UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SEÑALIZACION PARA VOZ IP

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRONICO

PRESENTADO POR:

LUIS GUILLERMO MUÑOZ MORALES

PROMOCIÓN
2002 - II

LIMA – PERÚ
2006

SEÑALIZACION PARA VOZ IP

SUMARIO

El presente trabajo pretende determinar la Importancia de la Señalización para voz IP de los diferentes tipos de protocolos de señalización que utiliza para transmitir voz como paquetes sobre una red con protocolo IP. Por lo que Voz IP se puede lograr en cualquier red de datos que use IP.

En el capitulo I explica como el protocolo H.323 es usado para la señalización, inicialización y término de las llamadas, así como también cargar la información requerida para localizar a los usuarios.

En el capitulo II se refiere al Protocolo de Inicio de la Sesión; Es un protocolo de control de aplicaciones de capas para crear, modificar y terminar sesiones con uno o más usuarios de Voz IP

En el capitulo III se explica dos Protocolos de Control de gateway del Grupo IETF que se utilizan para controlar los gateways de Voz sobre IP desde elementos externos de control de llamadas: el Protocolo simple de control de gateway (SGCP) y el Protocolo de control de gateway de medios (MGCP).

También explica otra especificación de dispositivo de control que tiene un impacto significativo en la industria de la telefonía de paquetes.

El capitulo IV se centra en el controlador de switch virtual (VSC) , que es un componente arquitectónico básico del switch virtual basado en la redes de voz actuales que se están moviendo desde una infraestructura de múltiplexión por división de tiempo (TDM) a una nueva infraestructura de servicios de voz basada en paquetes.

INDICE

CAPITULO I

H.323

CAPITULO II

PROTOCOLO DE INICIO DE LA SESION

CAPITULO III

PROTOCOLO DE CONTROL DE GATEWAY

PROLOGO

El presente trabajo tiene como propósito posibilitar las redes de datos para efectuar llamadas telefónicas y determinar la importancia de la señalización de voz IP logrando así información sobre la señalización de transmisión de la voz sobre ip la cual se demostrará que utiliza los protocolos de señalización que es la parte importante ya que de ella dependerá la eficacia, la complejidad de la comunicación y las ventajas que ofrece al utilizar estos protocolos de señalización. El método de trabajo que se utiliza es de nivel explorativo y de tipo informativo.

Este trabajo ha sido desarrollado en Lima-Perú, en la Universidad Nacional de Ingeniería, en el area de Ingeniería Eléctrica y Electrónica en la especialidad Ingeniería Electrónica en el Programa de Titulación Profesional por Actualización de Conocimientos, entre las limitaciones que podemos mencionar son las siguientes:
Dificultad para recoger la información y la falta de tiempo, para lograr una mayor profundización del tema.

Bajo el titulo de Señalización para voz IP, presentamos este trabajo de investigación que consta de cuatro capítulos, H.323, Protocolo de inicio de la sesión, Protocolos de control de gateway y Controlador de switch virtual incluyendo las conclusiones. Todos estos han sido desarrollados de manera sencilla para su mejor comprensión.

CAPITULO I
H.323

1.1. Introducción

Hace ya varios años se descubrió que la transmisión de señales en modo digital era mucho más sencillo y rápido: Antes de mandarlo se tenía que digitalizar con un ADC, después transmitirlo, y al final transformarlo con un DAC para poder usarlo. Así fue como surgió la idea de la comunicación de voz sobre el Internet en vez de la PSTN, que se volvió una realidad en Febrero de 1995 cuando Volcaltec, Inc. quiso profundizar esta idea de unir la red de datos con la de voz y transmitirla por el protocolo de Internet y para esto introdujo su software. Diseñado para PC 486 a 33 MHz o mayores, equipadas con tarjeta de sonido, bocinas, micrófono y MODEM. El funcionamiento del software se basa en la compresión de la señal de voz, traduciéndola a paquetes IP para la transmisión por Internet. Poco tiempo después la tecnología de la convergencia de redes empezó a avanzar. Varios de los desarrolladores de software, ofrecen ahora, el software de telefonía, pero, algo más importante son los gateways (compuertas) que están emergiendo para actuar como una interfaz entre el Internet y la PSTN. Equipadas con tarjetas de procesamiento de voz, estos servidores facilitan a los usuarios la comunicación vía los teléfonos convencionales.

Todas las llamadas que se hacen por la PSTN se van al gateway Server ("servidor de la compuerta"), el cual digitaliza la señal de voz análoga, la comprime en paquetes de IP, y la manda por el Internet para transportarlo a una gateway que la recibe. Con esto soporta las llamadas de computadora-teléfono, teléfono-computadora y teléfono-teléfono ya que representan un paso significativo en la convergencia de las redes de voz y datos.

Es importante tener en cuenta también que todas las redes deben tener de alguna forma las características de direccionamiento, enrutamiento y señalización. El direccionamiento es requerido para identificar el origen y destino de las llamadas, también es usado para

asociar clases de servicio a cada una de las llamadas dependiendo de la prioridad. El enrutamiento por su parte encuentra el mejor camino a seguir por el paquete desde la fuente hasta el destino y transporta la información a través de la red de la manera más eficiente, la cual ha sido determinada por el diseñador. La señalización alerta las estaciones terminales y a los elementos de la red; su estado y la responsabilidad inmediata tienen al establecer una conexión en el cual utiliza como soporte cualquier medio basado en routers y los protocolos de transporte UDP/IP.

Existen varios organismos involucrados en los Standard para la señalización: el ITU-T (que dio lugar a la suite de protocolos H.323, por ejemplo); el ETSI (con el proyecto Tiphon) y el IETF (que administra los protocolos de Internet, SIP por ejemplo).

Los protocolos de señalización son de diversos tipos. El ITU-T H.323 es aplicado para acciones dentro de una Intranet. Fundamentalmente es una cobertura para una suite de protocolos como el H.225,H.245 y RAS que se soportan en TCP y UDP. El IETF define otros tipos de protocolos: el MGCP para el control de las gateway a la red publica PSTN y SIP hacia las redes privadas o publicas. La señal vocal se transmite sobre el protocolo de tiempo real RTP (con el control RTPC) y con transporte sobre UDP.

El protocolo de reservación de ancho de banda RSVP puede ser de utilidad en conexiones unidireccionales (distribución de señal de broadcasting, por ejemplo).
En la actualidad la voz y video se están convirtiendo en herramientas clave para la comunicación entre personas. Entre las motivaciones principales tenemos la reducción de costo, convergencia, mayores servicios y distribución de inteligencia sobre la red.

1.2. Concepto

H.323 es una especificación de la ITU-T para transmitir audio, vídeo y datos a través de una red de Protocolo Internet (IP), incluida la propia Internet. Cuando son compatibles con H.323, los productos y aplicaciones de los fabricantes pueden comunicarse e ínter operar unos con otros. El H.323 estándar dirige la señalización y control de llamadas, transporte y control multimedia y control de ancho de banda para conferencias punto a punto y multipunto. La serie H de las recomendaciones también especifica H.320 para la Red

Digital de Servicios Integrados (RDSI) .y H.324 para el Servicio telefónico analógico convencional (POTS, Plain Old Telephone Service) como mecanismos de transporte.
El H.323 estándar consta de los siguientes componentes y protocolos:

Función	**Protocolo**
Señalización de llamadas	H.225
Control de medios	H.245
Códecs de audio	G.711, G.722, G.723, G.728, G.729
Códecs de vídeo	H.261, H.263
Compartir datos	T.120
Transporte de medios	RTP/RTCP

El sistema H.323 se explica en las tres siguientes secciones:

- Elementos H.323.
- Conjunto del protocolo H.323.
- Flujos de llamadas H.323.

1.3. Elementos h.323

La figura 1.1 nos muestra los elementos de un sistema H.323. Estos elementos incluyen terminales, gateways, gatekeepers y unidades de control multipunto (MCU, Multipoint Control Units).
Los terminales, a los que a menudo se hace referencia como puntos finales, proporcionan conferencias punto a punto y multipunto para audio y, de manera opcional, vídeo y datos. Los gateways interconectan con la Red pública de telefonía conmutada (PSTN) o la red ISDN (RDSI) para interworking el punto final de H.323. Los gatekeepers proporcionan el control de admisión y servicios de traducción de direcciones para terminales o gateways. Las MCU son dispositivos que permiten que dos o más terminales o gateways realicen conferencias con sesiones de audio y/o vídeo.

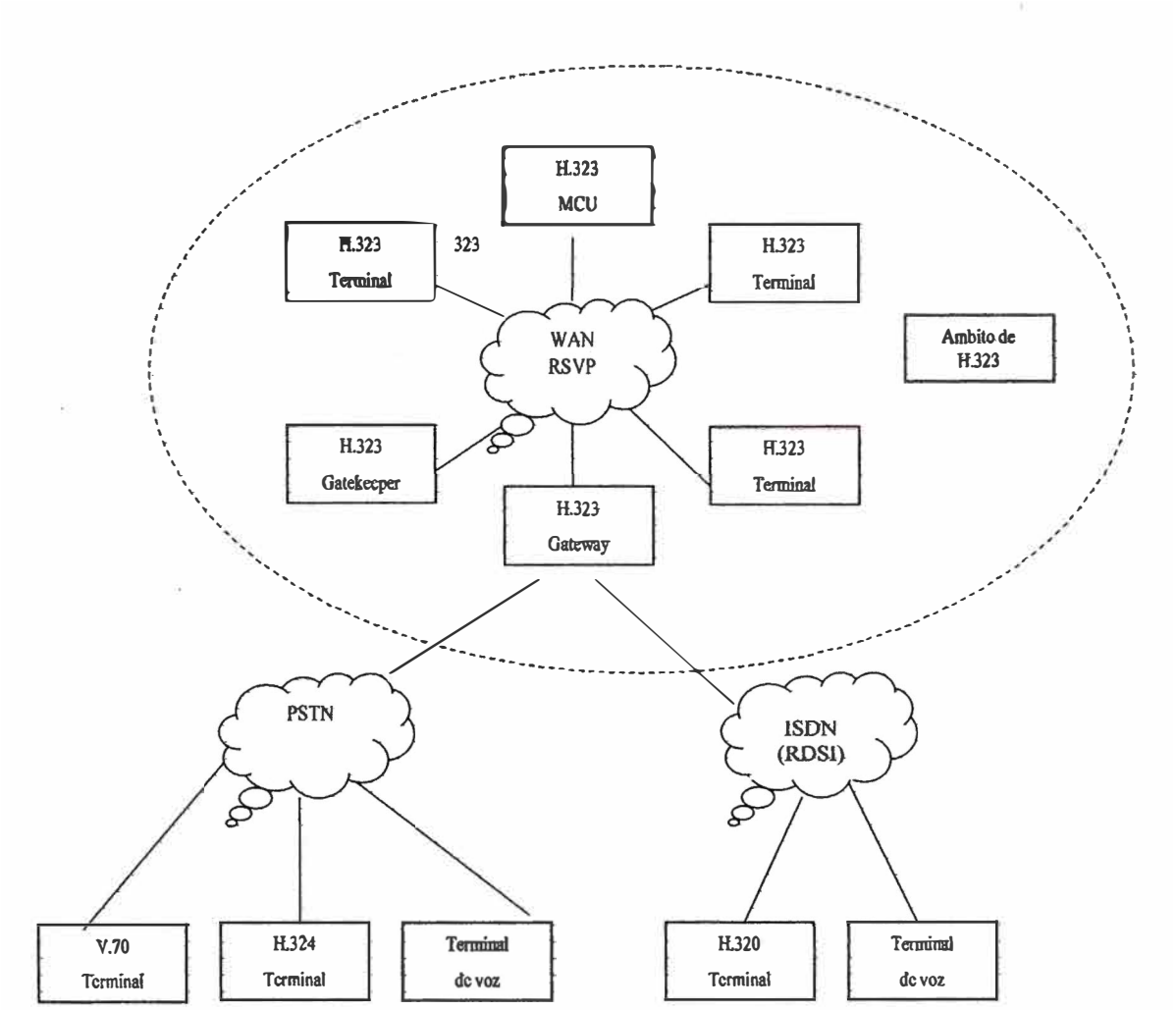

Figura 1.1 Elementos de Networkimg H.323

1.3.1. Terminal

La figura 1.2 nos ilustra el elemento de red que está definido en H.323 como un terminal. Los terminales H.323 deben tener una unidad de control de sistema, una transmisión de medios, códec de audio e interfaz de red basada en paquetes. Los requisitos opcionales incluyen un códec de vídeo y aplicaciones de datos de usuario. Las siguientes funciones y posibilidades se encuentran dentro del ámbito del terminal H.323:

- Unidad de control de sistema. Proporciona a H.225 y H.245 el control de llamadas, intercambio de capacidad, mensajería y señalización de comandos para una actividad apropiada del terminal.

➢ Transmisión de medios. Formatea el audio, vídeo, datos, flujos de control y mensajes transmitidos en la interfaz de red. La transmisión de medios recibe también el audio, vídeo datos, flujos de control y mensajes desde la interfaz de red.

➢ Códec de audio. Codifica la señal desde el equipo de audio para su transmisión y descodifica el código de audio entrante. Las funciones que se requieren incluyen la codificación y descodificación de voz G.711.

➢ De manera opcional, se pueden soportar la codificación y descodificación G.722, G.723.1, G.728 y G.729.

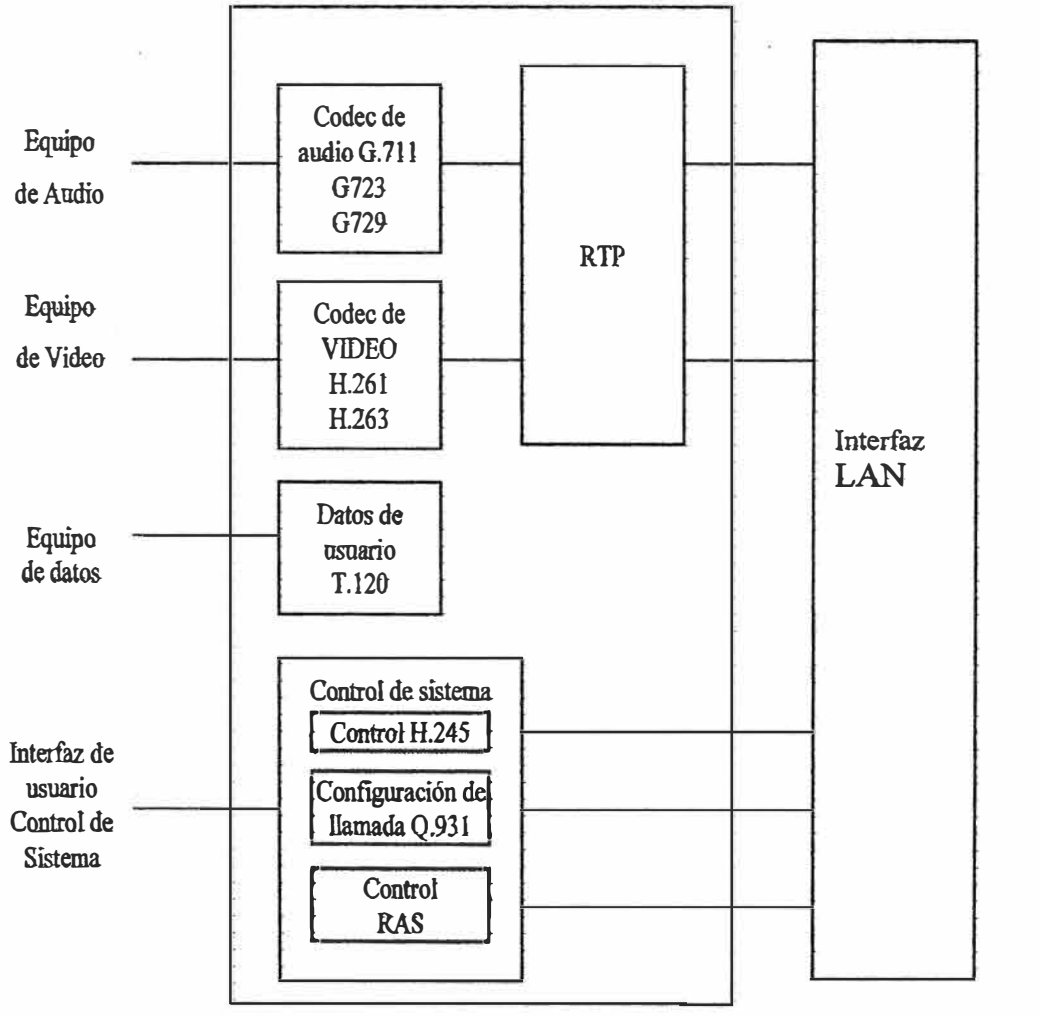

Figura 1.2 Relaciones entre los componentes de H.323

➢ Interfaz de red. Una interfaz basada en paquetes que puede hacer servicios de unidifusión y multidifusión de extremo a extremo de Protocolo para el control de la transmisión (TCP) y el Protocolo de datagrama de usuario (UDP).

➢ Códec de vídeo. Es opcional, pero si está proporcionado, debe ser capaz de codificar y descodificar vídeo de acuerdo con el Quarter Comment Intermediate Format (QCIF) H.261.

➢ Canal de datos. Soporta aplicaciones como acceso a base de datos, transferencia de archivos y conferencias audiográficas (la posibilidad de modificar una imagen común sobre múltiples computadoras de usuarios de forma simultánea).

1.3.2. Gateway

El gateway H.323 refleja las características de un punto final de una red de circuito conmutado (SCN) y un punto final H.323. Traduce entre formatos de audio, vídeo y transmisión de datos, así como en sistemas de comunicación y protocolos. Esto incluye la configuración y el borrado de la llamada en la red IP y en la red SCN. Los gateways no son necesarios a menos que se requiera la interconexión con la SCN. Por tanto, los puntos finales H.323 pueden comunicar directamente sobre la red de paquetes sin conectar con un gateway. El gateway actúa como un terminal H.323 o MCU en la red y un terminal SCN o MCU en la SCN, como muestra en la figura 1.3

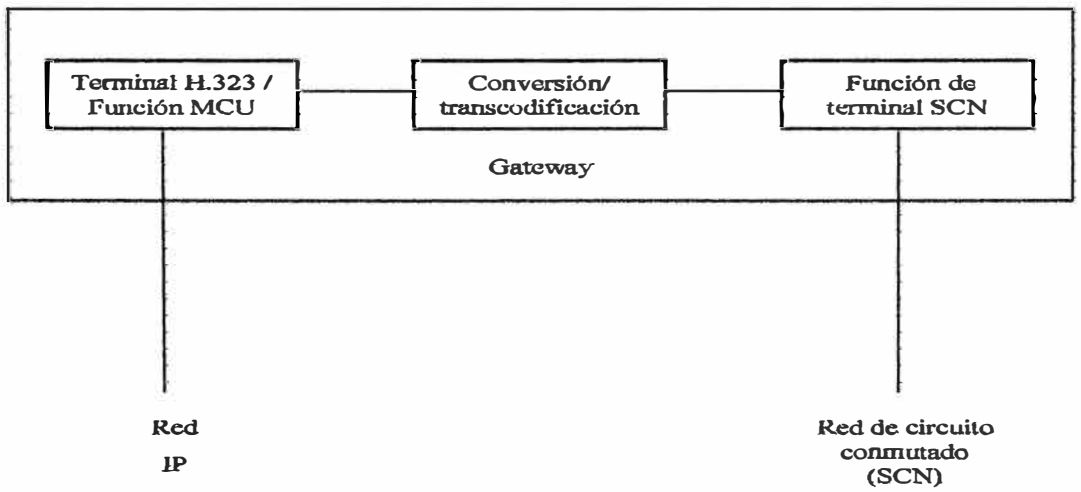

Figura 1.3 Elementos de un Gateway H.323

1.3.3. Gatekeeper

El gatekeeper es una función opcional que proporciona servicios de control de prellamada y nivel de llamada a los puntos finales H.323. Los gatekeepers están lógicamente separados de los demás elementos de la red en los entornos H.323. Si se implementa más de un gatekeeper, se lleva a cabo la intercomunicación de una manera no especificada.
Las nuevas versiones de H.323, como la versión 3, que estaba previsto estuvieran finalizadas a finales de 1999, intentan recomendar una especificación de intercomunicación de gatekeeper. El gatekeeper puede utilizar una simple secuencia consulta/ respuesta (Location Request [LRQ] o Location Confirmation [LCF]) para localizar a los usuarios remotos. Otro protocolo, el Open Settlements Protocol (OSP), también especificado como el Instituto europeo de normas de telecomunicación TS 101 321 (ETSI, European Telecommunication Standards Institute), se utiliza mucho para interacciones entre dominios tanto desde el gateway como desde el gatekeeper.
Si un gatekeeper está presente en un sistema H.323, debe llevar a cabo lo siguiente:

- Conversión de direcciones. Proporciona direcciones IP de punto final desde los alias H.323 (como pcl @cisco.com) o direcciones E164 (números de teléfono normales).

- Control de admisiones. Proporciona acceso autorizado a H.323 utilizando los mensajes Admission Request/Admission Confirm/Admission Reject (ARQ/ACF/ARJ) , que se explican en la sección "Señalización RAS" de este mismo capítulo.

- Control de ancho de banda. Consiste en la administración de los requisitos de ancho de banda utilizando los mensajes Bandwidth Request/Bandwidth Confirm/Bandwidth Reiect (BRQ/BCF/BRJ) , que se explican en la sección "Señalización RAS" de este capítulo.

- Administración de zona. Para los terminales, gateways y MCU registrados; se explica en la sección "Señalización RAS" de este capítulo.

Opcionalmente, el gatekeeper puede aportar la siguiente funcionalidad:

➢ Señalización de control de llamadas. Utiliza el modelo Señalización de llamadas de gatekeeper enrutado (GKRCS, Gatekeeper Routed Call Signaling) , que se verá en la sección "Señalización de control de llamadas (H.225)" de este capítulo.

➢ Autorización de llamada. Permite que el gatekeeper restrinja el acceso a determinados terminales y gateways o restrinja el acceso sobre la base de normas de la hora del día.

➢ Administración de ancho de banda-Permite que el gatekeeper rechace la admisión si el ancho de banda requerido no está disponible.

➢ Administración de llamada. Los servicios incluyen el mantenimiento de una lista de llamadas activas que se puede utilizar para indicar que un punto final está ocupado.

1.3.4. La mcu y los elementos

El controlador multipunto (MC) soporta conferencias entre tres o más puntos finales en una conferencia multipunto. Los MC transmiten el conjunto de capacidades para cada punto final en la conferencia multipunto y pueden revisar las capacidades durante la conferencia. La función MC puede residir en un terminal, gateway, gatekeeper o MCU.

El procesador multipunto (MP) recibe audio, vídeo y/o flujos de datos y los distribuye a los puntos finales que participan en una conferencia multipunto (multiconferencia) y La MCU es un punto final que soporta conferencias multipunto y, por lo menos, consta de un MC y uno o más MP. Si soporta conferencias multipunto centralizadas, la MCU típica consta de un MC, un MP de audio, vídeo y datos.

1.3.5. Servidor proxy h.323

Un servidor proxy H.323 es un proxy específicamente diseñado para el protocolo H.323. El proxy actúa en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los proxies pueden determinar el destino de una llamada y realizar la conexión si se desea. El proxy soporta las siguientes funciones clave:

- Los terminales que no soportan el Protocolo de reserva de recursos (RSVP, Resource Reservatíon Protocol) se pueden conectar a través de un acceso o redes de área local (LAN) con una calidad de servicio (QoS) relativamente buena con el proxy. Los pares de proxies pueden entonces negociar una QoS adecuada para tunelar a través de la red IP. Los proxies pueden administrar la QoS con RSVP y/o bits de precedencia IP.

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

- Un proxy es compatible con la conversión de dirección de red, permitiendo que los nodos H.323 sean desplegados en las redes con un espacio de dirección privado.

- Un proxy desplegado sin un firewall o independientemente de un firewall proporciona seguridad, por lo que únicamente el tráfico H.323 pasa por el mismo. Un proxy desplegado junto con un firewall permite que el firewall sea configurado para pasar todo el tráfico H.323 tratando al proxy como si fuera un nodo de confianza. Esto permite que el firewall proporcione la seguridad del networking de datos y que el proxy proporcione la seguridad H.323.

1.4. Conjunto del protocolo h.323

El conjunto del protocolo H.323 está basado en varios protocolos, como muestra la Figura 1.4. La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos de medios y los mensajes en los sistemas H.323. Estos protocolos son soportados por mecanismos de entrega de paquetes seguros y poco seguros sobre las redes de datos.

A pesar de que la mayoría de las implementaciones H.323 utilizan actualmente el protocolo TCP como el mecanismo de transporte para la señalización, la versión 2 de H.323 admite un transporte UDP básico. Asimismo, otras corporaciones estándar están investigando la utilización de mecanismos UDP seguros para crear métodos de señalización más escalables.

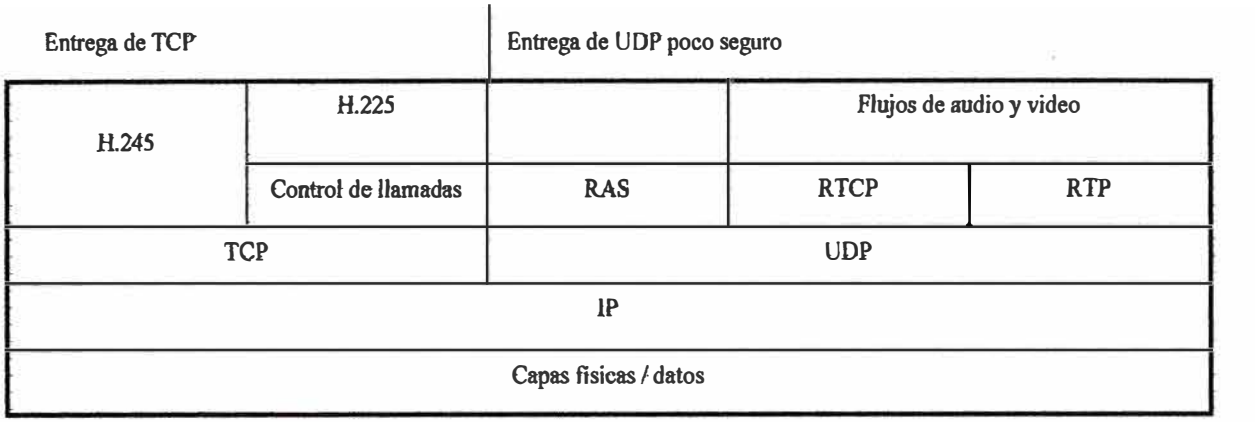

Figura 1.4 Capas del conjunto de Protocolo H.323

El conjunto del protocolo H.323 está dividido en tres áreas de control principales:

- Señalización de registro, admisiones y estado (RAS). Proporciona un control de pre-llamadas en las redes basadas en gatekeeper H.323.

- Señalización de control de llamadas. Se utiliza para conectar, mantener y desconectar llamadas entre puntos finales.

- Control y transporte de medios. Proporciona el canal H.245 seguro que transporta los mensajes de control de los medios. El transporte ocurre con un flujo UDP no seguro. El resto de esta sección se centra en estas tres funciones clave de señalización.

1.4.1. Señalización ras

La señalización RAS proporciona un control de prellamadas en las redes H.323 donde existen gatekeepers y una zona. El canal RAS se establece entre puntos finales y gatekeepers a través de una red IP. El canal RAS está abierto. antes de que ningún otro canal sea establecido, y es independiente de la señalización de control de llamadas y de los canales de transporte de medios. Esta conexión UDP no segura transporta los mensajes RAS que realizan el registro, las admisiones, los cambios del ancho de banda, el estado y los procedimientos de desenganche

a. Descubrimiento del gatekeeper

El descubrimiento de gatekeeper es un proceso manual o automático que los puntos finales utilizan para identificar con qué gatekeeper registrarse. En el método manual, los puntos finales están configurados con la dirección IP del gatekeeper y, por tanto, puede intentar el registro inmediatamente, pero únicamente con el gatekeeper predefinido. El método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como autodescubrimiento (auto discovery).

El autodescubrimiento permite que un punto final, que tal vez no conozca a su gatekeeper, pueda descubrirlo a través de un mensaje de multidifusión. Como los puntos finales no tienen por qué estar estáticamente configurados o reconfigurados para los gatekeepers, este método tiene menos cargas administrativas. La dirección de difusión del descubrimiento de gatekeeper es 224.0.1.41, el puerto de descubrimiento UDP del gatekeeper es 1718, y el puerto de estado y registro UDP del gatekeeper es 1719. Se utilizan estos tres mensajes RAS para el autodescubrimiento del gatekeeper H.323:

- Gatekeeper Request (GRQ). Mensaje de multidifusión enviado por un punto final que está buscando al gatekeeper.

- Gatekeeper Confirm (GCF). Respuesta a un GRQ de punto final que indica la dirección de transporte del canal RAS del gatekeeper.

- Gatekeeper Reject (GRJ). Avisa al punto final de que el gatekeeper no quiere aceptar su registro. Normalmente se debe a una configuración en el gateway o gatekeeper.

En la figura 1.5 siguiente observaremos los procesos de mensajes y secuencias para el autodescubrimiento.

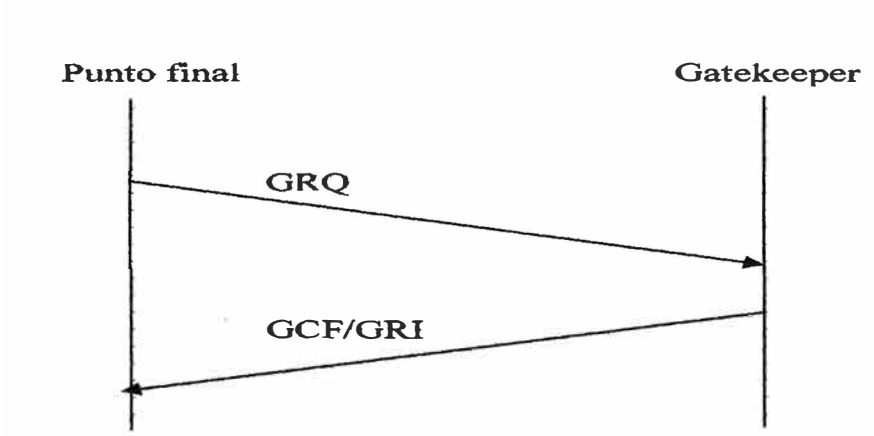

Figura 1 .5 Autodescubrimiento de Gatekeeper

Para propósitos de redundancia, el gatekeeper puede identificar gatekeepers alternativos en los mensajes GCF. Se pueden utilizar estos gatekeepers alternativos cuando falla el gatekeeper principal.

b. Registro

El registro es el proceso que permite que los gateways, puntos finales y MCU alcancen una zona e informen al gatekeeper de sus direcciones IP y alias. El registro, que es un proceso necesario, ocurre después del proceso de descubrimiento, pero antes de que se intente realizar ninguna llamada. Se pueden utilizar los seis mensajes siguientes para permitir que un punto final registre y cancele registros:

- Registration Request (RRQ). Enviado desde un punto final a la dirección del canal RAS del gatekeeper.

- Registration Confirm (RCF). Enviado por el gatekeeper, confirma un registro de punto final.

- Registration Reject (RRJ). Enviado por el gatekeeper, rechaza un registro de punto final.

- Unregister Request (URQ). Enviado desde un punto final o gatekeeper para cancelar un registro.

- Unregister confirm (UCF). Enviado desde el punto final o gatekeeper para confirmar la cancelación de un registro.

- Unregister Reject (U RJ). Indica que el punto final no estaba preregistrado con el gatekeeper.

c. Localización de punto final

En la figura 1.6 observamos los puntos finales y gatekeepers que utilizan la localización de punto final para obtener información de contacto cuando sólo está disponible la información de alias. Los mensajes locate (localizar) son enviados a la dirección del canal RAS del gatekeeper o son multidifundidos a la dirección de difusión de descubrimiento del gatekeeper. El gatekeeper responsable del punto final solicitado responde indicando su propia información de contacto o la del punto final.
El punto final o gatekeeper puede incluir una o más direcciones E164 fuera de la zona en la petición. Se pueden utilizar los siguientes tres mensajes para localizar puntos finales:

- LRQ. Se envía para solicitar información de contacto del punto final o gatekeeper para una o más direcciones E164.

- LCF. Se envía por el gatekeeper y contiene el canal de señalización de llamadas o dirección del canal RAS de sí mismo o del punto final solicitado. Utiliza su propia dirección cuando se utiliza GKRCS y la dirección del punto final solicitado cuando se utiliza la Señalización de llamada directa de punto final (Direct Endpoint Call Signaling).

- Location Reject (LRJ). Se envía por los gatekeepers que reciben un LRQ para el que no está registrado el punto final solicitado o tiene recursos no disponible

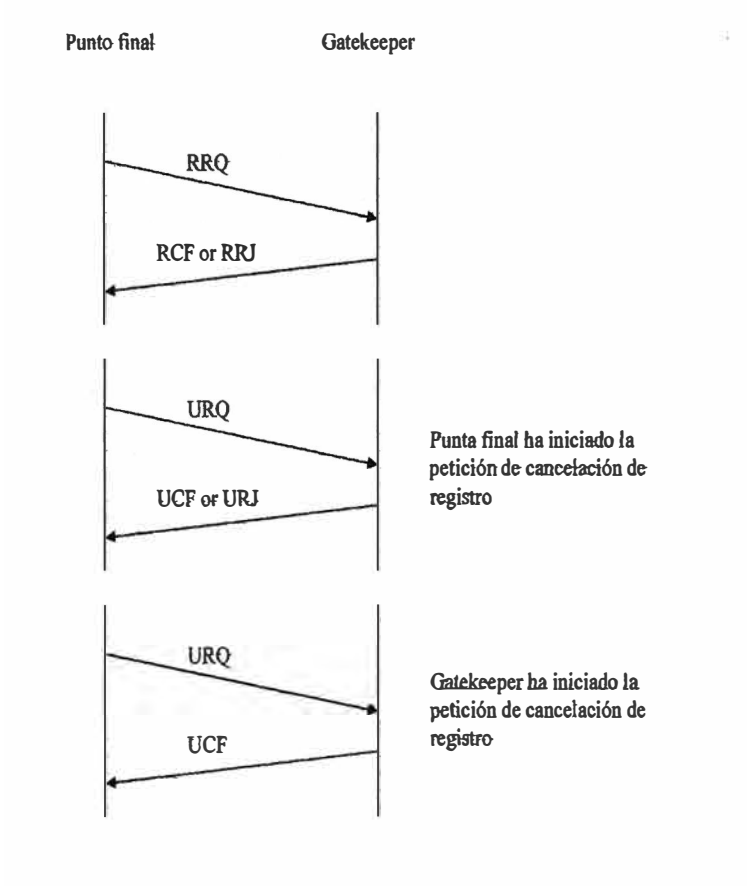

Figura 1.6 Registro de Punto final y cancelación de registro de punto final y gatekeeper

d. Admisiones

Los mensajes de admisión entre puntos finales y gatekeepers proporcionan las bases para la admisión de llamadas y control de ancho de banda. Los gatekeepers autorizan el acceso a las redes H.323 confirmando o rechazando una petición de admisión. Una petición de admisión incluye el ancho de banda solicitado, que puede ser reducida por el gatekeeper en la confirmación. Los siguientes mensajes proporcionan control de admisión en las redes H.323:

- ARQ. Un intento realizado por un punto final para iniciar una llamada.

- ACF. Una autorización dada por el gatekeeper para admitir la llamada

- ARJ. Deniega la petición del punto final de tener acceso a la red para esta llamada determinada.

El mensaje ACF contiene la dirección IP del gateway o gatekeeper de terminación y permite que el gateway de origen inicie inmediatamente los procedimientos de señalización de control de llamadas.

e. Información de estado

El gatekeeper puede utilizar el canal RAS para obtener información de estado desde un punto final. Podemos utilizar este mensaje para monitorizar si el punto final está en línea (online) o no (offline) debido a una condición de fallo. El período típico de sondeo para los mensajes de estado es de 10 segundos. Durante la ACF, el gatekeeper puede también solicitar que el punto final envíe mensajes de estado periódicos durante una llamada. Podemos utilizar los tres mensajes siguientes para proporcionar el estado en el canal RAS:

- Information Request (IRQ). Se envía desde el gatekeeper al punto final que solicita el estado

- Information Request Response (IRR) . Se envía desde el punto final al gatekeeper en respuesta a una petición de información IRQ. Este mensaje es también enviado desde un punto final si el gatekeeper solicita actualizaciones periódicas del estado.

- Status Enquiry. Se envía fuera del canal RAS en el canal de señalización de llamadas. Un punto final o gatekeeper puede enviar mensajes Status Enquiry a otro punto final para verificar el estado de la llamada. Los gatekeepers suelen utilizar estos mensajes para verificar si las llamadas siguen activas.

f. Control de ancho de banda

El control de ancho de banda se administra inicialmente a través del intercambio de admisiones entre un punto final y el gatekeeper en una secuencia ARQ/ACF/ARJ. Sin embargo, el ancho de banda puede cambiar durante una llamada. Podemos utilizar los siguientes mensajes para cambiar el ancho de banda:

- BRQ. Es enviado por un punto final al gatekeeper pidiendo un incremento o disminución en el ancho de banda de la llamada.

- BCF. Es enviado por el gatekeeper para confirmar la aceptación de la petición de cambio de ancho de banda.

- BRJ. Es enviado por el gatekeeper para rechazar la petición de cambio de ancho de banda (enviada si el ancho de banda solicitado no está disponible).

1.4.2. Señalización de control de llamadas (h.225)

En las redes H.323, los procedimientos de control de llamadas se basan en la recomendación H.225 de la ITU-T, que especifica la utilización y soporte de los mensajes de señalización Q.931. Un canal de control de llamadas seguro se crea en una red IP en el puerto 1720 del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre dos puntos finales para el propósito de conectar, mantener y desconectar las llamadas. El control de llamadas real y los mensajes de actividad se mueven a puertos efímeros después de configurar la llamada inicial. Pero 1720 es el puerto que se conoce para las llamadas H.323. H.225 también especifica la utilización de los mensajes Q.932 para servicios suplementarios. Los siguientes mensajes Q.931 y Q.932 son los mensajes de señalización más utilizados en las redes H.323:

- Setup. Un mensaje hacia delante enviado por la entidad H.323 que llama en un intento de establecer conexión con la entidad H.323 llamada. Este mensaje se envía en el puerto TCP 1720 de H.225.

- Call Proceeding. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad que llama para avisar que los procedimientos de establecimiento de llamada se han iniciado.

- Alerting. Un mensaje hacia atrás enviado desde la entidad llamada para avisar a la parte llamada que el sonido de llamada se ha iniciado.

- Connect. Un mensaje hacia atrás enviado desde la entidad llamada a la entidad llamante indicando que la parte llamada ha respondido a la llamada. El mensaje de conexión puede contener la dirección de transporte UDP/IP para la señalización de control H.245.

➢ Release Complete. Enviado por el punto final que inicia la desconexión, que indica que la llamada ha sido liberada. Se puede enviar este mensaje únicamente si el canal de señalización de la llamada está abierto o activo.

➢ Facility. Un mensaje Q.932 utilizado para solicitar o confirmar servicios suplementarios. También se utiliza para indicar si una llamada debe ser dirigida o debe ir a través de un gatekeeper.

En la figura 1.7 nos muestra los mensajes de señalización para la configuración de la llamada. La interacción con el gatekeeper se limita a los mensajes RAS para los mensajes de estado de permiso y posibilidad de llamada.

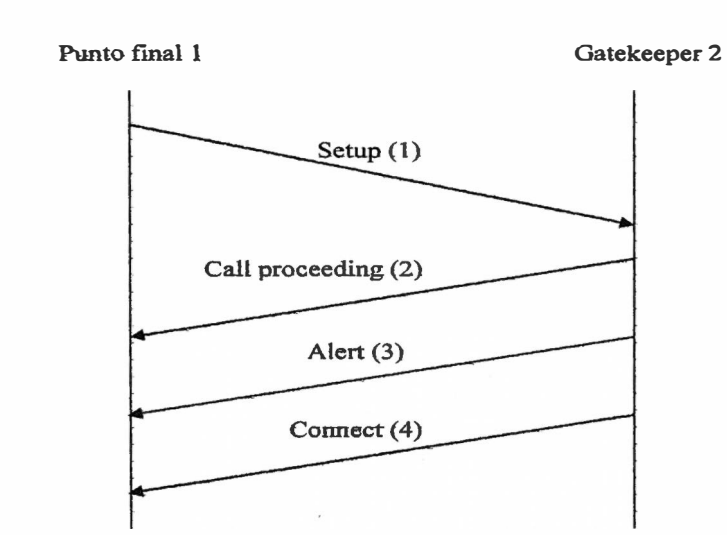

Figura 1.7 Mensajes de señalización de configuración de llamada

Se puede enrutar el canal de señalización de la llamada en una red H.323 de dos maneras: a través de Señalización de llamada directa de punto final (Direct Endpoint Call Signaling) y de Señalización de llamada de gatekeeper enrutado (GKRCS, Gatekeeper Routed Call Signaling). En el método de Señalización de llamada directa de punto final, los mensajes de señalización se envían directamente entre los dos puntos finales, como muestra en la figura 1.8

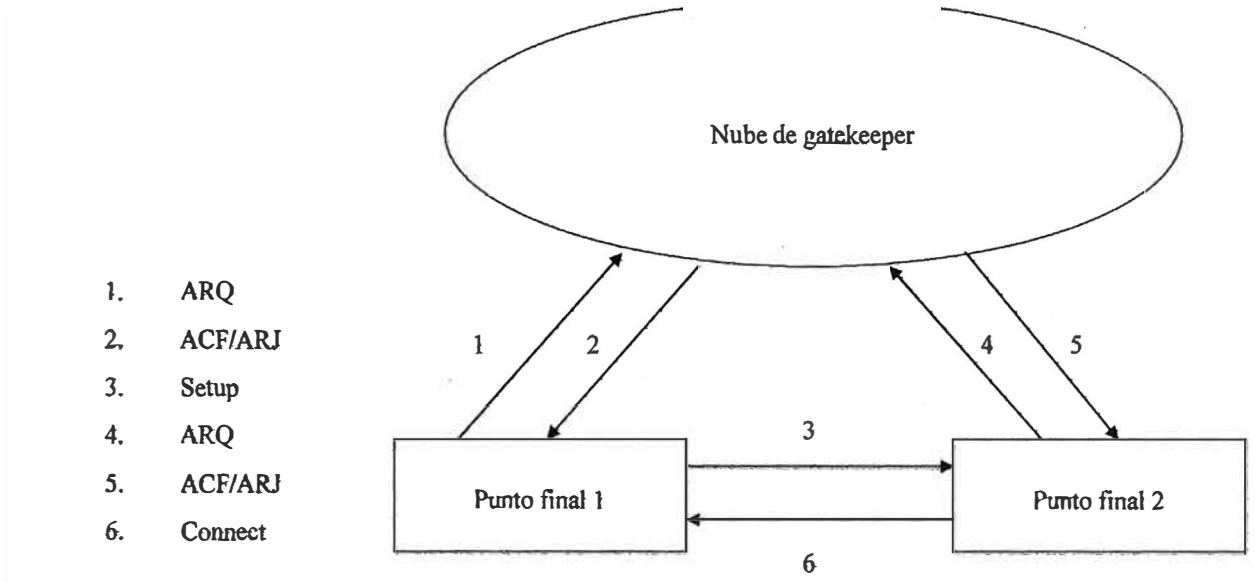

Figura 1.8. Señalización de llamada directa de punto final

En el método GKRCS, los mensajes de señalización de las llamadas entre los puntos finales son enrutados a través del gatekeeper como muestra en la figura 1.9.

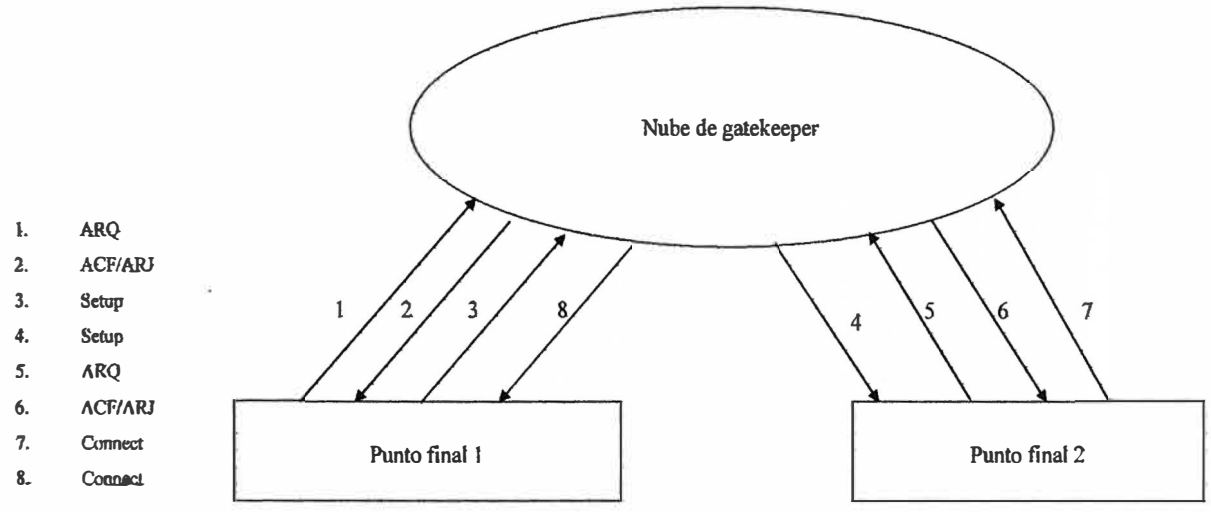

Figura 1.9 Señalización de llamada gatekeeper enrutado

Se pueden ofrecer servicios suplementarios a través del método GKRCS si el canal de señalización de la llamada permanece abierto durante la misma. Los gatekeepers también pueden cerrar el canal de señalización de la llamada después de que se haya completado su configuración.

1.4.3. Control y transporte de medios (h.245 y rtp/rtcp) h.245

Maneja mensajes de control de extremo a extremo entre entidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, vídeo, datos y canal de control. Un punto final establece un canal H.245 para cada llamada con el punto final que está participando. El canal de control seguro se crea sobre IP utilizando el puerto TCP dinámicamente asignado en el último mensaje de señalización de llamada. El intercambio de capacidades, la apertura y cierre de canales lógicos, los modos de preferencia y el control de los mensajes ocurren sobre este canal de control. H.245 también permite intercambio de capacidades separadas para la transmisión y recepción, así como la negociación de las funciones, como determinar qué códec se debe utilizar. Si utilizamos la señalización de llamadas de gatekeeper enrutado, podemos controlar el enrutamiento del canal de dos maneras: utilizar Direct H.245 Control, que tiene lugar directamente entre dos puntos finales participantes, o bien utilizar Gatekeeper Routed H.245 Control, que tiene lugar entre cada punto final y su gatekeeper. Podemos hacer uso de los siguientes procedimientos y mensajes para permitir la operación de control H.245: Capability Exchange. Consiste en mensajes que intercambian de manera segura las capacidades entre dos puntos finales, también llamados terminales. Estos mensajes indican capacidades del terminal para transmitir y recibir audio, vídeo y datos al terminal que está participando. Para audio, el intercambio de capacidades incluye códecs de transcodificación de voz de la serie G, como G.729 a 8 kbps, G.728 a 16 kbps, G.711 a 64 kbps, G.723 a 5,3 ó 6,3 kbps, o G.722 a 48, 56 y 64 kbps. También incluye las velocidades de muestreo de las series de la International Organization for Standardization (ISO) IS.111723 con 32, 44,1 y 48 kHz, e IS.13818-3 con 16, 22,05, 24, 32, 44,1, y 48 kHz; así como los códecs de audio de voz de tasa completa, tasa media y tasa mejorada de GSM.

➢ Master-Slave Termination. Procedimientos utilizados para determinar qué punto final es el principal (maestro) y qué punto final es el secundario (esclavo) para una llamada determinada. La relación se mantiene durante la duración de la llamada y se utiliza para resolver conflictos entre puntos finales. Las reglas maestro-esclavo (master-slave) se utilizan cuando ambos puntos finales solicitan acciones similares a la vez.

➢ Round-Trin Delay. (Retraso de ida y vuelta.) Procedimientos utilizados para determinar el retraso entre los puntos finales de origen y de terminación. El mensaje Round Trip Delay Request mide el retraso y verifica si la entidad remota del protocolo H.245 está activa.

➢ Logical Channel Signaling. Abre y cierra el canal lógico que transporta la información de audio, vídeo y datos. El canal se prepara antes de la transmisión real para asegurar que los terminales están preparados y son capaces de recibir y descodificar información. Los mismos mensajes de señalización establecen los canales unidireccionales y bidireccionales. Cuando se ha establecido la señalización de canal lógico con éxito, el puerto UDP para el canal de medios RTP es pasado desde el punto de final de terminación hasta el punto final de origen. Asimismo, cuando se utiliza el modelo Gatekeeper Call Routed, es en este punto donde el gatekeeper puede desviar los flujos RTP proporcionando la dirección UDP/IP real del punto final de terminación.

a. Procedimientos de conexión rápida

Los dos procedimientos disponibles para establecer canales de medios entre puntos finales son H.245 y Fast Connect. Fast Connect permite que se establezca la conexión de medios para llamadas básicas punto a punto con un mensaje de intercambio de ida y vuelta. Estos procedimientos dictan que el punto final llamante incluye el elemento faststart (inicio rápido) en el mensaje de configuración inicial. La parte faststart consiste en secuencias de canal lógico, capacidades de canal de medios y los parámetros necesarios para abrir e iniciar la transmisión de medios. En respuesta, el punto final llamado devuelve un mensaje H.225 (call proceeding, progress, alerting o connect) que contiene un elemento faststart que selecciona las capacidades de terminal aceptadas. En ese momento, tanto los puntos finales llamantes como los llamados pueden transmitir medios si la secuencia de configuración basada en H.225 ha alcanzado el estado conectado.

a.1. Tunneling h.245

Se puede encapsular o "tunelar" mensajes H.245 dentro del canal de señalización de llamadas H.225 en lugar de crear un canal de control H.245 separado. Este método mejora el tiempo de conexión de llamada y la asignación de recursos, y proporciona una sincronización entre la señalización y el control de llamadas. Se pueden encapsular múltiples mensajes H.245 en un mensaje H.225. Asimismo, en cualquier momento un punto final puede conmutar con una conexión H.245 separada.

a.2. Terminación de llamada

Cualquier punto final que participe en una llamada puede iniciar el procedimiento de terminación de llamada. En primer lugar, deben cesar las transmisiones de medios (como audio, vídeo o datos) y cerrarse todos los canales lógicos. A continuación, debe finalizar la sesión H.245 y enviarse un mensaje de liberación completa (release complete message) en el canal de señalización de llamada, si sigue estando abierto o activo. En ese momento, si ningún gatekeeper está presente, se termina la llamada. Cuando un gatekeeper está presente, se utilizan los siguientes mensajes en el canal RAS para completar la terminación de llamada:

- Disengage Request (DRQ). Se envía por un punto final o gatekeeper para terminar una llamada.

- Disengage Confirm (DCF). Se envía por un punto final o gatekeeper para confirmar la desconexión de la llamada.

- Disengage Reject (DRJ). Se envía por el punto final o gatekeeper para rechazar la desconexión de la llamada.

a.3. Transporte de medios (rtp/rtcp)

RTP proporciona transporte de medios en H.323. De manera más específica, RTP permite la entrega de extremo a extremo en tiempo real de audio, vídeo y datos interactivos sobre redes de unidifusión o multidifusión. Los servicios de empaquetamiento y transmisión incluyen la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización.RTP depende de otros mecanismos y de las capas bajas para asegurar la

entrega a tiempo, la reserva de recursos, la fiabilidad y la QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios. El canal de medios se crea utilizando UDP, donde los flujos RTP actúan en un número de puerto par y el flujo RTCP correspondiente actúan en el siguiente número de puerto más alto (impar).

1.5. Flujos de llamada h.323

Los flujos de llamadas descritos en esta sección muestran cómo la familia de protocolos H.323 proporciona una configuración de llamada entre dos puntos finales. Imaginemos que son llamadas de voz y que todos los puntos finales han completado el registro con el gatekeeper apropiado. Los ejemplos de configuración de llamada incluyen dos implementaciones de gatekeeper diferentes, así como dos métodos de señalización de llamada diferentes. Los ejemplos muestran, de forma detallada, los procedimientos de configuración de llamada para las implementaciones de un único gatekeeper. La figura 1.10 y 1.11 nos ilustra los flujos de llamada que utilizan la señalización directa de punto final entre dos puntos finales que comparten el gatekeeper.

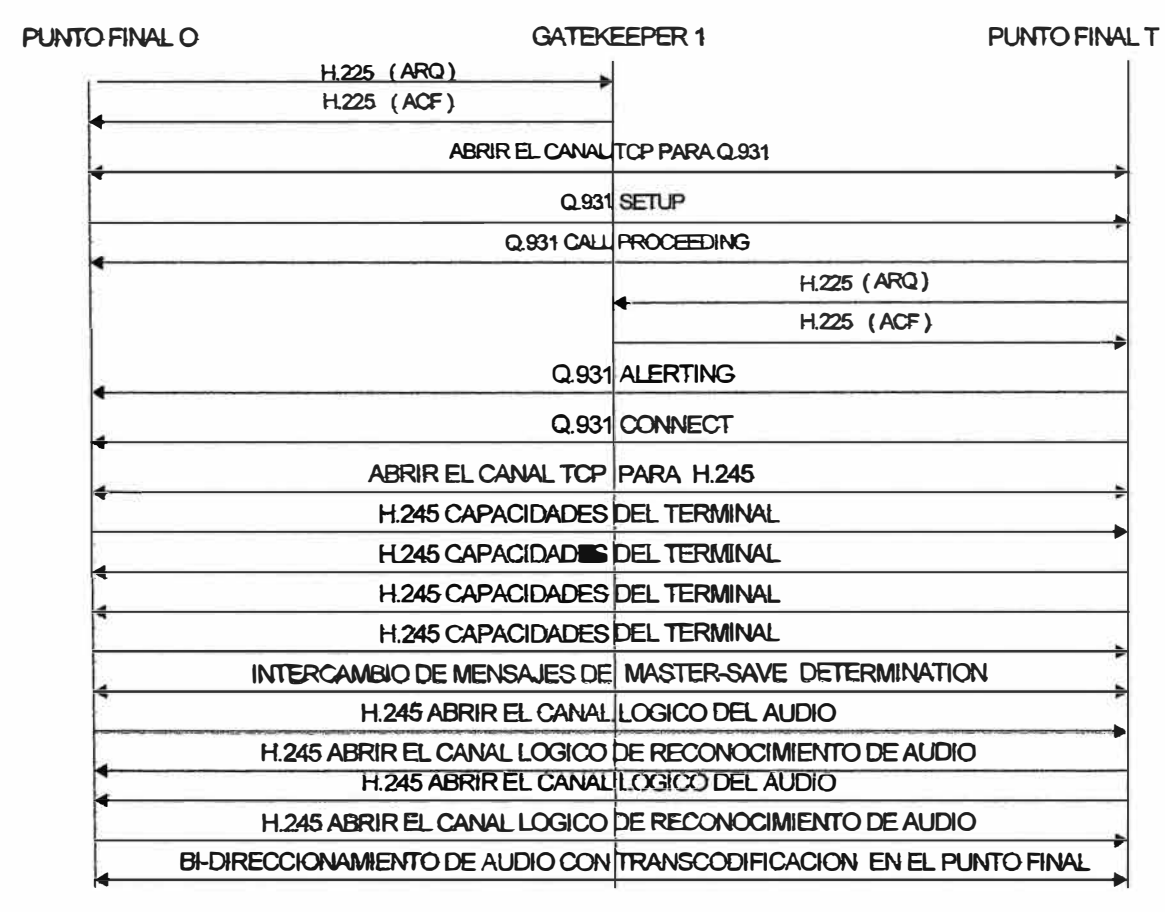

Figura 1.10: Señalización directa de punto final. Mismo gatekeeper

La figura 1.11 nos muestra los flujos de llamada que utilizan la señalizacion de llamada de gatekeeper enrutado entre dos puntos finales que compaten el gatekeeper.

Se debe tener en cuenta que el procedimiento H.245 esta manejado directamente entre los puntos finales y esta enrutado por el gatekeeper

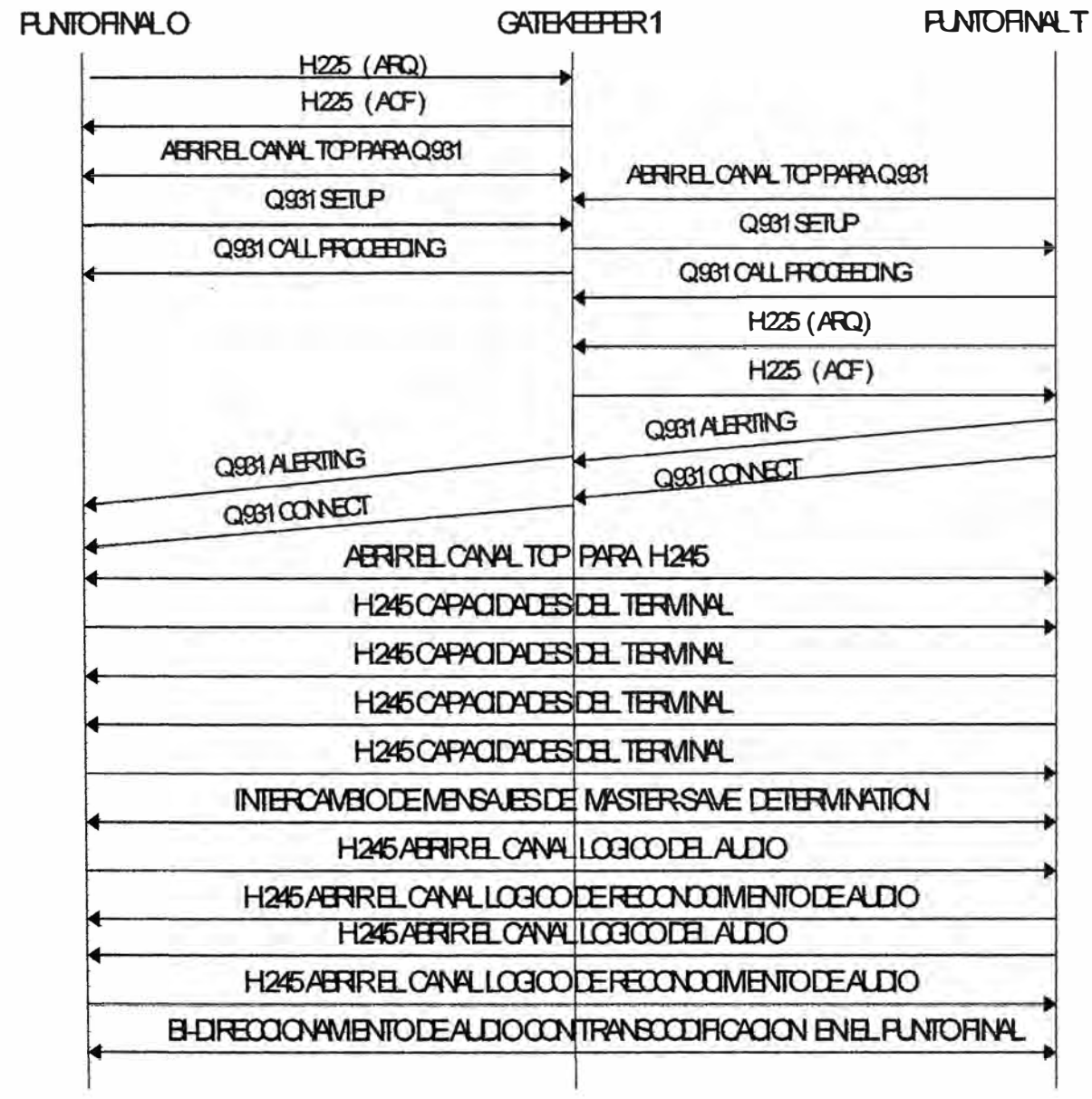

Figura 1.11. Señalización de llamada de gatekeeper erutado. Mismo gatekeeper

Los ejemplos de las siguientes figuras detallan los procedimientos de llamada para implementaciones de gatekeeper doble. De manera especifica, la figura 1.12 nos ilustra los flujos de llamada utilizando una señalización de punto final directa entre dos puntos finales que tienen diferentes gatekeepers. La principal diferencia entre la GKRCS y la señalización de llamada directa es que en el primer caso el caso de configuración es diseccionado hacia el gatekeeper y en la señalización de llamada directa es diseccionado hacia el punto final de terminación

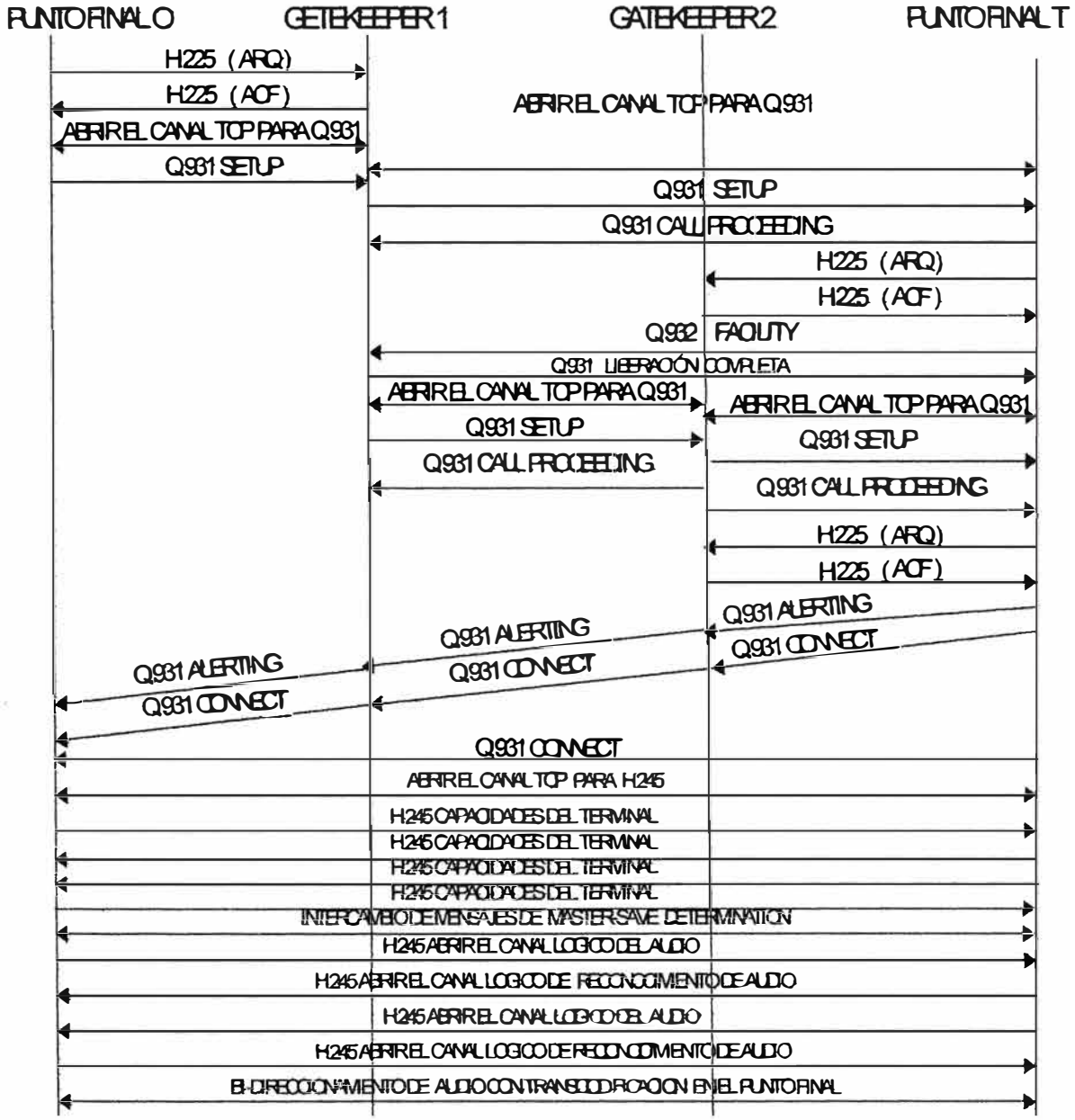

Figura 1.12. Señalización directa de punto final. Dos gatekeepers

En la figura 1.13 nos muestra los procedimientos de configuración de llamada para el método GKRCS, donde cada punto final tiene un gatekeeper diferente. Esto permite que se puedan enviar LRQ y LCF entre los dos gatekeepers, lo que a su vez permite el control de los registros de facturación en el gatekeeper, ya que todas las configuraciones y mensajes de control pasan a través del mismo

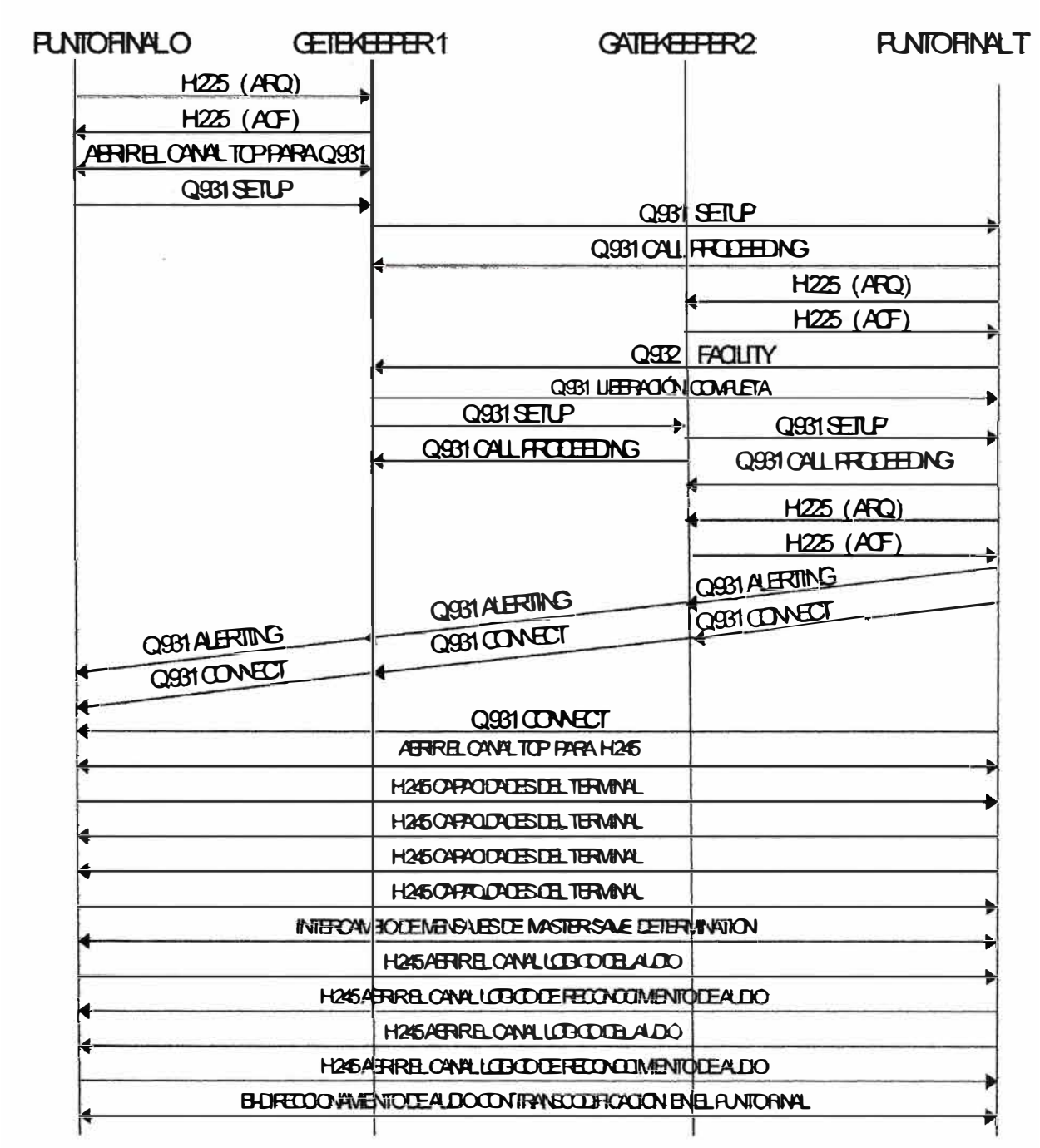

Figura 1.13. Señalización de llamada de gatekeeper erutado. Dos gatekeeper

CAPITULO II
PROTOCOLO DE INICIO DE LA SESIÓN

2.1. Concepto

El Protocolo de inicio de la sesión (SIP) es un protocolo de control de señalización de la capa de aplicación que se utiliza para establecer, mantener y terminar sesiones multimedia. Las sesiones multimedia incluyen la telefonía Internet, las conferencias y otras aplicaciones similares que proporcionan medios como audio, vídeo y datos. Se pueden utilizar invitaciones SIP para establecer sesiones y transportar descripciones de la sesión. SIP soporta sesiones unidifusión y multidifusión, así como llamadas punto a punto y multipunto. Las comunicaciones se pueden establecer y terminar utilizando estas cinco facetas de SIP: localización de usuario, capacidad de usuario, disponibilidad de usuario, configuración de la llamada y manejo de la llamada.

SIP, en el que se basa la petición de comentarios (RFC) 2543, es un protocolo basado en texto que es parte de la arquitectura multimedia general del Grupo IETF (Internet Engineering Task Force). El IETF incluye también el Protocolo de reserva de recursos (RSVP, Resource Reservation Protocol; RFC 2205), el Protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol, RFC 1889), el Protocolo de streaming en tiempo real (RTSP, Real-Time Streaming Protocol; RFC 2326), el Protocolo de anuncio de la sesión (SAP, Session Announcement Protocol, borrador Internet) y el Protocolo de descripción de la sesión (SDP, Session Description Protocol; RFC 2327). Sin embargo, las funciones SIP son independientes, por lo que no dependen de ninguno de estos protocolos. Es importarte tomar nota de que SIP puede operar en conjunción con otros protocolos de señalización, como el H.323. La telefonía del Protocolo Internet (IP) se sigue desarrollando y en el futuro requerirá posibilidades adicionales de señalización. La extensibilidad de SIP permite dichos desarrollos de funcionalidad incremental. Las cabeceras de los mensajes SIP son versátiles y se pueden registrar funciones adicionales con la Agencia de asignación de

números Internet (IANA, Internet Assigned Numbers Authority). La flexibilidad del mensaje SIP también permite que los elementos construyan servicios telefónicos avanzados, incluidos los servicios de tipo de movilidad.
En las próximas páginas explicaremos los siguientes temas:

- Visión general de SIP. Componentes, direccionamiento e invitaciones. Mensajes. Cabeceras, peticiones y respuestas.

- Operatividad básica. Operatividad de servidor proxy y de redirección.

2.2. Visión general de sip

Esta sección describe la funcionalidad básica y los elementos clave de SIP. Los dos componentes de un sistema SIP son los agentes de usuario y los servidores de red. Las partes que llaman y son llamadas se identifican con direcciones SIP; las partes necesitan localizar servidores y usuarios. Las transacciones SIP también se explican como parte de esta visión general.

2.2.1. Agentes de usuario

Los agentes de usuario son aplicaciones cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como cliente y servidor, respectivamente.

- Cliente. Inicia las peticiones SIP y actúa como el agente usuario del llamante.

- Servidor. Recibe las peticiones y devuelve las respuestas en nombre del usuario; actúa como el agente de usuario llamado.

2.2.2. Servidores de red

Existen dos tipos de servidores de red SIP: los servidores proxy y los servidores redirect (de redirección). En la sección "Operatividad básica de SIP", más adelante en este capítulo, se presentan algunos ejemplos funcionales de estos servidores.

- Servidor proxy. Actúa en nombre de otros clientes y contiene funciones de cliente y de servidor. Un servidor proxy interpreta y puede rescribir cabeceras de peticiones antes de pasarlas a los demás servidores. Rescribir las cabeceras identifica al proxy como el iniciador de la petición y asegura que las respuestas siguen la misma ruta de vuelta hasta el proxy en lugar de hasta el cliente.

- Servidor de redirección. Acepta las peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor. Los servidores de redirección no aceptan llamadas ni tampoco procesan o reenvían peticiones SIP.

2.2.3. Direccionamiento

Las direcciones SIP, también llamadas localizadores universales de recursos (URL) SIP, existen en la forma de usuarios @ hosts. Similar a una dirección de correo electrónico, un URL SIP se identifica por usuario@host. La parte de usuario de la dirección puede ser un nombre de usuario o un número de teléfono, y la parte de host puede ser un nombre de dominio o una dirección de red. Se puede identificar a un URL SIP de un usuario por su dirección de correo electrónico. Estos ejemplos muestran dos posibles direcciones URL SIP:

sip:ciscopress@cisco.com

sip:4085262222@171.171.171.1

2.2.4. Localización de un servidor

Un cliente puede enviar una petición SIP directamente a un servidor proxy configurado localmente, o bien a la dirección IP y puerto del correspondiente URL SIP. Enviar una petición SIP es relativamente fácil, ya que la aplicación de sistema final conoce al servidor proxy. Enviar una petición SIP de la segunda manera es algo más complicado, por las siguientes razones:

- El cliente debe determinar la dirección IP y el número de puerto del servidor al que va destinada la petición.

- Si el número de puerto no está enumerado en el URL SIP, el puerto predeterminado es 5060.

➢ Si el tipo de protocolo no está enumerado en el URL SIP pedido, el cliente debe primero intentar conectar utilizando el Protocolo de datagrama de usuario (UDP) o el Protocolo para el control de la transmisión (TCP).

➢ El cliente consulta el servidor de Sistema de denominación de dominio (DNS) para buscar la dirección IP del host. Si no encuentra ningún registro de dirección, el cliente es incapaz de localizar al servidor y no puede continuar con la petición.

2.2.5. Transacciones sip

Cuando se ha resuelto el tema de la dirección, el cliente envía una o más peticiones SIP y recibe una o más respuestas desde el servidor especificado. Todas las peticiones y respuestas asociadas con esa actividad están consideradas como parte de una transacción SIP. Para una mayor simplicidad y coherencia, los campos de cabecera en todos los mensajes de petición coinciden con los campos de cabecera en todos los mensajes de respuesta.

Se pueden transmitir transacciones SIP en los protocolos UDP y TCP. En el caso de TCP, se pueden transportar todos los mensajes de petición y respuesta relacionados con una única transacción SIP sobre la misma conexión TCP. También se pueden transportar. transacciones SIP separadas entre las dos entidades sobre la misma conexión TCP. Si se utiliza UDP, la respuesta se envía a la dirección identificada en el campo de cabecera de la petición.

2.2.6. Localización de un usuario

La parte llamada puede desplazarse desde uno a varios sistemas finales a lo largo del tiempo. Puede moverse desde la red de área local (LAN) corporativa a una oficina en casa conectada a través de su proveedor de servicios de Internet (ISP) o a una conexión pública Intemet mientras atiende a una conferencia. Por tanto, para los servicios de localización, SIP necesita acomodar la flexibilidad y la movilidad de los sistemas finales IP. Las localizaciones de estos sistemas finales pueden estar registradas con el servidor SIP o con otros servidores de localización fuera del ámbito de SIP. En este último caso, el servidor SIP almacena la lista de localizaciones basadas en el servidor de localización exterior que está devolviendo múltiples posibilidades de host. La acción y resultado de localizar a un

usuario depende del tipo de servidor SIP que se esté utilizando. Un servidor de redirección simplemente devuelve la lista completa de localizaciones y permite que el cliente localice directamente al usuario. Un servidor proxy puede probar las direcciones en paralelo hasta que la llamada tenga éxito.

2.3. Mensajes sip

Existen dos tipos de mensajes SIP: peticiones iniciadas por los clientes y respuestas devueltas desde los servidores. Cada mensaje contiene una cabecera que describe los detalles de la comunicación. SIP es un protocolo basado en texto con una sintaxis de mensajes y campos de cabecera idénticos al Protocolo de transferencia de hipertexto (HTFP). Los mensajes SIP se envían sobre los protocolos TCP o UDP con múltiples mensajes transportados en una única conexión TCP o datagrama UDP.

2.3.1. Cabeceras de mensaje

Las cabeceras de mensaje se utilizan para especificar la parte llamante, la parte llamada, la ruta y el tipo de mensaje de una llamada. Los cuatro grupos de cabecera de mensaje son los siguientes:

- Cabeceras generales. Se aplica a las peticiones y a las respuestas.

- Cabeceras de entidad. Define información sobre el tipo de cuerpo del mensaje y longitud.

- Cabeceras de petición. Permite que el cliente incluya información de petición adicional.

- Cabeceras de respuesta. Permite que el servidor incluya información de respuesta adicional.

Estos cuatro grupos principales de cabeceras, junto con las 37 cabeceras correspondientes, se enumeran en la Tabla 2.1

TABLA 2.1 CABECERAS SIP.

Cabeceras Generales	Cabeceras de entidad	Cabeceras de petición	Cabeceras de respuesta
Accept	Content-Encoding	Authorization	Allow
Accept-Encoding	Content-Length	Contact	ProxyAuthenticate
Accept-Language	Content-Type	Hide	Retry-After
Call-ID		Max-Forwards	Server
Contact		Organization	Unsupported
CSeq		Priority	Warning
Date		Proxy-Authorization	WWW-Authenticate
Encryption		Proxy-Require	
Expires		Route	
From		Require	
Record-Route		Response-Key	
Timestamp		Subject	
To		User-Agent	
Via			

En la tabla 2.2 aporta una breve explicación de algunas cabeceras clave

TABLA 2.2 EXPLICACIÓN DE ALGUNAS CABECERAS SIP CLAVES.

Cabecera	Explicación
To	Identifica al receptor de la petición.
From	Indica quién ha iniciado la petición.
Subject	Describe la naturaleza y tema de la llamada.
Vía	Indica la ruta tomada por la petición.
Call-ID	Sólo identifica una invitación específica o todos los registros de un cliente determinado.

Content-Length	Identifica el tamaño del cuerpo del mensaje en octetos.
Content-Type	Indica el tipo medio del cuerpo del mensaje.
Expires	Identifica la fecha y hora a la que expira el contenido del mensaje.
Route	Indica la ruta tomada por una petición.

2.3.2. Peticiones de mensaje

La comunicación SIP presenta seis tipos de peticiones de mensaje. Estas peticiones, a las que también se hace referencia como métodos, permiten que los agentes de usuarios y servidores de red localicen, inviten y administren llamadas. Las seis peticiones SIP son las siguientes:

- INVITE. Este método indica que el usuario o servicio es invitado a participar en una sesión. Incluye una descripción de sesión y, para llamadas de dos vías, la parte llamante indica el tipo de medio. Una respuesta con éxito a una invitación INVITE de dos partes (respuesta 200 OK) incluye el tipo de medios recibido por la parte llamada. Con este simple método, los usuarios pueden reconocer las posibilidades del otro extremo y abrir una sesión de conversación con un número limitado de mensajes e idas y vueltas.

- ACK. Estas peticiones corresponden a una petición INVITE. Representan la confirmación final por parte del sistema final y concluye la transacción iniciada por el comando INVITE. Si la parte llamante incluye una descripción de la sesión en la petición ACK, no se utilizan más parámetros adicionales en la misma. Si no se incluye una descripción de la sesión, los parámetros de la sesión en la petición INVITE se utilizan como los predeterminados.

- OPTIONS. Este método permite consultar y reunir posibilidades de agentes de usuarios y servidores de red. Sin embargo, esta petición no se utiliza para establecer sesiones.

➢ BYE. Este método se utiliza por las partes que llaman y son llamadas para liberar una llamada. Antes de liberar realmente la llamada, el agente de usuario envía esta petición al servidor indicando el deseo de liberar la sesión.

➢ CANCEL. Esta petición permite que los agentes de usuario y servidores de red cancelen cualquier petición que esté en progreso. Esto no afecta a las peticiones terminadas en las que las respuestas finales ya fueron recibidas.

➢ REGISTER. Este método se utiliza por los clientes para registrar información de localización con los servidores SIP.

2.3.3. Respuestas de mensajes

Las respuestas a los mensajes SIP están basadas en la recepción e interpretación de una petición correspondiente. Se envían como respuesta a una petición e indican si la llamada ha tenido éxito o ha fallado, incluido el estado del servidor. Las seis clases de respuestas, sus códigos de estado y explicaciones de lo que hacen aparecen en la Tabla 2.3. Las dos categorías de respuestas son provisionales, lo que indica que está en progreso, y final, lo que termina una petición. En la Tabla 2.3 las respuestas Informational son provisionales y las otras cinco son respuestas finales

TABLA 2.3. RESPUESTAS SIP.

CLASE DE RESPUESTA	CÓDIGO DE ESTADO	EXPLICACIÓN
Informational	100	Intentando
	180	Sonando
	181	La llamada está siendo reenviada
	182	Puesta en la cola
Success	200	OK
	300	Elección múltiple
	301	Movida permanentemente
	302	Movida temporalmente

	303	Véase otra
	305	Utilizar proxy
	380	Servicio alternativo
Client-Error	400	Petición defectuosa
	401	No autorizado
	402	Se requiere pago
	403	Prohibido
	404	No encontrado
	405	Método no permitido
	406	No aceptable
	407	Se requiere autenticación de proxy
Client-Error	408	Se acaba tiempo de petición
	409	Conflicto
	410	Se ha marchado
	411	Se requiere longitud
	413	Entidad pedida demasiado larga
	414	URL pedido demasiado largo
	415	Tipo de medio no soportado
	420	Extensión errónea
	480	No disponible temporalmente
	481	Segmento de llamada
	482	Detectado bucle
	483	Demasiados saltos
	484	Dirección incompleta
	485	Ambiguo
	486	Ocupado
Server-Error	500	Error interno de servidor
	501	Sin implementar
	502	Gateway erróneo
	503	Servicio no disponible
	504	Gateway fuera de tiempo
	505	Versión SIP no soportada
Global Failure	600	Ocupado en todas partes
	603	Rechazado
	604	No existe en ningún sitio
	606	No aceptable

2.4. Operatividad básica de sip

Los servidores SIP manejan las peticiones entrantes de dos maneras. Esta operatividad básica se fundamenta en invitar a un participante a una llamada. Los dos modos básicos de operar del servidor SIP que se describen en esta sección son los siguientes:

- Servidores proxy.
- Servidores de redirección

2.4.1 Ejemplo de servidor proxy

El intercambio de comunicación para el método INVITE utilizando el servidor proxy se ilustra en la siguiente figura. Los pasos operacionales en el modo proxy que se necesitan para que una llamada de doble vía tenga éxito son los siguientes:

1. El servidor proxy acepta la petición INVITE del cliente.

2. El servidor proxy identifica la localización utilizando las direcciones y los servicios de localización proporcionados.

3. Se emite una petición INVITE a la dirección de la localización devuelta.

4. El agente de llamadas de la parte llamada alerta al usuario y devuelve una indicación de éxito al servidor proxy peticionario.

5. Una respuesta OK (200) es enviada desde el servidor proxy a la parte llamante.

6. La parte llamante confirma la recepción emitiendo una petición ACK, que es transmitida por el proxy o enviada directamente a la parte llamada.

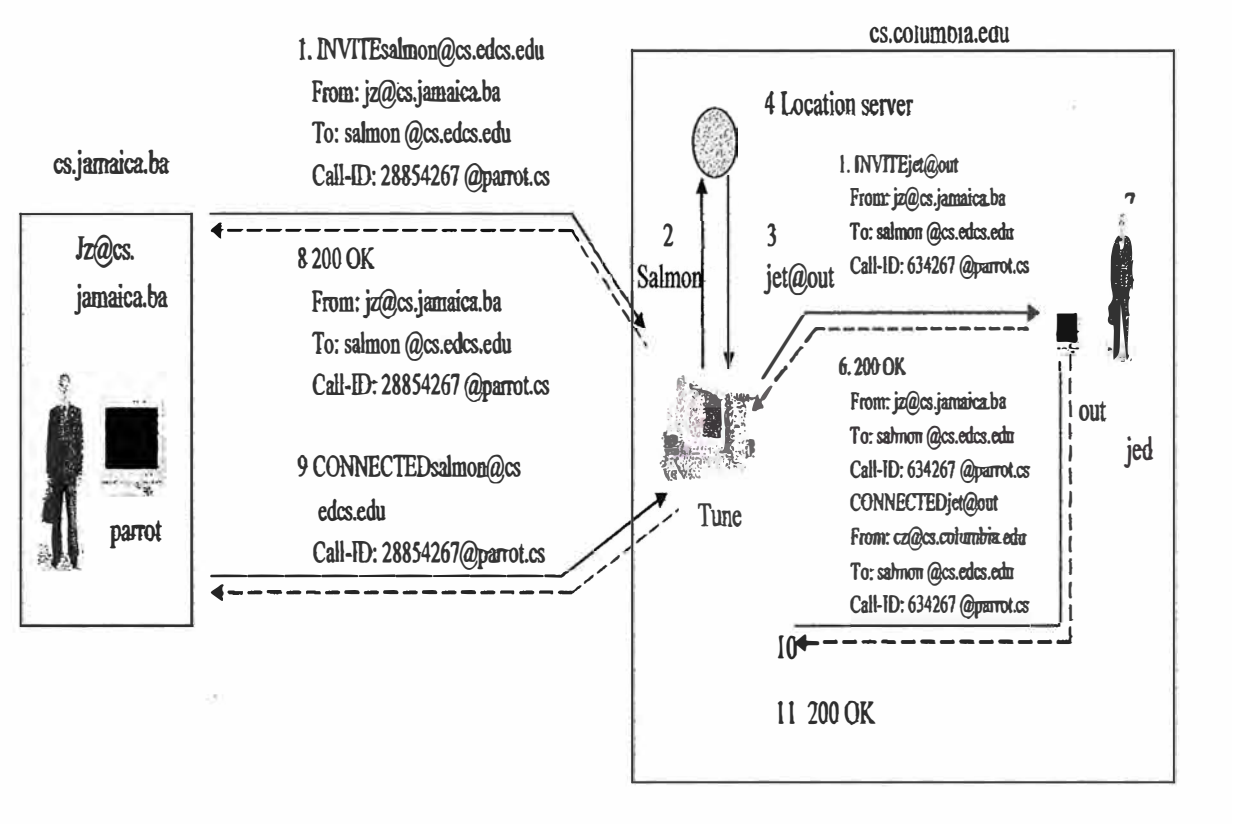

Figura 2.1 Mode de operación Proxy

2.3.2. Ejemplo de servidor de redirección

El intercambio de protocolo para la petición INVITE que utiliza el servidor de redirección aparece en la siguiente figura.

Los pasos operacionales en el modo de redirección (redirect) para que una llamada de doble vía tenga éxito son los siguientes:

1. El servidor de redirección acepta la petición INVITE desde la parte llamante y contacta los servicios de localización con la información facilitada.

2. Cuando se ha localizado al usuario, el servidor de redirección devuelve la dirección directamente a la parte llamante. A diferencia del servidor proxy, el servidor de redirección no emite ningún INVITE.

3. El agente de usuario envía un ACK al servidor de redirección confirmando que la transacción se ha completado.

4. El agente de usuario envía una petición INVITE directamente a la dirección devuelta por el servidor de redirección.

5. La parte llamada proporciona una indicación de éxito (200 OK) y la parte llamante devuelve un ACK.

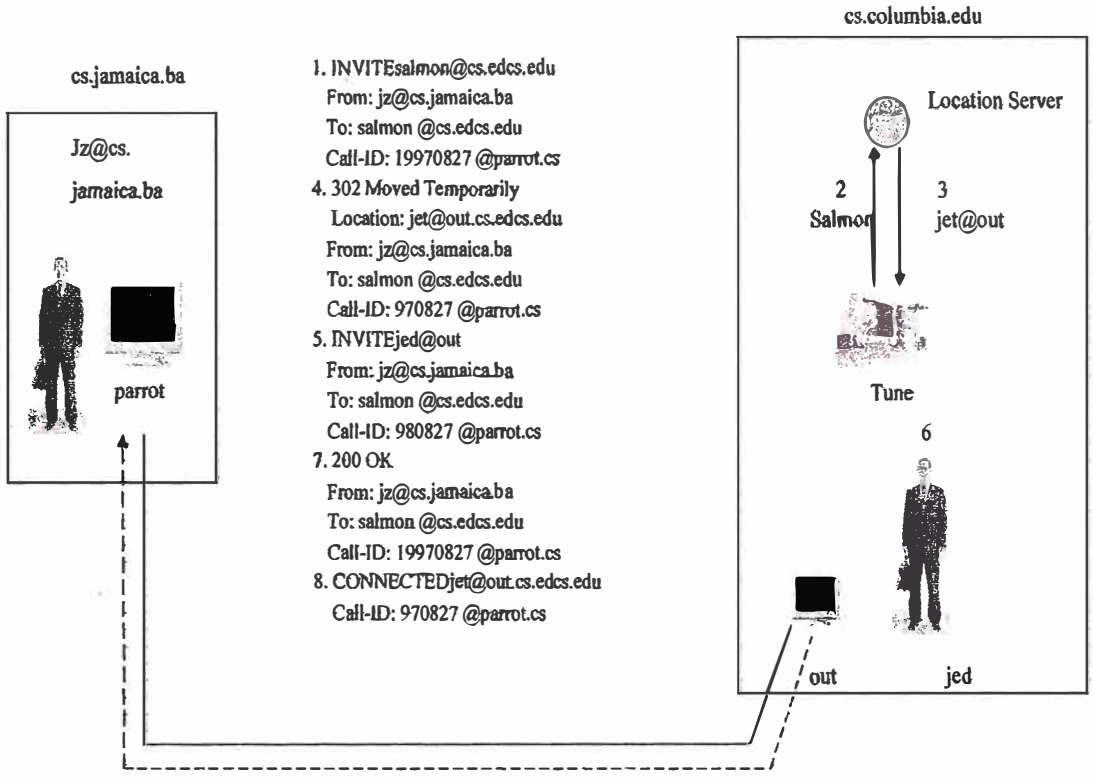

Figura 2.2 Mode de operación de redirección

CAPITULO III
PROTOCOLOS DE CONTROL DE GATEWAY

En este capítulo explica los dos protocolos de control de gateway del Grupo IETF (Internet Engineering Task Force) que se utilizan para controlar los gateways de Voz sobre IP (VoIP) desde elementos externos de control de llamadas: el Protocolo simple de control de gateway (SGCP, Simple Gateway Control Protocol) y el Protocolo de control de gateway de medios (MGCP, Media Gateway Control Protocol).

También explica otra especificación de dispositivo de control que tiene un impacto significativo en la industria de la telefonía de paquetes: el Control de dispositivo de protocolo Internet (IPDC, Internet Protocol Device Control) que se fusionó con SGCP para formar MGCP. Estos tres protocolos de control de gateway fueron diseñados para soportar gateways que tienen inteligencia externa (es decir, elementos externos de control de llamadas). Por tanto su utilización prevalece en grandes gateways troncales y residenciales.

3.1. Protocolo simple de control de gateway

El Protocolo simple de control de gateway (SGCP, Simple Gateway Control Protocol) permite elementos de control de llamadas para controlar las conexiones entre gateways VoIP troncales y residenciales y los de tipos de acceso. A pesar de que esos gateways tienen diferentes segmentos de mercado, todos ellos convierten la voz de multiplexión por división de tiempo (TDM) en voz por paquetes. Generalmente, se hace referencia a los elementos de control de llamadas como Controladores de gateway de medios (MGC, Media Gateway Controllers) o agentes de llamadas.SGCP asume una arquitectura cuya inteligencia de control de llamadas está fuera del gateway y está manejada por elementos de control de llamadas externos, llamados agentes de llamadas. En este modelo, uno o más agentes de llamadas pueden participar en la construcción de una llamada. La sincronización entre los agentes de llamadas se da por hecho y no está cubierta por el protocolo SGCP.

SGCP se utiliza para establecer, mantener y desconectar llamadas a través de la red del Protocolo Internet (IP). Esto se realiza controlando las conexiones requeridas entre los puntos finales deseados y correspondientes. La autorización de las llamadas y de las conexiones está fuera del ámbito de este protocolo. SGCP no contiene un mecanismo de seguridad para la configuración de llamadas no autorizadas o interferencias. Sin embargo, la especificación dice que se desea que todas las transacciones se lleven a cabo sobre conexiones Internet seguras. La seguridad de esas conexiones viene dada por la Arquitectura de seguridad IP (IP Security Architecture) como viene definido en la petición de comentarios (RFC) 1825 y utilizando la Cabecera de autenticación IP (IP Authentication Header [RFC 1826]), o bien la Encapsulación de seguridad de la carga útil IP (IP Encapsulating Security Payload [RFC 1827]).

3.1.1. Relación con otros estándares.

En el protocolo SGCP, los agentes de llamadas manejan funciones de señalización de llamadas y los gateways proporcionan funciones de conversión de audio. Los agentes de llamadas también pueden implementar capacidades de señalización H.323 y establecer llamadas utilizando el modelo de Señalización de llamada de gatekeeper enrutado (GKRCS, Gatekeeper Routed Call Signaling). En este caso, los agentes de llamadas pueden conectar llamadas entre gateways utilizando SGCP y entre terminales utilizando procedimientos H.323. El IETF produjo estándares para las aplicaciones multimedia. Éstos incluyen los protocolos de descripción de la sesión (SDP; RFC 2327), Protocolo de anuncio de la sesión (SAP), Protocolo de inicio de la sesión (SIP, explicado con más detalle en el Capítulo II, Protocolo de inicio de la sesión"), y Protocolo de streaming en tiempo real (RTSP; RFC 2326). Los tres últimos estándares proporcionan técnicas de señalización alternativa a SGCP; sin embargo, los cuatro estándares utilizan SDP para la descripción de la sesión y el Protocolo de transporte en tiempo real (RTP) para transmitir audio. El agente de llamadas también puede actuar entre técnicas de señalización alternativas y direccionar los flujos RTP entre los elementos correspondientes.

3.1.2. Protocolo de descripción de la sesión

El Protocolo de descripción de la sesión (SDP, Session Description Protocol) describe los parámetros de la sesión, como las direcciones IP, el puerto del Protocolo de datagrama de

usuario (UDP, User Datagram Protocol), los perfiles RTP y las posibilidades de conferencia multimedia. SGCP sigue las convenciones del SDP como se definen en la RFC 2327; y se espera que las implementaciones sean conformes. Sin embargó, SGCP limita su primera utilización multimedia de SDP a un tipo de medio: los circuitos audio en los gateways de telefonía. Los agentes de llamadas utilizan los siguientes parámetros SDP para abastecer a los gateways de telefonía:

- Direcciones IP. Especifica el gateway remoto, gateway local o las direcciones de conferencias de audio de multidifusión.

- Puerto UDP. Indica el puerto de transporte que se utiliza para recibir los paquetes RTP desde el gateway remoto.

- Medio de audio. Especifica el medio de audio, incluido el códec.

3.1.3. Transmisión sobre udp.

Los mensajes de petición de SGCP se envían a las direcciones IP de punto final especificadas utilizando el protocolo UDP. Los mensajes de respuesta también, se envían a través de UDP a la dirección IP de origen. UDP proporciona servicios sin conexión sobre IP y, por tanto, puede estar sujeto a pérdida de paquetes. SGCP maneja las respuestas perdidas o retrasadas repitiendo las peticiones. Para realizar estas peticiones, las entidades SGCP deben mantener una lista de las transacciones que se están ejecutando, así como todas las respuestas enviadas en los últimos 30 segundos. Esta lista permite que la entidad compare el identificador de transacción de las peticiones entrantes con el identificador de transacción de las últimas respuestas. Por tanto, si una entidad recibe una petición con un identificador de transacción que coincide con una respuesta caché, vuelve a enviar la respuesta. La responsabilidad de la entidad peticionaria es proporcionar un tiempo de expiración adecuado, proporcionar reintentos oportunos, limpiar las conexiones pendientes y buscar servicios redundantes.

3.1.4. Conceptos sgcp

La base de SGCP son los puntos finales y las conexiones. Los grupos de conexiones constituyen una llamada que es configurada por uno o más agentes de llamadas. Otro concepto clave que se explica en esta sección es la utilización de mapas de dígitos para recopilar dígitos en los gateways.

a. Puntos finales

Los puntos finales son fuentes o receptores de datos que existen física o lógicamente dentro de una entidad. Los circuitos troncales que conectan los gateways y los switches telefónicos son puntos finales físicos, mientras que los avisos almacenados en dispositivos de audio son puntos finales lógicos. Los puntos finales se identifican por dos componentes: el nombre de dominio de la entidad donde existe el punto final y el nombre local que especifica el punto final individual.

En el caso de los circuitos troncales, los agentes de llamadas tienen una interconexión del Sistema de señalización 7 (SS7) donde los circuitos están identificados por el grupo troncal y el número de circuito. Por tanto, cuando un agente de llamadas está creando una conexión, lo siguiente identifica al punto final:

nombre de dominio / interfaz / número de circuito

El nombre de dominio y la interfaz representan el gateway y enlace donde existe el punto final. El circuito representa la capa 0 de la señal digital física (DS-0) donde se termina la llamada.

b. Conexiones

Las conexiones existen tanto en la forma de punto a punto como en la forma multipunto. Se pueden utilizar varias conexiones punto a punto para construir una llamada y transferir datos entre puntos finales. Las conexiones multipunto conectan un punto final con una sesión multipunto. El gateway identifica la conexión cuando recibe la instrucción de crear una conexión. Estos identificadores de conexión representan la conexión entre el punto final y la llamada.

c. Llamadas

Un grupo de conexiones compone una llamada. Los agentes de llamadas asignan identificadores de llamada, que son únicos para cada llamada y son globalmente únicos a través de todo el sistema. Un identificador de llamada único enlaza todas las conexiones que están asociadas a una llamada. Ese identificador permite que ocurra la mediación de contabilidad o facturación para las llamadas basadas en SGCP.

d. Agentes de llamadas

Los agentes de llamadas son elementos externos que proporcionan la inteligencia de control de llamadas para las redes VoIP. Los agentes de llamadas se identifican dentro de la red por su denominación de dominio, no por su dirección IP. El servicio de denominación de dominio permite las implementaciones redundantes de agentes de llamadas y que ocurran cambios en la plataforma sin interrumpir el servicio.

e. Mapas de dígitos

Los gateways de acceso utilizan mapas de dígitos para enviar la totalidad del número que un usuario ha marcado al agente de llamadas. El agente de llamadas utiliza ese mapa de dígitos para instruir al gateway de que tiene que reunir los dígitos marcados.

También se pueden utilizar los mapas de dígitos con los gateways troncales (TGW) para reunir los códigos de acceso y los números de las tarjetas de crédito. Los mapas de dígitos están considerados como un conjunto de reglas del plan de marcación para que el gateway las utilice para reunir los dígitos apropiados, de tal manera que el agente de llamadas pueda tomar una decisión de enrutamiento.

Los mapas de dígitos indican al gateway cuándo debe dejar de reunir dígitos y transmitir el número. La Tabla 3.1 muestra diferentes secuencias marcadas que un gateway de acceso debe regular y saber cuándo transmitir.

TABLA 3.1. NÚMERO MARCADO Y SERVICIOS.

Número marcado	Servicio
0	Servicios de operador local en EE.UU.
411	Servicios de directorio en EE.UU.
911	Servicios de emergencia en EE.UU.
1 + hasta 10 dígitos	Servicios de larga distancia en EE.UU.
011 + hasta 14 dígitos	Número internacional en EE.UU.

3.1.5. Funciones de control

El servicio del protocolo SGCP consiste en las funciones de manejo del punto final y manejo de la conexión. El servicio SGCP permite que el agente de llamadas dé instrucciones al gateway sobre la creación, modificación y eliminación de la conexión e informe al agente de llamadas sobre los eventos que están ocurriendo en el gateway.

El protocolo SGCP tiene las siguientes cinco primitivas, o comandos (también conocidos como verbos):

- Notification Request. Los agentes de llamadas emiten este comando para indicar al gateway que tiene que detectar eventos como tonos off-hook y de marcación multifrecuencia (DTMF).

- Notify. Los gateways utilizan este comando para avisar al agente de llamadas sobre eventos.

- Deleate Connection. Los agentes de llamadas utilizan este comando para crear conexiones de punto final en el interior de un gateway.

➢ Modify Connection. Los agentes de llamadas emiten esta petición para cambiar los parámetros de conexión establecidos. Se puede utilizar este comando para cambiar el gateway de salida de la ruta de audio RTP a un gateway de salida diferente.

➢ Delete Connection. Los agentes de llamadas y gateways pueden utilizar este comando para desconectar las conexiones existentes.

Estas cinco funciones controlan los gateways e informan a los agentes de llamadas sobre los eventos. Cada comando o petición contiene parámetros específicos requeridos para ejecutar la transacción. La Tabla 3.2 proporciona los parámetros Obligatorio (M), Opcional (O) y Prohibido (F) para cada petición.

TABLA 3.2. PARÁMETROS DE PETICIÓN SGCP.

Parámetro	Notification Request	Create Notify	Modify Connection	Delete Connection	Connection
Identificador de llamada	M	M	O	F	F
Identificador de conexión	F	M	O	F	F
Identificador de petición	O	O	O	M	M
Opciones de Conexión local	O	M	F	F	F
Modo de conexión	M	M	F	F	F
Eventos solicitados	O	O	O	O	F
Petición de señal	O	O	O	O	F

Entidad notificada	O	O	O	O	O
Evento observado	F	F	F	F	M
Mapa de dígitos	O	O	O	O	F
Código de razón	F	F	O	F	F
Parámetros de Conexión	F	F	O	F	F
ID especificado de Punto de Terminación	F	F	F	F	F

Éste es un buen momento para explicar el concepto de los modos de conexión antes de profundizar en cada función de petición.

Un parámetro de modo determina y califica cómo manejar el audio recibido en las conexiones.

La operación de la conexión se describe en los modos de conexión ilustrados en la Tabla 3.3.

TABLA 3.3. MODOS DE CONEXIÓN.

Modo	Operación
sendonly	El gateway sólo deberá enviar paquetes.
Recvonl	El gateway sólo deberá recibir paquetes.
Sendrecv	El gateway sólo deberá enviar y recibir paquetes.
Inactive	El gateway no deberá enviar o recibir paquetes.
Loopback	El gateway deberá poner el circuito en el modo de bucle de prueba.
conttest	El gateway deberá poner el circuito en el modo de evaluación.

a. Notification request

El comando Notification Request indica al gateway que tiene que notificar al originador cuándo ocurre un evento determinado en un punto final. El agente de llamadas descarga una lista de eventos en el gateway que está pidiendo la detección y registrando determinados eventos. Normalmente, la petición de notificación contiene los siguientes campos:

- Endpoint ID (ID de punto final). Indica el punto final en el gateway donde actúa la petición.

- Notified Entity (Entidad notificada). Si está presente, especifica dónde deberá enviarse la notificación. Si no está presente, indica que la notificación deberá enviarse al originador.

- Request Identifier (Identificador de petición). Pone en correlación la petición con la notificación que la desencadena.

- Digit Map (Mapa de dígitos). Permite que el agente de llamadas descargue un mapa de dígitos que sólo devuelve los dígitos para notificaciones subsiguientes. Es un parámetro opcional.

- Requested Events (Eventos solicitados). Contiene la lista de los eventos que el gateway debe detectar y registrar en el agente de llamadas. Los posibles eventos de la lista incluyen los tonos de fax y módem, el tono de continuidad y detección, la transición on-hook y off-hook, el flash hook, la señalización asociada al canal (CAS), el parpadeo y la DTMF o dígitos de impulso. Además, cada evento tiene una acción asociada, como "notificar el evento inmediatamente", "cambiar audio para llamada en espera y llamada a tres", "acumular de acuerdo con el mapa de dígitos" e "ignorar el evento".

- Signal Requests (Peticiones de señal). Especifica un conjunto de acciones de punto final que se solicitan al gateway para que las haga. La lista de acciones incluye el sonido y sonido distintivo, así como los tonos de volver a llamar, marcado, intercepción, ocupado, llamada en espera, aviso off-hook y continuidad.

El evento solicitado hace referencia a la detección de un evento, y el evento de señal hace referencia a la acción resultante. Por ejemplo, si off-hook (descolgar) es el evento solicitado, el tono de marcado es el evento de señal.

b. Notification

El gateway envía una Notification basada en los eventos solicitados en la petición de notificación y en que ocurran esos eventos observados. El comando Notification contiene los siguientes parámetros:

- Endpoint ID (ID de punto final). Este parámetro indica el punto final en el gateway que está emitiendo la notificación.

- Notified Entity (Entidad notificada). Este parámetro opcional es igual al mismo parámetro en la petición de notificación correspondiente.

- Requested Identifier (Identificador solicitado). Este parámetro es el mismo en la petición de notificación y correlaciona la petición con la notificación.

- Observed Events (Eventos observados). Este parámetro contiene los datos reales observados basados en el parámetro de evento solicitado en la petición de notificación.

c. Createconnection

Como su nombre indica, esta función crea una conexión entre dos puntos finales. Los siguientes parámetros CreateConnection proporcionan la información necesaria para construir una vista de una conexión de un gateway:

- Call ID (ID de llamada). Todas las conexiones relacionadas con una llamada comparten este identificador único de red ancha o global.

- Endpoint ID (ID de punto final). Identifica el punto final en el gateway donde se ejecuta el comando CreateConnection.

- Notified Entity (Entidad notificada). Parámetro opcional que especifica dónde se deben enviar las notificaciones.

- Local Connection Options (Opciones de conexión local). Describe las características de datos de la comunicación que se utilizan para ejecutar el comando CreateConnection. Los campos en este parámetro incluyen método de codificación, periodo de empaquetamiento, banda ancha, tipo de servicio (ToS) y utiliza una cancelación de eco. Por defecto, la cancelación de eco se lleva a cabo siempre; sin embargo, este campo permite que se desactiven esas operaciones.

- Mode (Modo). Dicta el modo de operación para la conexión. Las opciones son dúplex completo, sólo recibir, sólo enviar, inactivo y loopbad.

- Remote Connection Descriptor (Descriptor de conexión remota). Indica las opciones de la conexión local enviadas al gateway remoto.

- Requested Events, Request Identifier, Digit Map, Signal Requests (Eventos solicitados, identificador de petición, mapa de dígitos, peticiones de señal). El agente de llamadas puede utilizar estos parámetros opcionales para transmitir una petición de notificación que puede ejecutarse cuando se crea una conexión.

d. Modifyconnection

La función ModifyConnection cambia las características de la vista de una conexión o llamada del gateway. Los parámetros y campos en ModifyConnection son los mismos que en la petición CreateConnection, con el añadido del parámetro Connection ID (ID de conexión). El parámetro Connection ID (ID de conexión) únicamente identifica las conexiones dentro de una llamada. Se pueden cambiar los siguientes parámetros de conexión cambiando el modo de parámetros del comando ModifyConnection: esquema de codificación, periodo de empaquetamiento, cancelación de eco y activar o desactivar conexiones.

e. Deleteconnection

Un agente de llamadas o gateway emite la función DeleteConnection para terminar una conexión. Los agentes de llamadas utilizan esta petición para dar por finalizada una conexión entre dos puntos o limpiar todas las conexiones que terminan en un punto final dado. El gateway emite este comando para limpiar las conexiones si detecta que un punto final ya no es capaz de enviar o recibir audio. Si el gateway limpia una conexión, se incluye un código de causa en el mensaje indicando la causa. Una vez que se han terminado las conexiones, los gateways deberán poner el punto final en modo inactivo haciendo que esté disponible para una sesión posterior. Un valioso atributo del comando DeleteConnection es que distribuye estadísticas que tienen que ver con una llamada. Los datos estadísticos contenidos en el mensaje DeleteConnection aparecen en la siguiente Tabla 3.4

TABLA 3.4. INFORMACIÓN ESTADÍSTICA: COMANDO DELETE CONNECTION DE SGCP.

Datos	Explicación
Paquetes enviados	Número de paquetes enviados en la conexión.
Octetos enviados	Número de octetos enviados en la conexión.
Paquetes recibidos	Número de paquetes recibidos en la conexión.
Octetos recibidos	Número de octetos recibidos en la conexión.
Paquetes perdidos	Números de paquetes perdidos según indican los números de secuencia.
Fluctuación de fase	Retraso medio entre paquetes en milisegundos.
Latencia	Latencia media en milisegundos.

3.1.6. Códigos de devolución y códigos de error

Los acuses de recibo de mensajes SGCP contienen códigos de devolución que identifican el estado de cada petición confirmada. Los códigos de devolución y las posteriores explicaciones para cada código se incluyen en la Tabla 3.5

TABLA 3.5. CÓDIGOS DE DEVOLUCIÓN Y DE ERROR.

Código de devolución	Explicación
200	Ejecución normal de la transacción.
250	La conexión ha sido borrada.
400	Incapaz de ejecutar la transacción debido a un error transitorio.
401	El teléfono está off-hook (descolgado).
402	El teléfono está on-hook (colgado).
500	Incapaz de ejecutar la transacción debido a un punto final desconocido.
501	Incapaz de ejecutar la transacción debido a que el punto final no está preparado.
502	Incapaz de ejecutar la transacción debido a insuficientes recursos de punto de terminación.
510	Incapaz de ejecutar la transacción debido a detección de error de Protocolo.
511	Incapaz de ejecutar la transacción debido a que la petición contiene una extensión no reconocida.
512	Incapaz de ejecutar la transacción debido a que el gateway es incapaz de detectar los eventos solicitados.
513	Incapaz de ejecutar la transacción debido a que el gateway es incapaz de generar una de las señales solicitadas.
314	Incapaz de ejecutar la transacción debido a que el gateway es incapaz de enviar el aviso especificado.

3.1.7. Flujos de llamada

Los flujos de llamada que presentamos en esta sección ayudan a mostrar el uso y partes operativas del protocolo SGCP. Dos ejemplos de llamadas básicas pueden mostrar los flujos de llamada entre un RGW y un TGW. En el primer ejemplo, el RGW es el gateway de origen y el TGW es el gateway de terminación, como muestra la figura 3.1. En el

segundo ejemplo, que aparece la Figura 3.2, el TGW es el gateway de origen y RGW, el gateway de terminación.
Ambas figuras incluyen el usuario (Usr), el RGW, el TGW y las cinco entidades siguientes:

- CO. Oficina central que inicia o termina los mensajes SS7.

- SS7/Parte de usuario de red digital de servicios integrados (ISUP)-Terminación de señalización de los mensajes SS7.

- CA. Agente de llamadas.

- CDB. Base de datos común que proporciona información de autorización y enrutamiento.

- ACC. Gateway de contabilidad que reúne información de principio y fin de la contabilidad.

3.2. Protocolo de control de gateway de medios

El Protocolo de control de gateway de medios (MGCP, Media Gateway Control Protocol) controla VoIP a través de elementos externos de control de llamadas.

Usr	RGW	CA	CDB	ACC	TGW	SS7/ISUP	C0
	<-	Notification Request					
	Ack	->					
Off-hook	Notify	->					
	<-	Ack					
	<-	Notification Request					
(Dial-tone)							
	Ack	->					
	Notify	->					
	<-	Ack					
Digit	<-	Notification Request					
	Ack	->					
(progres s)	<-	Create connection					
	Ack	->					
		Query (E.164 S, D)	->				
		<- Create connection	<- IP				
			-------	-------	-> (cut in)		
			-------	---------	ack		
		<- IAM	-------	---------	---------	->	->
						IAM <-	ACM
	<-	Modify Connection					
	Ack	->					
		<-	-------	-------	---------	ACM	
	<-	Notification Request					
	Ack	->					
		<-	-------	-------	-------	ANM	
	<-	Notification Request					
	Ack	->					
		Modify Connection					
	Ack (cut in)	->					
		Call start	-------	->			
		<-	-------	-------	-------	REL	
	<-	Delete Connection					
		Delete Connection	-------	-------	->		
	Perf Data	->					
		<-	-------	-------	perf data		
		Call end	-------	->			
	Notify	->					
	<-	Ack					
	<-	Notification Request					
	Ack	->					

Figura 3.1 LLamada básica de RGW a TGW

La primera versión de MGCP se basó en la fusión de SGCP e IPDC. Por tanto, esta sección se concentra en las diferencias entre MGCP y SGCP, que se deben en gran parte a la funcionalidad inspirada por IPDC.

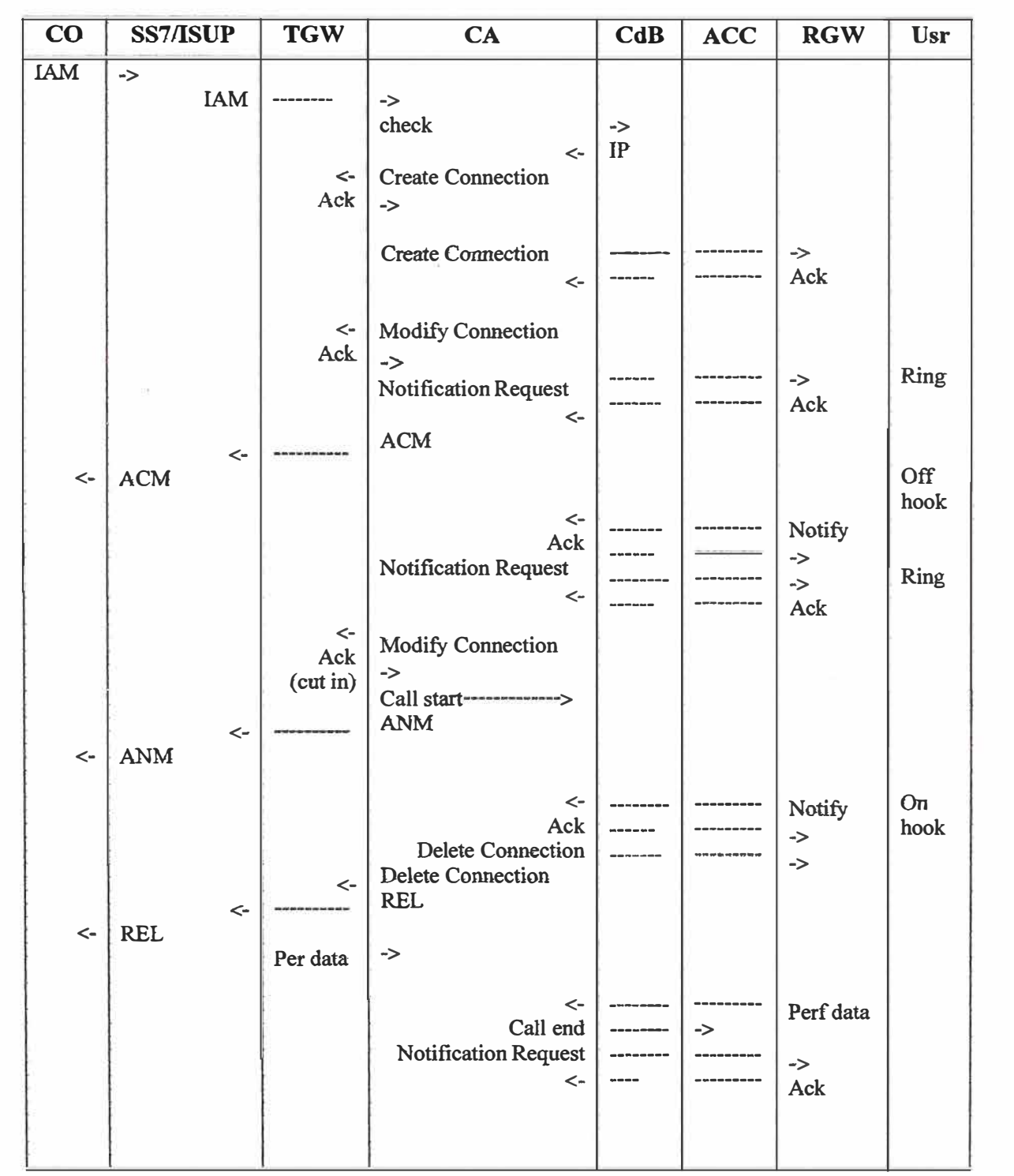

Figura 3.2 LLamada básica de TGW A RGW

MGCP permite que los gateways de telefonía sean controlados por elementos externos de control de llamadas (los MGC, a los que se hace referencia como agentes de llamadas en SGCP). Los gateways de telefonía incluyen lo siguiente:

- Trunk Gateways (Gateways troncales). La interfaz entre la red telefónica v la red VoIP.

- Voice over ATM Gateways (Gateways de voz sobre ATM). La interfaz entre la red telefónica y la red de Modo de transferencia asíncrona (ATM, Asynchronous Transfer Mode).

- Residential Gateways (Gateways residenciales). Permite que el acceso telefónico analógico tradicional interactúe a través de la red VoIP.

- Business and Access Gateways (Gateways de empresa y de acceso). Proporciona un Intercambio privado de ramas (PBX, Private Branch Exchange) analógico o digital y una interfaz de switch blando a una red VoIP.

- Network Access Servers (Servidores de acceso de red). La interfaz que proporciona el acceso a Internet a través de la Red pública de telefonía conmutada (PSTN) y los módems.

- Circuit or Packet Switches (Switches de circuitos o de paquetes). Ofrece acceso de control de llamadas a elementos externos de control de llamadas.

MGCP utiliza el mismo modelo de conexión que SGCP, donde lo más básico son los puntos finales y las conexiones. Los puntos finales pueden ser físicos o lógicos, y las conexiones pueden ser punto a punto o multipunto. Sin embargo, MGCP permite que las conexiones se establezcan sobre varios tipos de redes portadoras de la siguiente manera:

- Redes IP. Transmisión de audio sobre redes de Protocolo para el control de la transmisión/Protocolo Internet (TCP/IP) utilizando RTP y UDP.

- Redes ATM. Transmisión de audio sobre una red ATM utilizando la capa 2 de adaptación ATM (AAL2) u otra capa de adaptación.

➢ Conexiones internas. La transmisión de paquetes a través del plano trasero TDM o bus del gateway (como hairpinning, que tiene lugar cuando una llamada no es enviada dentro de la red de paquetes sino devuelta a la PSTN).

El resto de esta sección se ocupa de algunas diferencias sencillas entre SGCP y MGCP. También presentamos aquí una introducción para las dos grandes secciones que cubren el empaquetamiento de eventos y las funciones de control en MGCP.

MGCP utiliza SDP para abastecer a los gateways con direcciones IP y perfiles UDP/RTP idénticos a los de SGCP. Sin embargo, MGCP utiliza SDP para dos tipos de medios: circuitos de audio y circuitos de acceso de datos. Asimismo, los mensajes MGCP son transmitidos a través de la red de paquetes sobre el protocolo UDP, aunque se pueden añadir datos a los mensajes. MGCP permite que varios mensajes sean enviados al mismo gateway en un paquete UDP. Estos datos añadidos a los mensajes deberán procesarse como si fueran recibidos como varios mensajes simultáneos.

Una estructura de wildcard (comodín) formal, inspirada en IPDC, se introduce en MGCP. Los MGC, o agentes de llamadas, pueden utilizar la convención de wildcard cuando envían comandos a los gateways. El wildcard permite que el agente de llamadas identifique uno o todos los argumentos del comando.

Si se termina una llamada multipunto y se necesita desconectar un determinado número de conexiones, el agente de llamadas puede enviar una petición DeleteConnection utilizando la totalidad del argumento para especificar todas las conexiones relacionadas con el punto final especificado.
Los flujos de llamada adicionales no se proporcionan en esta sección, dado que MGCP tiene las mismas funciones de control de llamadas, mensajes y funciones de secuenciación que SGCP.

3.2.1. Paquetes de eventos

Inspirados en IPDC, los eventos y señales de MGCP están agrupados en paquetes. Cada paquete soporta los típicos eventos y señales requeridos para un tipo determinado de

punto final. Un paquete puede agrupar eventos y señales relacionados con un gateway troncal y otro paquete puede agrupar eventos y señales relacionados con una línea de tipo de acceso analógico. El término nombre de evento hace referencia a eventos y señales contenidos en un paquete de eventos. El nombre de paquete y evento, separados por una barra inclinada ("/"), identifica el nombre del evento. La Tabla 3.6 enumera los paquetes básicos definidos en MGCP.

TABLA 3.6. PAQUETES BÁSICOS.

PAQUETE	NOMBRE
Paquete genérico de medios	G
Paquete DTMF	D
Paquete MF	M
Paquete de enlace troncal	T
Paquete de líneas	L
Paquete de microteléfono	H
Paquete RTP	R
Paquete de servidor de acceso de red	N
Paquete de servidor de avisos	A
Paquete de scripts	Script

Como se ha mencionado anteriormente, cada paquete contiene eventos y señales específicos relacionados con el tipo de punto final. Para cada evento se requiere la siguiente información:

- Descripción del evento, señal de usuario generada y resultado de usuario observado. Por ejemplo, un posible evento es una transición off-hook. Este evento ocurre cuando un usuario descuelga y detecta un tono de marcado.

- Definir las características del evento, como las frecuencias y amplitudes de las señales de audio.

- Duración del evento.

Las señales son divididas en los siguientes tipos dependiendo del comportamiento y acción requeridos:

- On/Off (00). Como resultado de un evento, estas señales se aplican hasta que son desactivadas.

- Time-Out (TO). Una vez que han sido aplicadas, estas señales permanecen hasta que son desactivadas o hasta que expira el tiempo sobre la base de un periodo de tiempo específico de señal.

- Brief (BR). La duración de la señal es corta y se detiene por sí misma.

Cada paquete contiene una serie específica de señales y eventos. La Tabla 3.7 muestra algunos ejemplos de eventos y de duración de la señal.

TABLA 3.7. EVENTOS Y SEÑALES.

Símbolo de evento	Definición	Duración de la señal
hd	Transición off-hook	OO
hu	Transición on-hook	OO
dl	Tono de marcado	TO (120s)
rg	Timbre	TO (30s)
hf	Flash hook	BR
bz	Tono de ocupado	OO
aw	Tono de respuesta	OO
wt	Tono llamada en espera	TO (30s)
ci (string)	ID del que llama	BR
mt	Detectado tono de módem	---
ft	Detectado tono de fax	---
cg	Tono de congestión de red	TO
it	Tono de interceptar	OO

wk	Parpadear	BR
wko	Dejar de parpadear	BR
dtmf8	Dígito 8 de DTMF	BR
mf 9	Dígito 9 de MF	BR
ann	Realizar un aviso	TO (var.)
java	Cargar un Script Java	TO (var.)

MGCP tiene recomendaciones específicas por las que los paquetes de eventos deben ser implementados en determinados tipos de punto final. Los tipos básicos de punto final, sus perfiles y paquetes soportados se resumen en la Tabla 3.8.

TABLA 3.8. TIPOS DE PUNTO FINAL.

GATEWAY	PAQUETES SOPORTADOS
Gateway de enlace troncal (ISUP)	G, D, T, R
Gateway de enlace troncal (MF)	G, M, D, T, R
Servidor de acceso a red (NAS)	G, M, T, N
Gateway NAS/VoIP	G, M, D, T, N, R
Gateway de acceso (VoIP)	G, D, M, R
Gateway de acceso (VoIP, NAS)	G, D, M, R
Gateway residencial	G, D, L, R
Servidor de avisos	A, R

3.2.2. Funciones de control

MGCP proporciona servicios de manejo de la conexión y manejo de punto final similares a SGCP. Sin embargo, MGCP modifica ligeramente las cinco primitivas de SGCP y agrega cuatro funciones adicionales, debido en gran parte a las contribuciones aportadas desde IPDC. Los siguientes nuevos comandos permiten las posibilidades de manejo de MGCP:

- Los agentes de llamadas emiten comandos Endpoint Configuration a los gateways identificando las características de codificación del lado de línea de un punto final.

➢ Los agentes de llamadas emiten comandos Notification Request a los gateways indicando qué eventos específicos deben ser identificados. A su vez, los gateways utilizan el comando Notify para informar a los agentes de llamadas sobre los eventos solicitados.

➢ Los agentes de llamadas utilizan los comandos Create Connection, Modtfy Connection y Delete Connection para establecer, cambiar y desconectar las conexiones y las llamadas.

➢ Los agentes de llamadas utilizan los comandos Audit. Endpoint y Audit. Connection para revisar el estado y las conexiones en el contexto de un punto final.

➢ Los gateways pueden emitir el comando Restartin-Progress para avisar al agente de llamadas sobre cuándo los puntos finales están fuera de servicio o están de nuevo en servicio.

La Tabla 3.9 presenta un resumen de los comandos de control y los códigos correspondientes.

TABLA 3.9. COMANDOS MGCP.

Comando	**Código**
EndpointConfiguration	EPCF
NotificationRequest	RQNT
Notify	NTFY
CreateConnection	CRCX
ModifyConnection	MDCX
DeleteConnection	DLCX
AuditEndpoint	AUEP
AuditConnection	AUCX
RestartIn-Progress	RSIP

a. Endpoint configuration

Los comandos Endpoint Configuration permiten que el agente de llamadas especifique las señales de codificación recibidas por el punto final. Este comando pasa esta información al gateway con estos dos parámetros:

- Endpoint ID (ID de punto final). Identifica el nombre del punto final en el gateway. Si se utiliza la totalidad de la convención de wildcard, este parámetro identifica todos los puntos finales que coinciden con el wildcard.

- Bearer Information (Información portador). Identifica la técnica de codificación para los datos recibidos en el lado de línea del punto final identificado.

b. Notification request

El comando Notification Request en MGCP difiere ligeramente de en SGCP, ya que contiene estos tres parámetros nuevos:

- Quarantine Handling (Manejo de la cuarentena). Un parámetro opcional que especifica si los eventos en cuarentena deben ser procesados o descartados o si se requiere una o múltiples notificaciones de esta petición. Un evento en cuarentena es un mecanismo para que MGCP ponga en la cola algunos eventos mientras que otro está siendo notificado al agente de llamadas.

- Detect Events (Detectar eventos). Un parámetro opcional que especifica la lista de eventos en cuarentena para su detección durante el periodo de cuarentena. Los posibles eventos para la detección incluyen la alerta de calidad. Un evento detectado es la detección que necesita realizarse durante una cuarentena.

- Embedded Endpoint Configuration (Configuración incrustada de punto final). Si está incrustado, este parámetro puede insertar los parámetros transportados después de la petición de notificación y puede especificar la técnica de codificación para el lado de línea del punto final.

c. Notify

El comando Notify es el mismo en MGCP que en SGCP. Los gateways utilizan este comando para avisar al agente de llamadas sobre los eventos.

d. Create connection

La versión de MGCP del comando CreateConnection tiene algunas modificaciones y parámetros adicionales con respecto a la versión SGCP. Estos tres parámetros subrayan las diferencias:

- Second Endpoint ID (Segundo ID de punto final). Utilizado en lugar del descriptor de conexión remota para crear una conexión entre dos puntos finales en el mismo gateway. Este comando especifica conexiones locales sobre planos traseros TDM residenciales o interconexiones de bus.

- Embedded Notification Request (Petición de notificación incrustada). Permite que el agente de llamadas transmita los eventos opcionales solicitados, identificador de petición. mapa de dígitos y peticiones de señal, así como que pueda manejar eventos en cuarentena y detectar parámetros de eventos dentro de la petición incrustada.

- Embedded Endpoint Configuration (Configuración de punto final incrustada). Inserta los parámetros transportados después de la petición de notificación y especifica la técnica de codificación para el lado de línea del punto final.

e. Modifyconnection

Los parámetros utilizados en el comando Modify Connection son los mismos que en el Create Connection.

f. Deleteconnection

El comando Delete Connection cae básicamente en el mismo tema que las demás peticiones, por lo que la configuración de punto final incrustada y la configuración de notificación incrustada aumentan el marco SGCP existente.

Como se ha indicado en la sección sobre SGCP de este capítulo, algunos datos estadísticos acompañan la respuesta al comando Delete Connection. La diferencia en MGCP está en el

registro de las estadísticas para conexiones ATM y de tipo local. Los campos de datos son los mismos; sin embargo, la explicación para las estadísticas de ATM y de base local es diferente, como indican las Tablas 3.10 y 3.11.

TABLA 3.10. INFORMACIÓN ESTADÍSTICA ATM: COMANDO DELETE CONNECTION DE MGCP.

Datos	Explicación-Conexión ATM
Paquetes enviados	Número total de celdas enviadas sobre la conexión ATM.
Octetos enviados	Número total de octetos de carga útil enviados en celdas ATM.
Paquetes recibidos	Número total de celdas recibidas en la conexión ATM.
Octetos recibidos	Número total de octetos de carga útil recibidos en celdas ATM.
Paquetes perdidos	Número total de celdas perdidas.
Fluctuación de fase	Fluctuación de fase interllegada entre celdas ATM.
Latencia	Sin determinar si este parámetro es viable.

TABLA 3.11. INFORMACIÓN ESTADÍSTICA LOCAL: COMANDO DELETE CONNECTION DE MGCP.

Datos	Explicación-Conexión local
Paquetes enviados	Sin relevancia.
Octetos enviados	Número total de octetos de carga útil enviados sobre la conexión local.
Paquetes recibidos	Sin relevancia.
Octetos recibidos	Número total de octetos recibidos sobre la conexión local.
Paquetes perdidos	Sin relevancia.
Fluctuación de fase	Sin relevancia.
Latencia	Sin relevancia.

g. Auditendpoint

El agente de llamadas puede utilizar el comando AuditEndpoint para determinar el estado de un punto final. Esta petición contiene un parámetro de Encipoint ID, que identifica el punto final que está siendo revisado, y un parámetro Requested Information, que contiene los siguientes subparámetros:

- Endpoint List (Lista de punto final). Identifica el punto final que está siendo revisado. Se puede utilizar la totalidad de la convención de wildcard para indicar todos los puntos finales que coinciden con el wildcard.

- Notified Entity (Entidad notificada). Entidad actualmente notificada para peticiones activas de notificación.

- Requested Events (Eventos solicitados). Lista de los eventos actualmente solicitados.

- Digit Map (Mapa de dígitos). Actualmente utilizados por un punto final.

- Signal Requests (Peticiones de señales). Lista de las peticiones de señales aplicadas al punto final.

- Request Identifier (Identificador de petición). La última petición de notificación recibida.

- Connection Identifiers (Identificadores de conexión). Lista de las conexiones actuales existentes para el punto final especificado.

- Detect Events (Detectar eventos). Lista de los eventos que están siendo detectados en un modo en cuarentena.

- Local Connection Options (Opciones de conexión local). Lista de todos los valores actuales, como códec y periodo de empaquetamiento. Se puede también utilizar este comando para pedir los paquetes de eventos soportados en el punto final especificado.

h. Auditconnection

Los agentes de llamadas utilizan el comando audit. Connection para recuperar información sobre las conexiones. Este comando contiene el ID de punto final y el ID de conexión que indican la ubicación y la conexión que se está revisando. Los subparámetros de Requested Information contienen la siguiente información:

- Call ID (ID de llamada). Identificador único de la llamada para la que se está revisando una de sus conexiones.
- Notified Entity (Entidad notificada). Entidad actualmente notificada para la conexión.
- Local Connection Options (Opciones de conexión local). Opciones proporcionadas para esta conexión.
- Mode (Modo). Modo actual de conexión.
- Remote Connection Descriptor (Descriptor de conexión remoto). Proporcionado al gateway para la conexión.
- Local Connection Descriptor (Descriptor de conexión local). El gateway utilizado para la conexión.
- Connection Parámetros (Parámetros de conexión). Valor actual de los parámetros de conexión para la conexión.

i. Restartiln-progress

El gateway utiliza el comando Restartln-Progress para informar al agente de llamadas que un punto final o grupo de puntos finales está fuera de servicio o vuelve a estar de servicio. El comando Restartln-Progress contiene los siguientes parámetros:

- Endpoint ID (ID de punto final). Identifica el punto final. Utilizando la totalidad de la convención de wildcard, identifica el grupo de puntos finales que está siendo puesto fuera de servicio o que vuelve a estar de servicio.

➢ Restart Method (Método de reinicio). Especifica uno de los tres tipos de reinicio. El método de reinicio elegante (gracefuld) indica que los puntos finales especificados estarán fuera de servicio después de un tiempo determinado y que el agente de llamadas no deberá intentar establecer nuevas conexiones. El método de reinicio forzado (forced) indica que los puntos finales han sido puestos fuera de servicio de manera abrupta y que se han perdido las conexiones. El método reinicio (restart) indica cuándo los puntos finales que no tienen conexiones existentes estarán de nuevo de servicio.

➢ Restart Delay (Retraso de reinicio). Utilizado para expresar el retraso en un número de segundos

3.2.3 Códigos de devolución y códigos de error

Las peticiones MGCP son confirmadas, y las respuestas contienen códigos de devolución y códigos de error similares a los de SGCP. La Tabla 3.12 indica los códigos idénticos a los de SGCP y los nuevos códigos específicos de MGCP.

TABLA 3.12. CÓDIGOS DE DEVOLUCIÓN Y DE ERROR DE MGCP.

CÓDIGO DE DEVOLUCIÓN	EXPLICACIÓN
200-514	Igual que en SGCP.
515	La transacción se refiere a un ID de conexión incorrecto.
516	La transacción se refiere a un ID de llamada desconocido.
517	Modo no soportado.
518	Paquete de eventos no soportado.
519	El gateway no tiene un mapa de dígitos.
520	Incapaz de completar la transacción debido al reinicio del punto final.
522	No existe dicho evento o señal.
523	Acción o combinación de acciones desconocidas.
524	Incoherente con las opciones de conexión local.

CAPÍTULO IV
CONTROLADOR DE SWITCH VIRTUAL

4.1. Concepto

El concepto de switch virtual se basa en las redes de voz actuales que se están moviendo desde una infraestructura de multiplexión por división de tiempo (TDM) a una nueva infraestructura de servicios de voz basada en paquetes.

Esta nueva infraestructura consta de los siguientes elementos de red distribuidos:

- Gateways de medios (MG).
- Redes de paquetes.
- Señalización, servicios y control de llamadas.
- Suministro y administración de servicios.

El conjunto de estos elementos constituye un switch virtual, donde la intercomunicación se lleva a cabo utilizando protocolos abiertos basados en estándares. El VSC de Cisco proporciona las funciones de control de llamadas del switch virtual.

Utilizando las analogías de switches TDM existentes, el VSC implementa las funciones de los componentes de software encontrados en un Punto de switching de servicios (SSP, Service Switching Point). Otros términos equivalentes a VSC incluyen el Controlador de gateway de medios (MGC, Media Gateway Controller), el agente de llamadas, el switch blando (soft-switch) y el SSP basado en software.

4.2. Visión general del switch virtual

El concepto de switch virtual desarrolla el paradigma actual de switches TDM en una arquitectura distribuida. Este concepto se realiza mediante de la utilización de:

- Métodos de acceso multiservicio basado en paquetes, equivalente alas tarjetas de línea de la Red pública de telefonía conmutada (PSTN).

- Redes de switching portadoras de paquetes distribuidas: son análogas a la estructura de switch TDM.

- Servidores de control de llamadas VSC, similar a la funcionalidad SSP.

Sin embargo, además de las funciones que se encuentran habitualmente en un SSP, el VSC agrega más competencias, que abastecen a aplicaciones como H.323 y el Protocolo de inicio de la sesión (SIP). El VSC actúa en un entorno UNIX con la idea de proporcionar a los clientes un alto grado de interfaces abiertas y programabilidad. La realización del switch virtual de Cisco es un componente de la arquitectura Open Packet Telephony (OPT, Telefonía de paquetes abierta).

4.3. Telefonía de paquetes abierta

La arquitectura de Telefonía de paquetes abierta (OPT) de Cisco se basa en la creación de tres planos lógicos: control de conexión, control de llamadas y servicios. Cada plano representa un aspecto funcional diferente de un servicio de voz e interactúa con los otros planos lógicos a través de interfaces abiertas bien definidas. Los tres planos están organizados jerárquicamente, con el control de conexión en el nivel más bajo, el control de llamadas encima del control de conexión y los servicios encima del control de llamadas. La figura 4.1 nos ilustra la composición funcional de la arquitectura OPT.

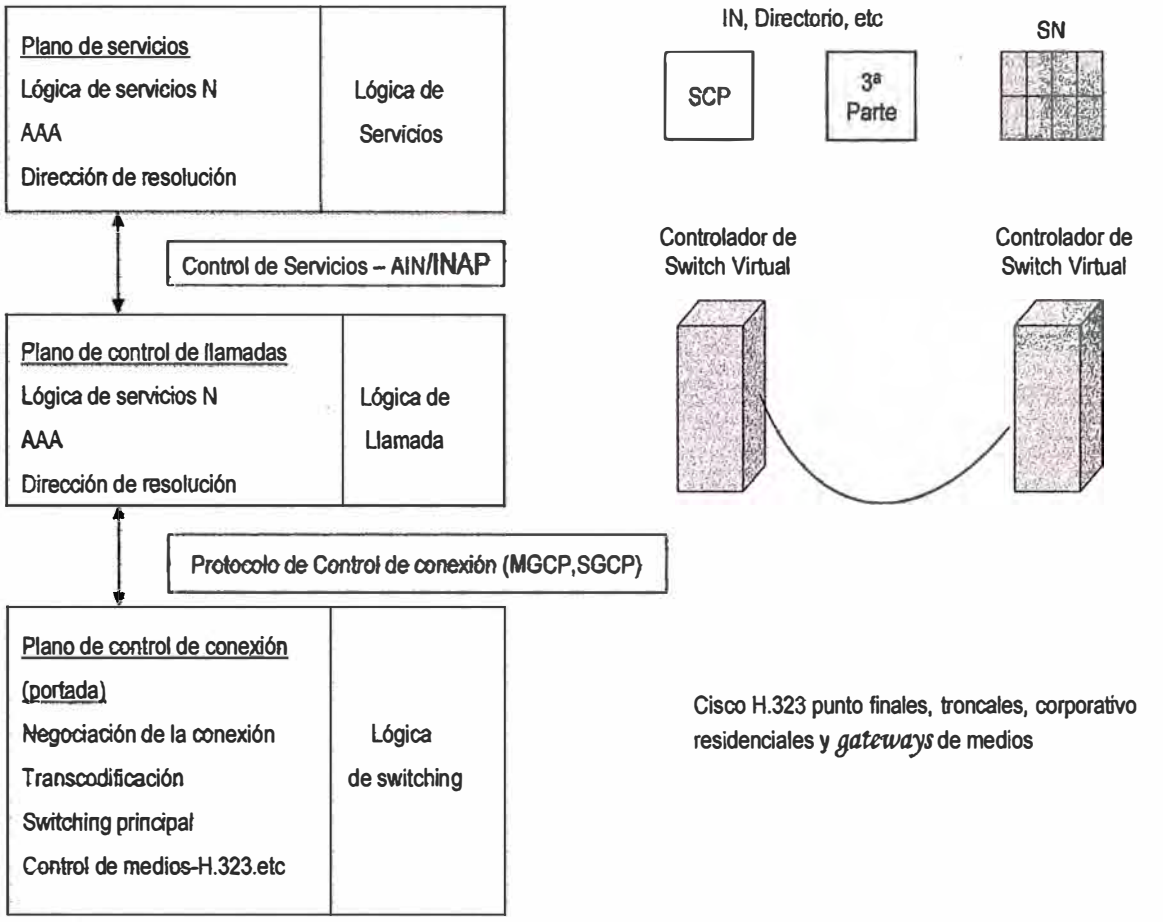

Figura 4.1. Arquitectuta de telefonia de paquetes abierta

El VSC proporciona las siguientes funciones de plano de control dé llamadas en la arquitectura OPT de Cisco (en la arquitectura del Media Gateway Control Protocol [MGCP], el VSC representa al MGC):

- El plano de control principal o de conexión abarca la funcionalidad necesaria para configurar, mantener y borrar rutas de voz a través de la red de paquetes. Los AS5300, MGX8850 y 8260, 2600, 3600, 3810 y uBR924 de Cisco se conocen como MG (gateways de medios). El plano de control de conexión comunica con el plano de control de llamadas utilizando un protocolo de control estándar de la industria, como el Protocolo de control de gateway simple (SGCP) o MGCP.

El plano de control de llamadas incluye la funcionalidad necesaria para señalizar, procesar y enrutar llamadas de voz y datos sobre la red de paquetes. Las funciones dentro de esta capa se acercan a las que se encuentran en la lógica del procesamiento de llamada de un switch TDM existente. Las funciones típicas del plano de control de llamadas incluyen el protocolo del Sistema de señalización 7 (SS7), el análisis y manipulación de dígitos, la selección de la ruta, el seguimiento, las funciones basadas en switch y la comunicación con programas lógicos de servicios externos.

➢ El plano de control de llamadas comunica con el plano de control de conexión utilizando MGCP o SGCP. El intento arquitectónico de esta interfaz es separar limpiamente el control de conexión del control de llamadas de tal manera que el plano de control de llamadas sea independiente (e inconsciente) del transporte de paquete de voz subyacente. Esto permite que se utilice el mismo plano dé control de llamadas con MG orientado a la Capa 3 (Protocolo Internet [IP]) o a la Capa 2 (Modo de transferencia asíncrona/Frame Relay [ATM/FR]).

La capa de control de llamadas también comunica con el plano de servicios para proporcionar servicios flexibles mejorados. Esta interfaz es típicamente un protocolo de red inteligente (IN) basado en estándares que funciona sobre TCAP (Parte de la aplicación de posibilidades de transacción) de SS7, a pesar de que existen muchas variantes y extensiones propietarias de los distintos fabricantes.

➢ El plano de servicios abarca la lógica necesaria para proporcionar servicios residentes nonswitch mejorados. Se pueden realizar dichas funciones con los puntos de control de servicio (SCP) o nodos de servicio.

Cuando se utilizan los SCP, el plano de control de llamadas señala el SCP utilizando la red de inteligencia avanzada (AIN, Advanced Intelligent Network), o el protocolo IN sobre TCAP de SS7. Las aplicaciones SCP típicas incluyen la conversión de número (800#), la autenticación del código de cuenta, la validación de la tarjeta de crédito y las redes privadas virtuales (VPN, Virtual Private Network).

Cuando utiliza los nodos de servicios, el VSC enruta normalmente una llamada al nodo de servicios para el procesamiento. El nodo de servicios aplica luego su propio tratamiento de la función específico a la voz y flujo de datos, y completa el enrutamiento de llamadas al destino deseado. Dependiendo de la función, el nodo de servicios puede permanecer en la

ruta de la llamada o dar el control de la llamada de nuevo al VSC. Las aplicaciones típicas de nodo de servicios incluyen correo de voz, la tarjeta de débito y la marcación por voz.

4.4. Visión general de la red de voz por paquetes

VSC proporciona una capacidad de control de llamadas para la siguiente generación de redes. Controla cómo un tráfico de voz TDM de banda estrecha es consolidado sobre la infraestructura de paquetes y de qué maneras se pueden aplicar los servicios a esas llamadas. Se puede utilizar el VSC en una variedad de aplicaciones para proporcionar funciones de control de llamadas. Los ejemplos de las aplicaciones habilitadas en la arquitectura de la red de voz por paquetes incluyen lo siguiente:

- Aplicaciones tándem de carrier de intercambio de voz por paquetes (IXC).
- Aplicaciones de clase 4 del carrier de intercambio local (LEC) de voz por paquetes.
- Aplicaciones multimedia de cliente de punto de terminación.
- Servicios de voz corporativos dentro de red y fuera de red.
- Aplicaciones de oficina final u oficina local de Voz sobre IP (VoIP) en infraestructura de cable.

La figura 4.2 nos describe una aplicación de voz por paquetes genérica e ilustra varios componentes arquitectónicos y la manera que tienen de interactuar unos con otros.

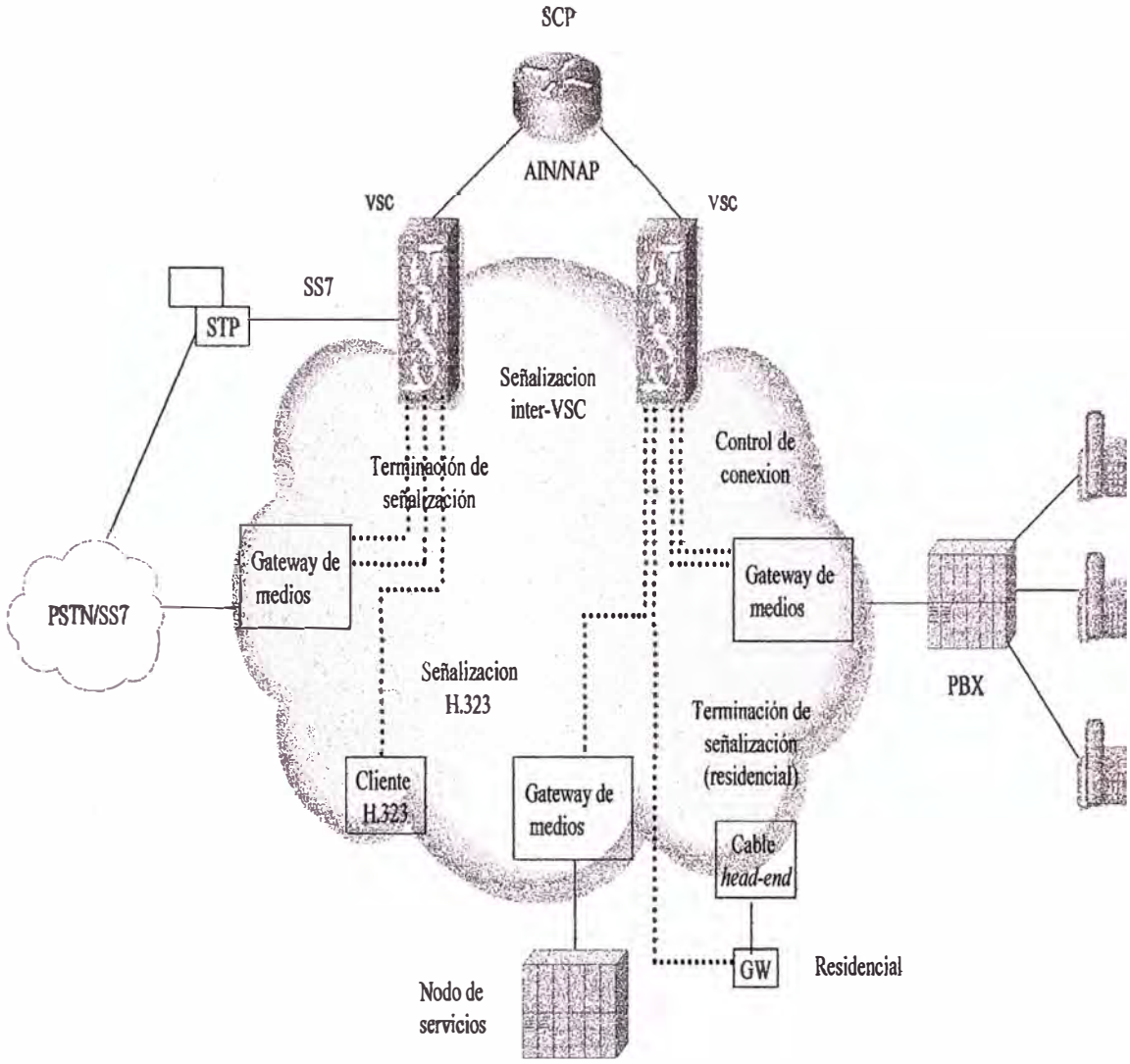

Figura 4.2. Arquitectura de red de voz por paquetes

4.4.1. Elementos de red

Esta sección revisa cada elemento de red en el dibujo. Entre ellos se incluyen los siguientes:

- VSC.
- MG.
- SCP.
- Nodo de servicios.
- Cable head end.
- Gateway residencial.
- Punto final/ cliente. H.323.

a. Controlador de switch virtual

En el nivel alto, el Controlador de switch virtual (VSC) proporciona las siguientes capacidades principales:

- Procesamiento de la señal de llamada, incluido el nivel 3 de la red digital de servicios integrados (ISDN) (Q.931), el nivel o de SS7 (Parte de usuario de ISDN JISUPJ), señalización H.323 asociada a canal multifrecuencia (MF/CAS), así como señalización de llamada hacia dispositivos ubicados en gateways residenciales conectados a través de cable o de un equipo terminal de abonado (CPE, Customer Premise Equipment) de una línea de abonado digital (DSL).

También incluye la posibilidad de traducir entre diferentes tipos de señalizaciones en distintos establecimientos de llamadas.

➢ Resolución de direcciones, enrutamiento de llamadas, administración de recursos, control de conexión y generación del Registro detallado de llamadas (CDR, Call Detail Record).

➢ Funciones de acceso a los servicios para acceder a servicios que se ejecutan en plataformas de servidores externos (como SCP o nodo de servicios).

➢ Interfaces de administración que utilizan el protocolo SNMP para errores, rendimiento y configuración; herramientas de configuración basadas en la Web y sistema de administración de elementos

b. Gateway de medios

El gateway de medios (MG, Media Gateway) lleva a cabo las siguientes funciones de alto nivel:

➢ Terminación física de la instalación TI /El TDM desde la PSTN o PBX (Private Branch eXchanges).

➢ Comunicación con el VSC para la configuración y borrado de la llamada utilizando SGCP o MGCP.

➢ Cancelación de eco en la red de circuito conmutado.

➢ Equilibrado de los búferes de fluctuación de fase.

➢ Detección de actividad de voz (VAD), como la supresión de silencio y la generación de ruido de apaciguamiento

➢ Compresión de voz utilizando las recomendaciones de la Unión internacional de las telecomunicaciones (ITU), como G.711, G.723.1, y G.729.

➢ Generación de tono, que genera los tonos de marcado, ocupado, ring-back y congestión.

➢ Transporte de marcación multifrecuencia (DTMF), que permite la utilización de touch tones para aplicaciones de correo de voz con códecs que soportan la detección y transporte DTMF.

c. Punto de control de servicio

El SCP (punto de control de servicio) proporciona el entorno de ejecución para la lógica del servicio.

El SCP es responsable de procesar las peticiones de transacción y de devolver una respuesta. Una petición de transacción típica en el mundo de la voz es una conversión de número.

Ejemplos de este tipo de servicio incluyen el servicio 800 (toll free) y la portabilidad del número local (LNP, Local Number Portability). Una aplicación toll free (gratuita) que se ejecuta en el SCP tiene una lógica sofisticada que permite que el usuario final controle cómo están enrutadas las llamadas entrantes.

Se puede basar el enrutamiento de llamadas toll free en un número marcado, la hora del día, el día de la semana, el punto geográfico de origen e incluso en cuán ocupada puede estar una distribución de llamadas automática de terminación en un momento dado. Los clientes o el proveedor de servicios (SP) pueden ser propietarios del SCP.

a. Nodo de servicios

El componente de nodo de servicios de la arquitectura de voz de Cisco se ha realizado por un switch programable abierto del VCO de Cisco. El VCO/4k es modular y escalable. Incorpora software genérico compatible, interfaces de red universales y recursos de servicios; también emplea tecnologías avanzadas, como SS7, ISDN (RDSI), control de llamadas jerárquico y administración de la red SNMP. Además, los VCO/4k son compatibles con la oficina central (CO) y se pueden desplegar en entornos completamente redundantes o no redundantes.

e. Cable head end

El router universal de banda ancha (Universal Broadband Router) es un sistema de terminación cable-módem integrado (CMTS, integrated cable modem termínation system) y un router de la serie 7200 de Cisco que utiliza tarjetas de línea de radiofrecuencia (RF). El Universal Broadband Router proporciona una única solución integrada con funcionalidad CMTS, la capacidad de terminar el protocolo Especificaciones de servicios de interfaz de datos sobre cable (DOCSIS, Data-over-Cable Service Interface Specifications) y la capacidad de realizar todas las funciones de enrutamiento de datos requeridas. La instanciación de este componente también incluye un multiplexor de línea digital de abonado (DSLAM, Digital Subscriber Line Multiplexer).

f. Gateway residencial

El gateway residencial es un dispositivo de equipo terminal del abonado (CPE) de voz y datos que proporciona entre dos y cuatro puertos de capacidad de Servicio telefónico analógico convencional (POTS, plain old Telephone Service). El dispositivo ejecuta el protocolo DOCSIS para proporcionar paquetes de datos y servicios de telefonía sobre el cable coaxial híbrido (HFC) al CMTS. Otro ejemplo de este componente también incluye un módem DSL.

g. Punto final/cliente h.323.

El cliente H.323 representa una amplia gama de aplicaciones de voz y multimedia que son alojadas de manera nativa en la red IP. El punto final H.323 se explica con más detalle en el Capítulo I, "H.323".

4.4.2. Interfases de red

En la figura 4.3 observamos las cuatro principales interfaces de red VSC que son la terminación de señalización, la señalización inter-VSC, el control de conexión y el control de servicios.

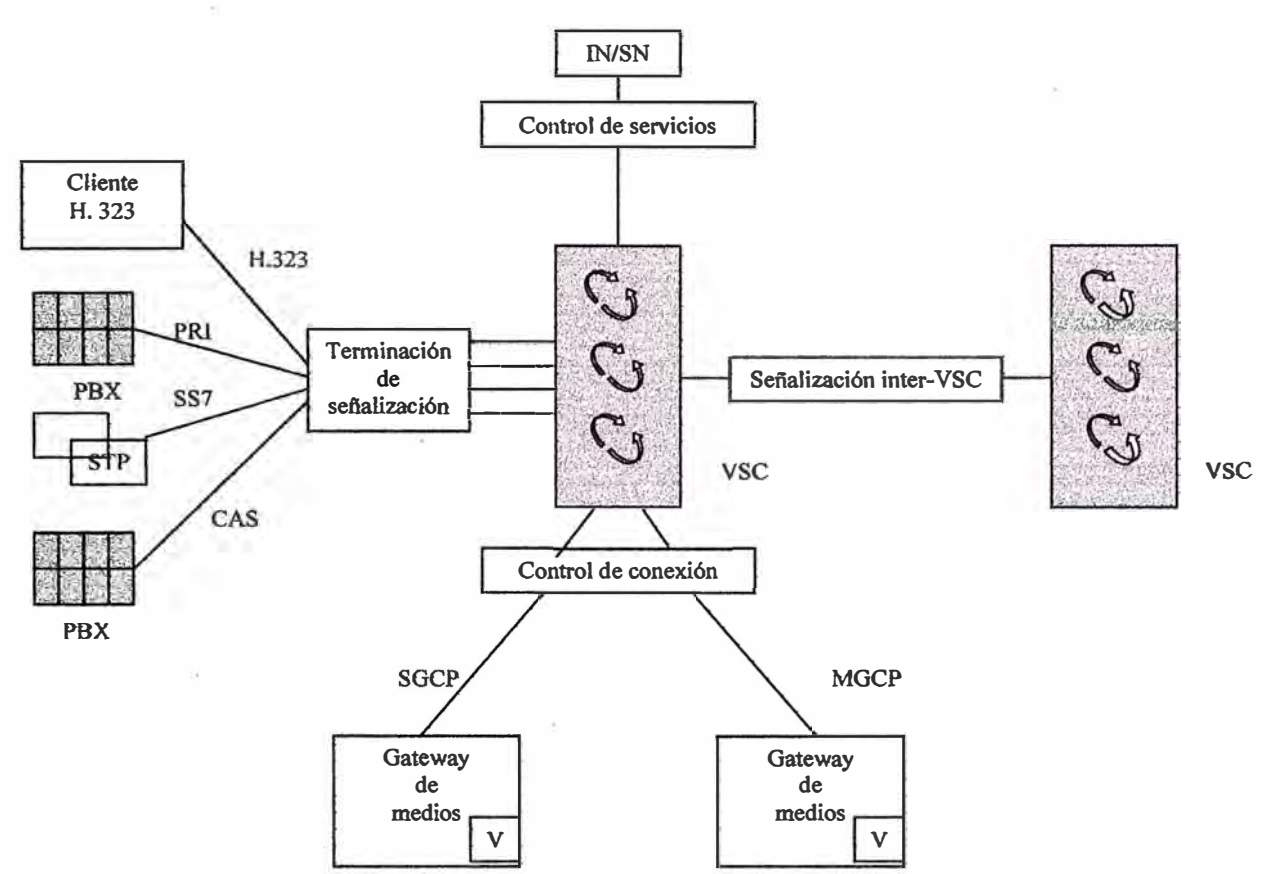

Figura 4.3. Interfases de Red

a. Terminación de señalización

La capacidad de terminación de señalización permite que VSC medie entre muchas variantes de señalización como SS7, interfaz de acceso principal (PRI, Primary Rate Interface), CAS y H.323, para citar sólo unas cuantas.

a.1. Enlaces ss7

Están disponibles varios mecanismos para terminar el tráfico de señalización SS7 en el VSC.

➢ Señalización no asociada (Enlaces A). Se termina directamente en el VSC utilizando una interfaz física V.35 o una TI /El. De manera opcional, para incrementar las características de fiabilidad, se puede configurar un conjunto de terminales de enlaces de señalización (SLT, Signaling Link Terminals) para manejar las capas bajas de SS7. Las

SLT se implementan utilizando los routers de la serie 2600 de Cisco que hacen frente a los servidores Sun que alojan la aplicación VSC.

➢ Señalización completamente asociada (Enlaces F). Transportan tráfico principal y están terminadas en el gateway de paquetes. El gateway de paquetes es responsable de ejecutar las partes 1 y 2 del mensaje de transferencia (MTP), encapsular la capa 3 de las unidades de datos del protocolo MTP (MTP L3) y de enviarlas al VSC para el procesamiento de MTP L3 y ISUP. El transporte entre el gateway de paquetes y el VSC se lleva a cabo utilizando el Protocolo de datos de usuario fiable (RUDP, Reliable User Data Protocol), una estrecha capa de fiabilidad en la parte superior del Protocolo de datos de usuario (UDP, User Data Protocol).

a.2. Enlaces pri

Los enlaces PRI transportan un canal D y terminan directamente en el gateway de voz. Los periféricos del gateway de voz ejecutan la capa 1(L1) y la capa 2 (L2), las capas más bajas de la interfaz PRI (Q921). La capa 3 (L3; Q.931) se encapsula en el paquete RUDP y se envía al VSC para el procesamiento de la llamada

a.3. Enlaces cas

Los enlaces CAS terminan directamente en el gateway de voz. Los protocolos CAS de bajo nivel (por ejemplo, la señalización de dirección y línea) se manejan desde la periferia del gateway. Se puede utilizar una API CAS para reunir los eventos del procesamiento de llamada sobre la IP al VSC para el manejo de la llamada.

a.4. H.323

VSC maneja las peticiones a nivel de prellamada de Registro, admisión y estado (RAS, Registration, Admissions, and Status), así como las peticiones a nivel de llamada Q.931 originadas desde los clientes H.323. Esta terminación de señalización sigue los procedimientos de entrega descritos en el estándar H.323. En otras palabras, el VSC tiene capacidades H.225 RAS/Q.931; sin embargo, no tiene la funcionalidad de gatekeeper H.323.

b. Señalización inter-vsc

El protocolo VSC a VSC escala la red distribuyendo el control sobre múltiples plataformas VSC. Un protocolo ISUP modificado, llamado ISUP mejorado (E-ISUP, Enhanced ISUP) intercambia información de control de llamadas entre los VSC sobre una red IP utilizando el protocolo RUDP. La información MTP no es necesaria y, por tanto, tampoco es transportada.

Los mensajes E-ISUP también transportan elementos del Protocolo de descripción de la sesión (SDP, Session Description Protocol) en elementos de información de dígitos genérica ISUP, que utiliza VSC para especificar los atributos de conexión en SGCP y MGCP

c. Control de conexión: sgcp/mgcp

Las conexiones de voz de extremo a extremo en la red de paquetes se establecen utilizando SGCP o MGCP, un mecanismo abierto para configurar las conexiones en las redes IP. SGCP y MGCP son protocolos de transacción basados en UDP que permiten la manipulación de las conexiones representadas por puntos finales físicos o lógicos. Las conexiones se describen utilizando atributos como direcciones IP, códecs, etc. SGCP y MGCP administran las peticiones de configuración de llamada desde los teléfonos conectados hasta los gateways, como el cable o módems DSL. SGCP/MGCP proporciona un mecanismo para especificar el historial enviado por el VSC al gateway residencial dándole instrucciones de cómo difundir los eventos de voz.

El VSC también soporta una interfaz de switch virtual (VSI, Virtual Switch Interface) en el switch de área amplia del BPX de Cisco. La VSI es una interfaz definida de Cisco que permite un dispositivo exterior para controlar un conmutador de área ancha de BPX de Cisco. Al igual que el controlador, el VSC implementa la funcionalidad principal de la VSI. El VSC revisa las conexiones actuales en el PBX frente a las conexiones actuales en el VSC. La interfaz subyacente entre el VSC y el PBX es la capa 5 de adaptación ATM (AAL5).

En VSI, el controlador (el VSC) solícita que el switch (el PBX) cree, delegue y cambie conexiones. Se requiere el switch para notificar al controlador de cambios su estado de sincronización (ID de sesión activa) y/o los cambios en sus interfaces lógicas (cambios de carga, cambios de estado, etc.).

d. Control de servicios

El acceso a los servicios puede seguir dos caminos:

➢ Plataformas IN (AIN/INAP/subcapa de convergencia-1 [CS-1]) como la interfaz SCP inicialmente sobre interfaces AIN/INAP basadas en estándares transportadas sobre la red SS7, con migración futura a un transporte basado en IP.

➢ Servicios de nodo de servicios (como tarjetas de llamada y correo de voz) inicialmente conectados sobre interfaces TDM PRI. En el futuro, las plataformas de nodo de servicios harán una transición a las redes IP para evitar un interworking de redes TDM/IP innecesario.

4.4.3. Arquitectura y operaciones vsc

En la figura 4.4 se describe los principales bloques fimcionales de la plataforma VSC de Cisco

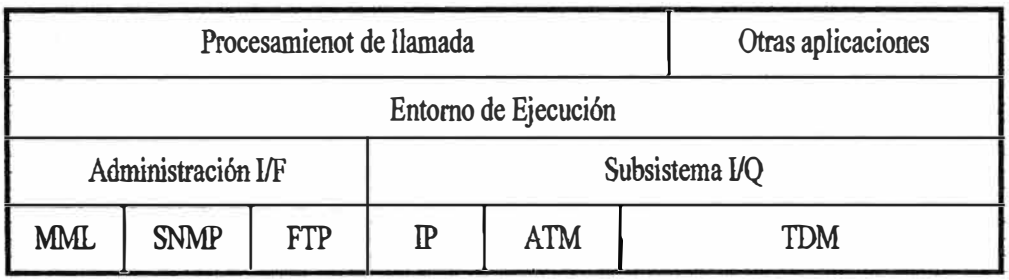

Figura 4.4. Comprobantes funcionales del VSC

El VSC de Cisco es una plataforma abierta y está construido para alojar terceras aplicaciones desarrolladas a través de un conjunto de herramientas de construcción de protocolo / aplicación potentes y API asociadas.

Entre estas herramientas se incluyen:

➢ Un conjunto de herramientas (toolkit) de la aplicación. Permite que los usuarios personalicen los protocolos y sus funciones de interworking. El toolkit también proporciona

potentes herramientas de lenguaje y una API para desarrollar aplicaciones state-and event-driven que residen en la plataforma VSC.

➢ Analizador de conversión. Genera informes de salida utilizando el rastreo en el motor de interworking. La información del informe incluye la entrada, conversión y salida del mensaje.

➢ Simulador. El simulador permite que los usuarios creen conjuntos de mensajes y los ejecuten a través de un motor de interuorking reflejado para determinar/diagnosticar errores de aplicación o de protocolo. Los informes detallados incluyen la entrada, conversión y salida del mensaje.

4.4.4. Protocolos soportados por vsc

Una de las mejores características de VSC es el hecho de que su arquitectura soporta múltiples protocolos de acceso y de red. Los nuevos protocolos y variaciones de los protocolos existentes siguen añadiéndose a la biblioteca. La Tabla 4.1 aporta una amplia lista de protocolos.

TABLA 4.1. PROTOCOLOS SOPORTADOS POR VSC.

ANSI ISUP (SS7)	ITU Q.931 PRI	ISUP Q761 belga
BTNUP	ETSI ISUP V2	Alcatel 4400 PRI
BTNUP	NRC ETSI Q.SIG	NI-2 (Bell-1268)
TUP chino	ITU Q.767ISUP	NI-2 + (Bell-1268-C3)
DNPSS	ISUP francés	ISUP polaco
ISUP holandés	ISUP alemán	ISUP Q761 finlandés
ETSI PRI	ISUP Q761 de Hong Kong	ISUP Q761 australiano

4.4.5. Entorno de ejecución

El entorno de ejecución (XE, Execution Environment) proporciona servicios comunes a programas de aplicación que se ejecutan en el host de señalización. Las principales metas del XE son las siguientes:

- Proporciona programas de aplicación con una infraestructura flexible, estable y coherente.

- Permite que las nuevas aplicaciones sean integradas más fácilmente con aplicaciones existentes que se ejecutan en la misma plataforma.

- Minimiza la cantidad de trabajo que los desarrolladores de la aplicación deben hacer para crear una aplicación nueva.

- Proporciona una interfaz simplificada a los servicios del sistema operativo, de forma que terceras partes pueden desarrollar aplicaciones personalizadas que pueden funcionar en un proceso en el VSC.

Los servicios proporcionados por el XE incluyen los siguientes:

- Administración de procesos. Permite que los procesos sean administrados por el XE. Esto incluye el arranque, parada y monitorización ordenada del proceso. La administración del proceso se utiliza también para implementar el cut-over (puesta en servicio) hacia una nueva versión de un proceso con una mínima interrupción del servicio.

- Alarmas. Permiten que los procesos registren, definan y limpien las alarmas. Los procesos de configurar y limpiar las alarmas son automáticamente registrados en los procesos que requieren este servicio. Se puede utilizar esta posibilidad para reportar alarmas a interfaces de administración enlazadas, permitiendo dichos procesos para implementar una acción de recuperación necesaria.

- Registros (logs). Permite que un proceso registre mensajes para archivos de registro compartidos, basados en un nivel de rigor de registro y la facilidad.

- Estadísticas. Permite que el proceso actualice los contadores compartidos que se están utilizando para los informes y las alarmas. Las alarmas basadas en contadores compartidos son automáticamente generadas en nombre de todos los procesos en la plataforma. Los informes de mediciones son automáticamente generados a intervalos de tiempo periódicos.

- Administración de comandos. Permite que los procesos intercambien comandos y respuestas. Este servicio se utiliza también para proporcionar una interfaz unificada para el motor de conversión del protocolo y/o para sistemas externos que controlan o monitorizan la plataforma XE a través de una interfaz de administración (como TransPath Man-Machine Language [MML]).

- Administración de configuración. Permite que un proceso sea notificado cuando cambian los datos de la configuración. Coordina una reconfiguración dinámica a través de todos los procesos en la plataforma.

- Control de acceso. Asegura que los servicios de la plataforma son proporcionados únicamente a aquellos procesos que están autorizados a utilizarlos.

- Shell de proceso. Proporciona un marco utilizado por los procesos para comunicar con los servicios aportados bajo el XE. Presenta un mecanismo de expedición de evento uniforme, soporte para una comunicación inter-procesos (IPC), temporizadores y señales, así como un conjunto de clases de fundación para el desarrollo de las aplicaciones.

- IPC. Permite que los procesos dentro de la plataforma intercambien mensajes.

- Manejo de la señal. Proporciona una interfaz para condiciones señalizadas a través del sistema operativo.

4.4.6. Plan de numeración de américa del norte (nanp)

El VSC puede manejar el Plan de numeración de América del Norte (NANP, North American Numbering Plan) presentado a un tándem de acceso o red IXC:

- Servicios de operador (0-, 0+, 00) con o sin 10XXX o 101XXXX enrutados a la numeración de América del Norte (NXX-XXXX o NPA-NXX-XXXX) o a la numeración internacional (CC+NN-nodo de red NN).

- Llamadas con o sin 10XXX o 101XXXX enrutadas a la numeración de América del Norte (NXX-XXXX o NPA-NXX-XXXX) o a la numeración internacional (CC+NN).

- Soporte para indicador de final de numeración #. Esto permite que los que llaman pulsen # para indicar al switch que debe dejar de esperar otro digito antes de procesar el número marcado.

- Llamada a carriers por método de corte (10XXX+# o 101XXXX+#).

- Soporte para números de formato 950-XXXX (ambos tipos de direcciones [NOA]).

- Conversión de números NXX-XXXX a números NPA-NXX-XXXX. Soporte para triggers de IN (red inteligente) (toll free, servicio premium y LNP).

4.4.7. Análisis de la ruta

El enrutamiento de llamadas VSC se realiza desde el MG de ingreso hasta el MG de salida apropiado. El enrutamiento de llamadas no se refiere al enrutamiento de paquetes dentro del ámbito de paquetes; la capa de control de conexión maneja eso.

Si los MG de origen y terminación están controlados por el mismo VSC, el enrutamiento de llamadas tiene lugar dentro del VSC.
Si el gateway de salida está controlado por un VSC diferente, ambos VSC se ven involucrados en el enrutamiento de llamadas. El VSC de origen analiza el mensaje de petición de llamada, como un mensaje inicial de dirección SS7 (IAM, Initial Address Message), y selecciona una ruta para alcanzar el gateway de salida o VSC de terminación que sirve al gateway de salida. El análisis de la ruta selecciona una de estas posibilidades:

- Un hop-off o gateway de salida conectado al grupo troncal seleccionado.

- La dirección IP del VSC de terminación que determina el gateway de salida.

- El gateway residencial.

- Una conexión hair-pinned en el gateway de ingreso hacia la red de origen.

Si se necesitan dos VSC, el VSC de origen utiliza E-ISUP para comunicar con el VSC de terminación y realizar la configuración de la llamada.

En la siguiente figura 4.5 nos ilustra el desbordamiento de congestión principal y secundaria, tal como determina el proceso de selección de ruta.

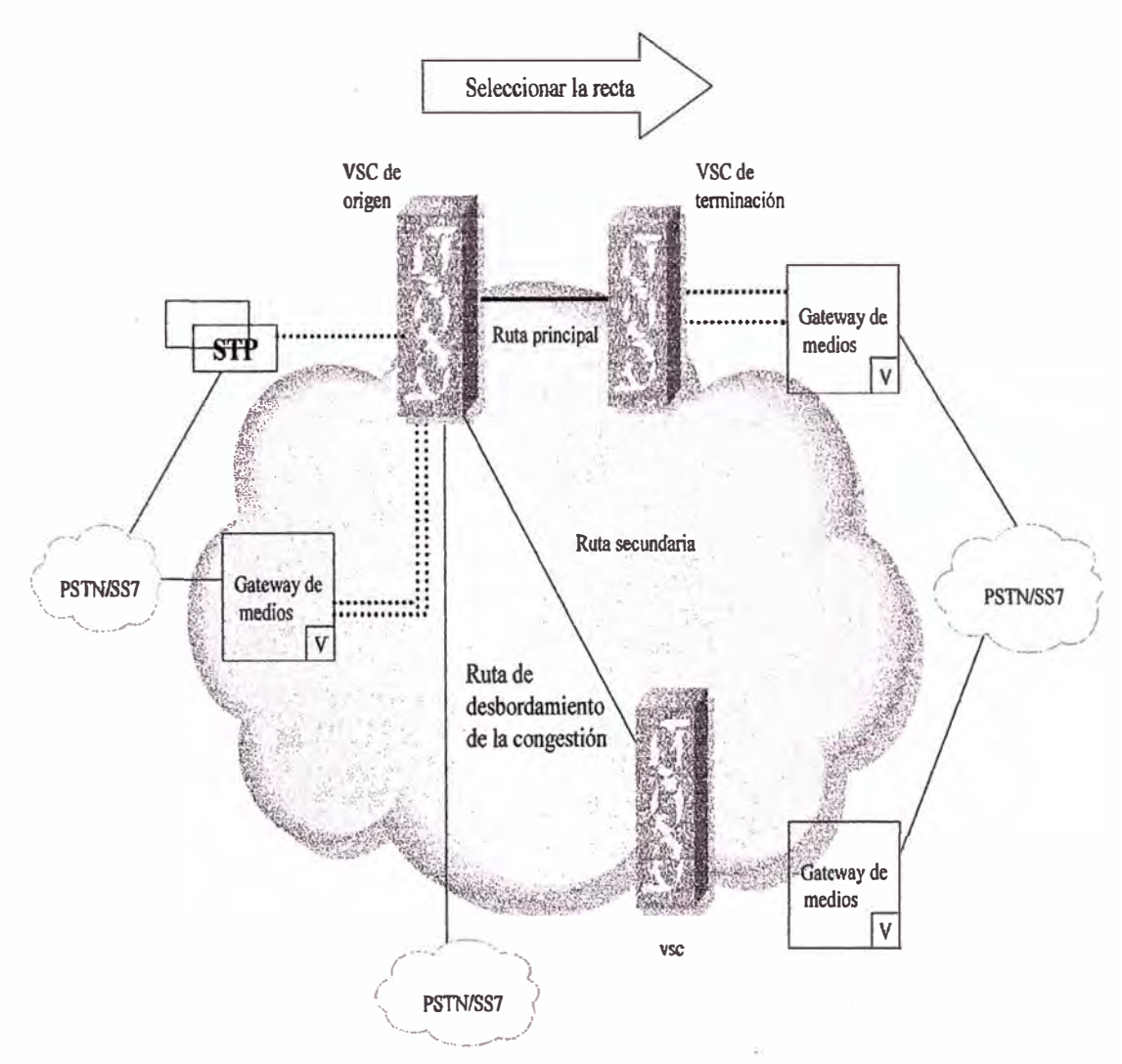

Figura 4.5. Proceso de selección de ruta

4.4.8. Análisis de dígito

El VSC lleva a cabo un análisis de dígito y función de ocultación frente a números A o B (triggers LNP y AIN /INAP). El número marcado o convertido selecciona la ruta, y el VSC de terminación es responsable de seleccionar el gateway de salida. La selección se realiza primero por un análisis de dígito y selección de los gateways hop-off preferidos (como los grupos troncales). Luego, con el manejo ocupado/ desocupado en los recursos del gateway de terminación, seleccionando un circuito saliente en la interfaz TDM y, finalmente, invocando los procedimientos de señalización apropiados (SUP IAM) hacia los switches PSTN de terminación.

En la figura 4.6 notamos el proceso de sección de gateway de salida

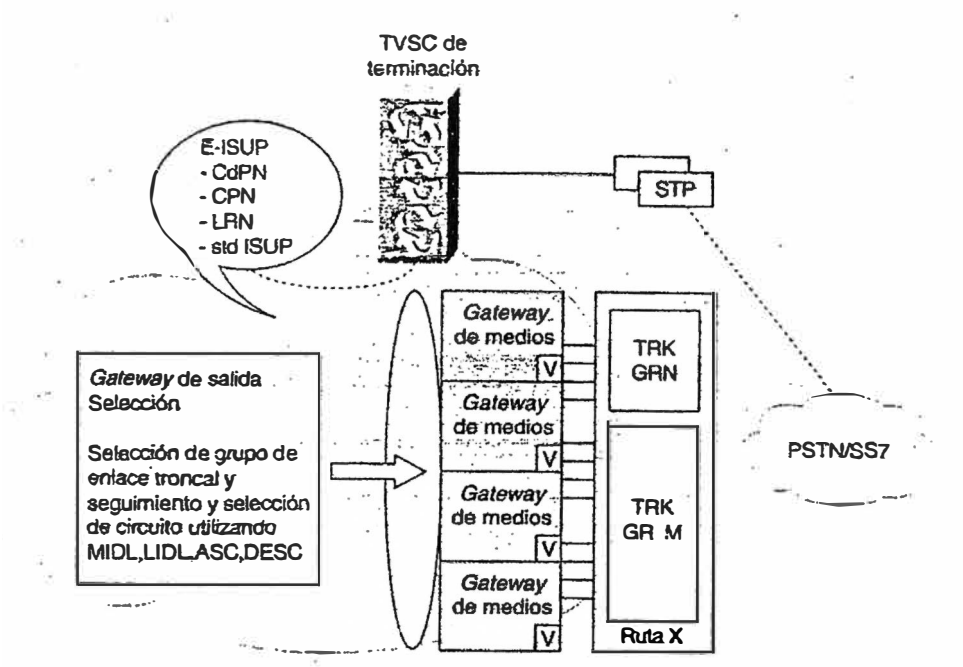

Figura 4.6. Selección de gateway de salida

4.4.9. Reenrutamiento en congestión

El VSC contiene el estado de los enlaces troncales conectados a los gateways de salida (ocupado/ desocupado) que VSC controla.

Si un gateway de salida no puede completar una llamada debido a un error de recurso interno, se envía una indicación explícita de vuelta al VSC con un reconocimiento MGCP/SGCP negativo.

El VSC puede entonces elegir otra ruta para realizar la llamada.

Si están involucrados dos VSC, el VSC de terminación informa al VSC de origen utilizando E-ISUP (Release [REL] con congestión) y se intenta un reenrutamiento de la llamada si se facilitaran rutas alternativas.

4.5. Implementación de vsc

El VSC puede proporcionar un alto nivel de disponibilidad igual a o mejor que un switch tradicional. El sistema en la figura 4.7 se basa en plataformas tolerantes a errores de Sun, que constan de una unidad activa y de reserva y un conjunto separado de SLT utilizado para terminar el tráfico SS7. La información del estado de la llamada se copia desde la unidad activa hasta la unidad de reserva. Este proceso se llama también check-pointing y asegura que las llamadas estables (respondidas) no se pierden en el paso de un VSC activo a otro de reserva. Los SLT terminan el tráfico MTP L2 y envían la información MTP L3 a la unidad activa.

Un análisis preliminar indica una disponibilidad combinada del sistema de 0,9999985 ó 0,782 minutos de inactividad por año.

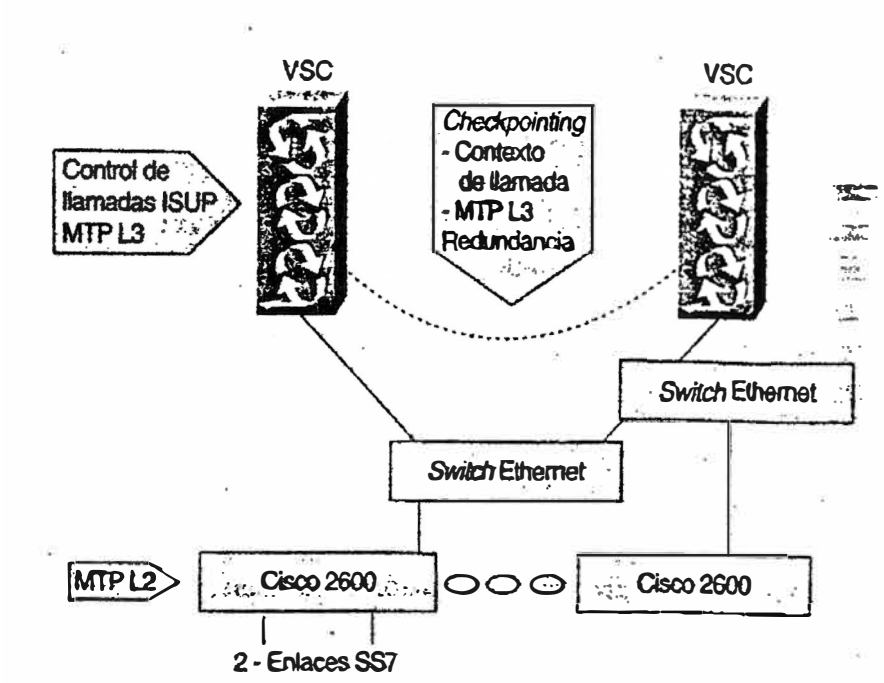

Figura 4.7. Implementación VSC

Para maximizar la tolerancia a fallos de VSC, el tráfico MTP L2 se termina en plataformas de hardware separadas y el tráfico MTP L3 se transmite a través de switches Ethernet dobles. Este nivel de redundancia permite que los sistemas activo y de reserva compartan los enlaces SS7 y las redes de área local/redes de área amplia (LAN/WAN). Cisco 2600 es el primer router que soporta la funcionalidad SLT. Se puede eliminar, agregar o servir un SLT sin trastornar la red SS7. El SLT de Cisco 2600 soporta dos puertos de enlace SS7, mientras que cada puerto puede manejar un conjunto de dos erlangs de tráfico. (Un erlang es el número de llamadas multiplicadas por el Average Hold Time [AHT] de la llamada dividido por 3.600.) Los SLT están conectados a través de la Ethernet estándar y entregan información MTP L3 al VSC a través de RUDP por la LAN / WAN.

4.5.1. Check-pointing de la aplicación

El check-pointing ocurre entre los VSC y asegura que las llamadas en progreso están protegidas en el caso de que ocurra un fallo.

El motor de procesamiento de llamadas envía los acontecimientos de checkpointing al proceso de checkpoint local durante la configuración de la llamada y las fases de liberación de la misma.Durante la fase de configuración de la llamada, el primer acontecimiento de checkpoint se genera cuando el administrador de recursos asegura el recurso de circuito físico desde el gateway de paquetes. El evento contiene suficiente información para permitir que el administrador de recursos remoto actualice el estado lógico del circuito asignado.

El segundo evento de checkpoint se genera cuando la llamada es respondida. Los datos del evento almacenados en el administrador de recursos remoto contienen sólo suficiente información para que el motor de procesamiento de llamada remoto mantenga la llamada hasta que sea liberada. Por tanto, en el caso de un fallo, las llamadas siguen estando en servicio, si bien no se soporta ninguna función de servicio. Durante la fase de liberación de la llamada, se genera un checkpoint cuando el administrador de recursos recibe un reconocimiento desde el gateway de paquetes asociado con la petición de liberación de llamada.El check-pointing se aplica también a los mensajes de supervisión de protocolo en el caso de que ocurran cambios en el estado lógico de los circuitos portadores entre la configuración y la liberación de la llamada inicial. Estos mensajes incluyen:

- Comandos y mensajes de bloqueo y desbloqueo.

- Comandos y mensajes de reinicio de circuitos.

4.5.2. Virtual switch manager

El Virtual Switch Manager (VSM) es una solución basada en la Telecommunication Management Network (TMN) para la administración de redes de extremo a extremo que suministra servicios SS7. VSM proporciona una administración consolidada de elementos de red de Cisco (NE), permitiendo así que el sistema de switch virtual sea tratado como un único elemento administrado. Las responsabilidades de VSM incluyen los elementos de red físicos que comprenden la voz y las partes de señalización del switch virtual, entre ellos:

- VSC.

- Unidades de codificación de voz.

- Tráfico de voz dentro del dominio de switch virtual.

- Tráfico de señalización intra switch e inter switch virtual.

- Tráfico de señalización entre la PSTN o PBX y la red de switch virtual como se ha visto con el VSC.

Las responsabilidades de VSM excluyen:

- Elementos externos de red de voz (switches telefónicos).

- Redes de datos o TDM que suministran voz o señalan la transmisión al switch virtual.

- Señalización de tráfico a o desde la PSTN y el dominio de switch virtual.

El dominio de VSM abarca elementos de señalización y trafico de voz y aparece en la figura 4.8.

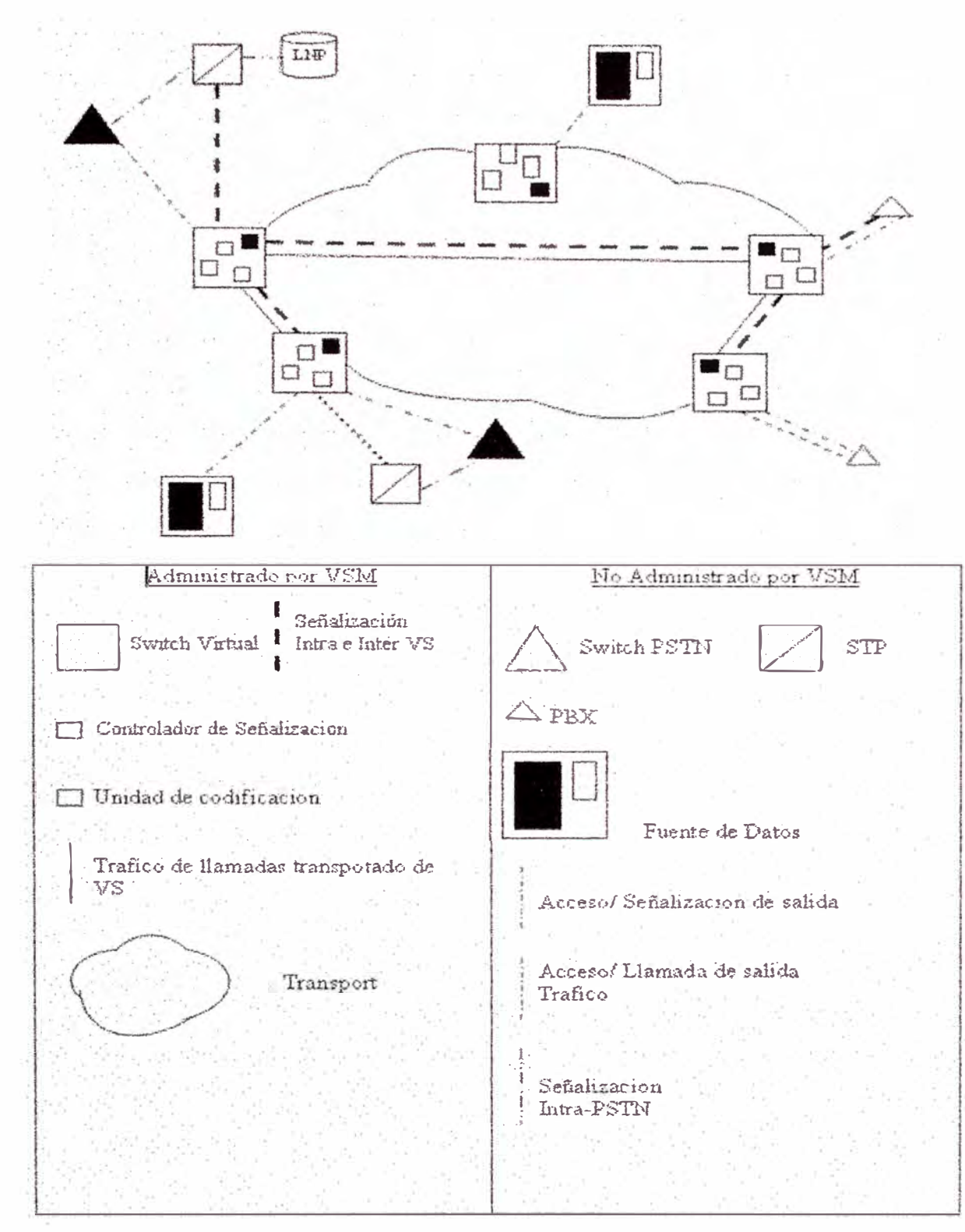

Figura 4.8. Dominio Virtual Switch Manager

En este dominio, el VSM proporciona una funcionalidad tradicional FCAPS para la administración de fallos, configuración, rendimiento y seguridad. Sin embargo, los servicios de contabilidad están proporcionados por CDR generados por el propio VSC. El VSM administra directamente el VSC e interactúa a través de SNMP y otras interfaces con los Sistemas de administración de elementos (EMS, Element Management Systems) externos. En realidad, los EMS externos administran los NE que componen la parte restante del switch virtual. La funcionalidad VSM para errores, configuración, rendimiento y seguridad en el interior del dominio es como sigue:

- Administración de errores. Muestra una representación gráfica de la información de alarma específica del dominio y niveles de seguridad. Soporta también una sofisticada correlación de eventos, aislamiento de problemas e información de estado resumida en el nivel de componentes. El navegador de administración de errores soporta una navegación point-and-click a través de las jerarquías de alarma y mapas de topología de red para la identificación simple de elementos.

- Administración de configuración. Proporciona utilidades basadas en texto y gráficos, así como soporte de interfaz gráfica de usuario (GUI, Graphical User Inteface), para todos los NE del dominio. En algunos casos, el VSM integra o comunica con administradores de elementos de Cisco para potenciar la robusta línea de productos de administración actualmente desplegada en los sitios de clientes de Cisco. Se accede a las utilidades de administración específica de elementos a través de una interfaz point-and-click desde el mapa de topología de red.

- Administración de rendimiento. El VSM reúne datos de tráfico y rendimiento a partir de elementos relevantes y los archiva en una base de datos central. El VSM proporciona un informe básico y aplicaciones gráficas para revisar los datos reunidos. Se proporciona una interfaz de base de datos abierta de Lenguaje de consulta estructurado (SQL, Structured Query Language) para herramientas de análisis e informes de cliente específico y offline.

- Administración de seguridad. El VSM soporta el acceso basado en el rol para varias funciones de administración y NE. Se pueden definir grupos de usuarios para simplificar la administración de usuarios; se soporta la funcionalidad estándar de ID de usuario y

contraseña. La seguridad de la cadena de comunidad SNMP estándar gobierna el acceso SNMP.

El VSM también proporciona interfaces northbound SNMP, TL1 y SQL (tiempo no real) para propagar alarmas a la capa superior de la administración de la red. Además de estas interfaces, el VSM puede proporcionar interfaces basadas en estándares para sistemas de administración de red Operation Support System (OSS), incluido el Protocolo de información de administración común (C MIP/Q2, Common Management Information Protocol/Q2) y Common Object Request Broker Architecture (CORBA). El VSM proporciona una GUI que permite a los usuarios controlar el EMS directamente.

La arquitectura VSM tiene en consideración los siguientes requisitos SP clave:

- Configuración, contabilidad, rendimiento, errores y seguridad separados por la especificación TMN.

- Proporciona una arquitectura de administración por capas, con la posibilidad de integrarse con sistemas de administración de red propietaria o sistemas planificados para el futuro.

- Utiliza un modelo recursivo de objeto de red por capas.

- Adopta CORBA como una dirección estratégica para las interfaces.

- Proporciona un aprovisionamiento a través del flujo.

- Admistra el rendimiento del tráfico de red.

- Pone en correlación las alarmas.

- Proporciona interfaces basadas en estándares.

4.5.3. Contabilidad

Cada llamada que maneja el VSC produce una información detallada de la misma. La cantidad de detalles generados es muy amplia; cada CDR contiene la siguiente información:

- Número que llama y que es llamado.
- Tiempo de respuesta, tiempo de desconexión y códigos de terminación de la llamada.
- Información de ruta, miembro y grupo troncal de origen, y miembro y grupo troncal de terminación.
- Información ISUP.
- Extensiones e información de servicios ISDN (RDSI).
- Números de identificación personal y códigos de la cuenta.

Junto con esta información, están disponibles más de 80 elementos adicionales para la configuración personalizada de CDR en formatos flexibles definidos por el usuario. Si un dato o elemento de uso no está disponible, el lenguaje TransPath Message Definición Language (MDL) puede generar campos separados en una matriz especial marcada como "personalizado" para requisitos CDR futuros. Estas matrices están configuradas para los estándares ITU y ANSI (American National Standards Institud).

Los registros detallados de las llamadas están escritos para un archivo spool que se cierra automáticamente a intervalos definidos por el cliente o cuando el archivo excede de un tamaño específico.

Se pueden recuperar archivos cerrados o enviarlos por sistemas de procesamiento de flujo descendente, como los dispositivos de mediación de facturación Automatic Messaging Accounting (AMA), según sea necesario. Los clientes también pueden generar información CDR a mitad de una llamada que registra los datos de hasta ocho puntos de eventos en una llamada.

CONCLUSIONES

1.- H.323 es un sistema híbrido construido a base de gatekeepers inteligentes centralizados, MCU, y puntos finales menos inteligentes. A pesar de que el H.323 estándar es más completo tras las recientes revisiones, han surgido problemas, como el tiempo de configuración de llamadas largas, el coste adicional de un protocolo de conferencias lleno de funciones, la necesidad de demasiadas funciones en cada gatekeeper y la preocupación por la escalabilidad de las implementaciones de gatekeeper de llamada enrutado.
Para casos en que se necesitan gateways de alta densidad para la interconexión PSTN, se han desarrollado alternativas, como el Protocolo Simple Gateway Control Protocol (SGCP) y el Protocolo Media Gateway Control Protocol (MGCP). Estos sistemas de control de llamada proporcionan una solución más efectiva y con capacidad de ampliación para satisfacer las implementaciones de clase de portadora. Del mismo modo, para las configuraciones inteligentes de punto final, el protocolo SIP (Protocolo de inicio de la sesión) resuelve algunos de los problemas encontrados en H.323 y está siendo implementado como alternativa.

2.- SIP es un protocolo de señalización IETF basado en estándares para aplicaciones multimedia con uno o más participantes. La propuesta de IETF es crear una arquitectura de capas funcional en la que se desarrollen prestaciones y funcionalidad específicas con protocolos altamente optimizados. SIP es un protocolo flexible que tiene posibilidades de extensión para funciones y servicios adicionales.
El estándar de señalización H.323 de la ITU-T 1, difiere del protocolo SIP del IETF. SIP presume de tener algunas ventajas sobre H.323, tales como una configuración de la llamada más rápida y menos compleja, una

implementación parecida a HTTP con una arquitectura modular que contiene funciones que residen en protocolos separados. La implementación de SIP es también "sin estado", lo que significa que los servidores no necesitan mantener el estado de la llamada.

3.- SGCP y MGCP son componentes vitales que se utilizan durante la transacción desde una red cuyos componentes están en una plataforma monolítica a una red cuyos componentes están distribuidos. SGCP y MGCP forman la base para que los agentes de llamadas y los gateways se comuniquen. Es una de las claves de una red de paquetes distribuidos.

4.- La arquitectura OPT permite separar la aplicación, el control de las llamadas y los planos portadores (principales). El agente de llamadas es uno de los componentes más importantes de esta arquitectura, ya que ayuda a las aplicaciones puente a portar los planos. El VSC es la ilustración de un agente de llamadas. Como implica esta arquitectura, el VSC permite que los clientes utilicen diferentes fabricantes en cada componente de la arquitectura (aplicación, control de llamadas y portadores). Esto permite utilizar los gateways de medios (MG) con agentes de llamadas de otros fabricantes, así como con el VSC.
Construir un agente de llamadas para un cliente SP requiere prestar atención a muchos detalles. La selección de la ruta, el control de llamadas y la fiabilidad son sólo unos cuantos de esos aspectos que se explican cuando se construye esta pieza de la arquitectura OPT.

BIBLIOGRAFÍA

1. Jonathan Davidson y James Peters, "Fundamentos de voz sobre IP", Pearson Educación –Madrid, 2001

2. http://www.iec.uia.mx/proy/titulacion/pr04/proy01/prueba.htm , "Convergencia de Redes"

2. http://www.monografias.com/trabajos3/voip/voip.shtml , "Voz sobre IP"

3. http://www.acticven.com/documentos.php , "Protocolos de señalización para transporte de voz sobre redes IP"

4. http://www.recursosvoip.com/tutoria1/preindex.php , "Protocolo H.323"