multipunto que muestran diversas topologías de conexión y diversos tipos de nodos

La Figura 2 es un ejemplo de conferencia en la que intervienen terminales de capacidades diversas, pertenecientes a múltiples redes diferentes, y a través de distintas administraciones.

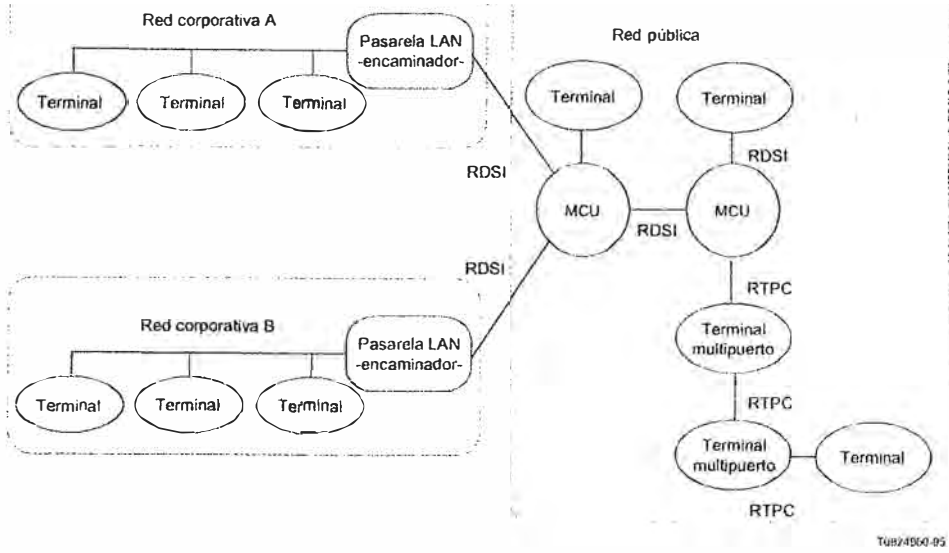


FIGURA 2/T.120

Ejemplo de topología de conferencia de red mixta

6 El modelo de sistema T.120

El modelo T.120 está compuesto por una infraestructura de comunicaciones y los protocolos de aplicación que hacen uso de la misma. La Figura 3 muestra el modelo completo con aplicaciones normalizadas y no normalizadas. El modelo sirve para mostrar el alcance de la serie T.120 de Recomendaciones (se indica con fondo sombreado) y la relación entre cada una de las Recomendaciones y otros componentes del sistema.

Generalmente, cada capa proporciona servicios a la capa superior y comunica a su par (o pares) enviando unidades de datos de protocolo (PDU, *protocol data units*) a través de servicios proporcionados por la capa inferior.

En esta cláusula se tratará cada uno de los niveles funcionales de la Figura 3: aplicaciones de usuario, protocolos de aplicación, controladores de nodos, infraestructura de comunicaciones y redes.

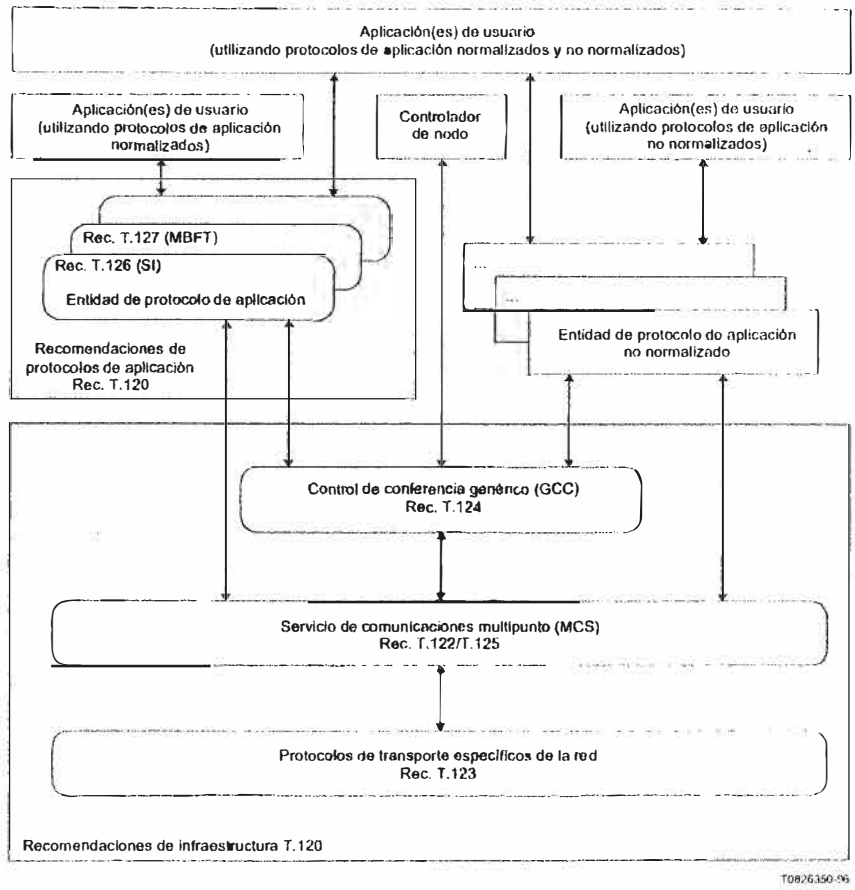


FIGURA 3/T.120

Modelo de sistema T.120

6.1 Aplicaciones de usuario

Las aplicaciones *per se* no son objeto de normalización en la serie T.120. Las aplicaciones que utilizan los servicios ofrecidos por la serie T.120 serán en general conscientes del modo multipunto, y estarán diseñadas para utilizar los servicios T.120 proporcionados por el GCC y el MCS. Estas aplicaciones se denominan aplicaciones de usuario y pueden utilizar cualquier combinación de protocolos normalizados y no normalizados para comunicar con aplicaciones de usuario pares. El entorno T.120 soporta múltiples aplicaciones de usuario que funcionan concurrentemente en la misma conferencia proporcionando mecanismos para que las aplicaciones coordinen el uso de los recursos de comunicaciones. La plantilla de aplicación genérica (Recomendación T.121) proporciona orientación a los desarrolladores de aplicaciones de usuario sobre el modo de utilizar la infraestructura T.120 de una manera coherente y consecuente. Una aplicación de usuario trata las tareas que no producen un efecto directo en el interfuncionamiento (por ejemplo, una interfaz de

ANEXO I
Tabla de Acrónimos

ACELP: Algebraic Code Excited Linear Prediction

ACR: Absolute Category Rating

ADPCM: Adaptative Differential Pulse Code Modulation

ALT: Autonomous Line Terminating Unit

ANI: Automatic Identification Number

ANS: Access Node Switch

ANSI: American National Standards Institute

ARPA: Advanced Research Program Agency

ARPANET: Advanced Research Program Agency Network

ARQ: Admission Request

ASCII: American Standard Code Information Interchange

BNC: Bayonet Neill-Concelman

CAS: Channel Associated Signalling

CBR: Constrained Based Routing

CCSS7: Common Channel Signalling System 7

CDC: Centros de Comunicaciones

CDR: Call Detail Report

CS-ACELP: Conjugate Structure Algebraic Code Excited Linear Prediction

CSB: Circuit Switch Block

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

CTU: Clock and Tone Unit

DMZ: Demilitarized Zones

DNS: Domain Name System

DoS: Denial of Service

DRQ: Disengage Request

DSU: Data Service Unit

DTMF: Dual-Tone Multifrequency

EBCDIC: Extended Binary Coded Decimal Interchange Code

ENUM: Telephone Number Mapping

ERL: Echo Return Lost

ETSI: European Telecommunications Standards Institute

FDM: Frequency Division Multiplexing

FEC: Forwarding Equivalent Class

FTP: File Transfer Protocol

FWSM: Firewall Security System

GIF: Graphics Interchange Format

GLBP: Gateway Load Balancing Protocol

HSRP: Hot Stand By Router Protocol

HSSI: High Speed Serial Interface

HTTP: Hypertext Transfer Protocol

ICANN: Internet Corporation for Assigned Names and Numbers

IEEE: Institute of Electrical and Electronics Engineers

IETF: Internet Engineering Task Force

IHL: Internet Header Length

IMS: IP Multimedia Subsystem

IMX: IP Multimedia Exchange

IP: Internet Protocol

IPCC: International Packet Communications Consortium

IPv4: Internet Protocol version 4

IPv6: Internet Protocol version 6

ISC: International Softswitch Consortium

ISDN: Integrated Services Digital Network

ISDN-PRI: ISDN-Primary Rate Interface

ISO: International Standards Organization

ISP Internet Service Provider

ITU: International Telecommunication Union

ITU-T: ITU- Telecommunication Standardization Sector

IVR: Interactive Voice Response

JPEG: Joint Photographics Experts Group

LAN: Local Area Network

LDI: Larga Distancia Internacional

LDN: Larga Distancia Nacional

LRQ: Location Request

LSP: Label Switched Path

LSR: Label Switched Router

MAC: Media Access Control

MCU: Multipoint Control Unit

MDF: Main Distribution Frame

MOS: Mean Option SCore

MPEG: Moving Pictures Experts Group

MPLS: Multi Protocol Label Switching

MP-MLQ: Multipulse Maximun Likelihood Quantization

MSX: Multiprotocol Session Exchange

NAT: Network Address Translation

NGN: Next Generation Networks

NIC: Network Interface Card

OSI: Open System Interconnection

PABX: Private Automatic Branch Exchange

PAMS: Perceptual Analysis Measurement System

PAT: Port Address Translation

PCM: Pulse Code Modulation

PDH: Plesiochronous Digital Hierarchy

PDV: Post Delay Variance

PESQ: Perceptual Evaluation of Speech Quality

PHB: Per Hop Behavior

PRI: Primary Rate Interface

PSB: Packet Switch Block

PSQM: Perceptual Speech Quality Measurement

PSTN: Public Switched Telephone Network

PSU: Power Supply Unit

QoS: Quality of Service

QoV: Quality of Voice

RADIUS: Remote Authentication Dial In User Service

RAS: Registration Admission Status

RFC: Request for Comments

RRQ: Registration Request

RSM: Real time Session Management

RSVP: Resource Reservation Protocol

RTCP: Real Time Control Protocol

RTP: Real Time Protocol

SBC: Session Border Controller

SCP: Service Control Point

SCP: Session Control Protocol

SDH: Synchronous Digital Hierarchy

SDP: Session Description Protocol

SHU: System Handling Unit

SIP: Session Initiation Protocol

SL: Signalling Links

SLA: Service Level Agreements

SMTP: Simple Mail Transfer Protocol

SP: Signalling Point

SSP: Service Switching Point

STM: Synchronous Transport Module

STP: Signal Transfer Point

TCP: Transmission Control Protocol

TDM: Time Division Multiplexing

TDMS: Synchronous Time Division Multiplexing

ToS: Type of Service

TTL: Time to Live

UA: User Agent

UAC: User Agent Client

UAS: User Agent Server

UDP: User Datagram Protocol

UMG: Universal Media Gateway

URQ: Unregister Request

VAD: Voice Activity Detection

VAU: Voice Announcement Unit

VLAN: Virtual Local Area Network

VoD: Video on Demand

VoIP: Voice over Internet Protocol

VPN: Virtual Private Network

WAN: Wide Area Network

ZIP: Zone Information Protocol

BIBLIOGRAFIA

[1]. Franklin D. Ohrtman, "SOFTSWITCH Architecture for VoIP", The McGraw Hill Companies, 2004

[2]. Ing. Percy Fernandez Pilco, "TELECOMUNICAIONES IV", Universidad Nacional de Ingeniería, 2012

[3]. TECSUP LIMA, "Voz y Telefonia IP", Programa de Capacitación Continua, 2010

[4]. Andrew S. Tanenbaum, "Redes de Computadoras", Pearson Educación cuarta edición, 2003

[5]. Huawei Training Center, "SOFTX3000 Operation and Maintenance Training", Training Program, 2012

[6]. José Manuel Huidobro, "Tecnología VoIP y Telefonía IP", España, 2006

[7]. Md. Arifnoor Chowdhury, "Softswitch Design and Performance Analysis", LAP Lambert Acad. Publ., 2010

[8]. James F. Durkin, "Voice-Enabling the Data Network", Cisco Press, 2003

[9]. Matthew Stafford, "Signaling And Switching For Packet Telephony", Artech House, 2004

[10]. Daniel Collins, "Carrier Grade Voice Over Ip", McGraw-Hill Education, 2005

[11]. Huawei Technologies Proprietary, "Performance Measurement Manual U-SYS UMG8900 Universal Media Gateway", www.huawei.com, 2012

[12]. Huawei Technologies Proprietary, "U-SYS SoftX3000 SoftSwitch System Operation Manual", www.huawei.com, 2012