Universidad Autónoma Metropolitana
Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería
Licenciatura en Ingeniería en Computación

Proyecto de Integración en Ingeniería en Computación I

Implementación de VoIP en una VPN

Asesor
M. en C. Arturo Zúñiga López
No. Económico: 28779

Alumno
Ulises Arturo Pérez Lovera
Matrícula: 205303243

Trimestre 14-Invierno
9 de Abril de 2014

Yo, Arturo Zúñiga López, declaro que aprobé el contenido del presente Reporte de Proyecto de Integración y doy mi autorización para su publicación en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

_____

Firma

Yo, Ulises Arturo Pérez Lovera, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento en la Biblioteca Digital, así como en el Repositorio Institucional de UAM Azcapotzalco.

_____

Firma

Resumen

Los antecedentes de la voz sobre IP nos llevan a 1876 cuando Alexander Graham Bell realizo la primera llamada de voz en un circuito ring-down, de ahí nos pasamos a las redes telefónicas conmutadas donde al inicio de estas redes una persona era la que realizaba el trabajo de conmutador luego fueron reemplazadas por conmutadores electrónicos, años después se empezaron a realizar.

La voz sobre IP se puede definir como el envío de voz a través de una red por medio del encapsulamiento del tráfico de voz en paquetes IP. La voz sobre IP utiliza protocolos de señalización para el control de llamadas, protocolo Skinny, también utiliza protocolos para el transporte de voz a través de la red como por ejemplo el protocolo RTP y codecs para la codificación de la voz como es el G.711.

Las redes virtuales son redes lógicas que permiten conectar sitios remotos a través de internet ofreciendo protocolos de seguridad para el transporte de datos. IPSec proporciona una suite de protocolos para garantizar la seguridad y confidencialidad de los datos.

El proyecto consta de la implementación de una red privada virtual utilizando el conjunto de protocolos IPSec con capacidad de ofrecer servicios de telefonía en ambos extremos. En la implementación también se debe considerar el uso de NAT ya que este es comúnmente utilizado para conectar las redes privadas a la red pública, internet.

Se puede concluir que gracias a la encriptación proporcionada por los protocolos de IPSec se puede asegurar la confidencialidad de la llamada, debido a la encriptación que se implementó, las llamadas no puede ser interceptada ni decodificadas. Esto es un elemento muy importante para que las empresas u organizaciones opten por este tipo de esquema y dejar a un lado la telefonía tradicional que no proporciona la seguridad en los datos.

Tabla de contenido

Tabla de Ilustraciones

I. Introducción

Hoy en día el uso masivo de internet para la comunicación entre personas, ya sea por llamadas de voz o llamadas de voz y video, nos presenta la problemática de que tan seguro es utilizar este medio transmisión para este tipo de datos, una de las alternativas que se nos presenta para lidiar con esta problemática es el uso de la telefonía IP a través de la redes privadas virtuales las cuales nos proporcionan un canal seguro para poder comunicarnos sin preocuparnos de la integridad y seguridad de los datos. La implementación de estas tecnologías puede ser aprovechadas por las empresas y enfocarlas a sus actividades diarias ofreciéndole a sus trabajadores la posibilidad de trabajar desde sitios remotos como si estuvieran dentro de la red local, aprovechando todos los recursos que la red local ofrece, como puede ser el servicio de telefonía, y asegurando la privacidad de los datos de la empresa.

Nuestro proyecto busca aprovechar estas dos tecnologías, las redes privadas virtuales y la voz sobre IP, implantándolas de forma conjunta para poder ofrecer el servicio de telefonía IP a través de internet concentrando el control de llamadas de un solo lado de la VPN utilizando el conjunto de protocolos IPSec el cual no permite resguardar la privacidad de las llamadas de voz IP , así se ofrece de forma la prestación de un servicio que se encuentra en una red local de forma remota a través de internet. Este proyecto se podría implementar a una mayor escala permitiendo el acceso a más sitios remotos para poder consumir este servicio.

El siguiente documento, en su primera parte, trata temas relacionados con la voz sobre IP y las redes privadas virtuales, en su segunda parte describimos la implementación en conjunto de estas tecnologías, también en esta segunda parte hacemos un análisis de los resultados obtenidos.

La primera parte habla sobre los antecedentes de la voz sobre IP, nos cuenta acerca de la primera transmisión de voz realizada en la historia y de cómo esta tecnología ha ido evolucionando a través de los años pasando de las redes conmutadas hasta llegar a lo que hoy en día conocemos como voz sobre IP. Es interesante observar cómo estas tecnologías han ido evolucionando de solo tener dos dispositivos conectados por un cable hasta la conexión de miles de terminales utilizando internet como la infraestructura que hace posible la implementación de la voz sobre IP.

En el primer capítulo nos adentraremos a lo que hoy en día es la voz sobre IP, de cómo se convierte la voz en ceros y unos, y de la posibilidad de crear más aplicaciones que puedan aprovechar al máximo la infraestructura y crear mejores servicios relacionados con la voz sobre IP. En este capítulo abarcamos los protocolos H.323 y SCCP a fondo que en gran medida son los que nos permiten la comunicación de voz sobre IP en la red. También hablaremos de los codecs que son los encargados de hacer la transformación de las ondas de voz a unos y ceros, veremos las ventajas de utilizar la voz sobre IP y por último damos una introducción a lo que es la calidad de servicio y como esta es aplicada a la voz sobre IP.

Como continuación a nuestro trabajo abarcaremos las funcionalidades del *Cisco Call Manager*, que es el encargado de dar el servicio de telefonía IP dentro de las plataformas de servidores Cisco.

Describiremos las cuatro posibles topologías sobre las cuales es posible implementar de nuestros servidores *Cisco Call Manager* y de cuál es la mejor opción a tomar de acuerdo a las necesidades de la empresa.

En el capítulo tres definiremos lo que son las redes privadas virtuales, de cómo este tipo de tecnologías beneficia a las empresas y organizaciones permitiendo establecer conexiones de red seguras de largo alcance y de cómo hacen posible el consumir servicios como si se estuviera en una red de área local. Hablaremos de los tipos de redes privadas virtuales de capa uno y capa 2 y la diferencia que existe entre ellas. Abordaremos de forma más concreta lo relacionado con las redes privadas virtuales que utilizan el conjunto de protocolos IPSec, veremos la forma en la cual puede ser implementada y abordaremos un poco acerca de la seguridad que se utiliza en la red privada que utiliza IPSec.

Como último capítulo tenemos lo referente a la traducción de direcciones de redes, entenderemos su funcionamiento y las diferentes formas en la que funciona que puede ir desde establecer la traducción de direcciones de red uno a uno a la traducción de direcciones por puerto utilizando multiplexeo a nivel de puertos. En este capítulo se podrá observar como el uso más común de la traducción de direcciones es el de conectar redes privadas a la red pública, internet.

Como última parte de este trabajo encontraremos la implementación en conjuntos de las diferentes tecnologías abarcadas en los capítulos anteriores analizaremos los resultados obtenidos de esta implementación y se expondrán las diferentes configuraciones para lograr dicho propósito.

II. Antecedentes

La primera transmisión de voz enviada por Alexander Graham Bell, tuvo lugar en 1876, a través de lo que se llamó un circuito *ring-down,* significa que no hay marcación de número. En su lugar un cable conectaba físicamente dos dispositivos. Básicamente, una persona descolgaba el teléfono y otra persona se encontraba en el otro extremo (no había llamada). Con el tiempo, este diseño básico evoluciono desde una transmisión de voz de un único sentido, en la que sólo podía hablar un usuario, hasta una transmisión voz bidireccional, en la que ambos usuarios podían hablar. Para mover las voces por el cable se necesitaba un micrófono de carbón, una batería, un electroimán y un diafragma de hierro.

También se necesitaba un cable físico entre cada ubicación a la que el usuario quería llamar. Sin embargo, en ese tiempo todavía no existía el concepto de marcar un número para alcanzar un destino.

Se puede colocar un cable físico entre cada casa que solicite un teléfono; sin embargo una configuración así no es rentable ni segura. Para determinar cuantas líneas se necesitan en una casa hay que pensar en cada persona en a la que se llama como un valor de N y utilizar la siguiente ecuación: N x (N-1)/2. De esta manera si se quiere llamar a 10 personas, se necesitan 45 pares de líneas en una casa.

Debido al costo y a la imposibilidad de poner un cable físico entre todas las personas que quieren acceder a un teléfono en la Tierra, se ha desarrollad otro mecanismo que pueda asociar un teléfono con otro teléfono. Con este dispositivo llamado *switch*, los usuarios solo necesitan un cable que vaya a la oficina del *switch* central.

Al principio, un operador telefónico actuaba como el *switch*. Este operador preguntaba a la persona que llamaba dónde quería llamar y luego conectaba manualmente las dos rutas de voz. En la actualidad la conmutación por el hombre ha sido sustituida por la conmutación electrónica. Esto dio paso a la PSTN (Red pública de telefonía conmutada) moderna.

VoIP comenzó como el resultado del trabajo de un grupo de jóvenes en Israel durante 1995. En aquella época la única comunicación posible era de PC-a-PC. Poco más tarde *Vocaltec, Inc*. anuncio el lanzamiento del primer *softphone* que llamaron "*Internet Phone Software*". Este *softphone* estaba hecho para ser usado en una PC hogareña que tenía tarjeta de sonido, micrófono, parlantes y modem. El software funcionaba comprimiendo la señal de voz, convirtiéndola en paquetes de voz que eran enviados por Internet (exactamente igual que hoy). El software sólo funcionaba si las dos PC tenían el mismo software y el mismo hardware. Y fue comercialmente un fracaso principalmente porque las comunicaciones de banda ancha todavía no estaban disponibles. En 1997 Jeff Pulver decide juntar por primera vez a los pocos usuarios, fabricantes, e interesados en esta tecnología en VON, la primer feria/congreso que actualmente sigue siendo el mayor evento de *VoIP*. Ahora Pulver organiza VON 2 veces por año en EEUU, y ahora también una vez por año en varios países de Europa. También formó una compañía prestadora de servicio *VoIP* llamada *FreeWorldDialup* comúnmente llamada FWD (que puede confundirse con el término FWD = transferencia de llamadas) y es co-fundador de Vonage, el proveedor de *VoIP* más grande de EEUU. Pulver tiene varias empresas relacionadas con *VoIP* entre ellas PulverMedia, su empresa encargada de organizar VON y publicar medios en todo el mundo. En 1998 *VoIP* dio otro gran salto. Un grupo de emprendedores comenzó a fabricar los primeros *ATA*/*gateways* para permitir las primeras comunicaciones PC-a-teléfono convencional y finalmente las primeras comunicaciones teléfono-convencional - a - teléfono-convencional (con *ATAs* en cada extremo). Algunos de estos emprendedores inicialmente daban el servicio sin cargo a sus clientes para que pudieran probar la calidad y la tecnología. Estas llamadas contenían publicidad en el inicio y al final de cada comunicación. Estos servicios solo se prestaban en EEUU y funcionaban gracias a esta publicidad. A menudo debía comenzarse la comunicación a través de una PC para luego pasar a un teléfono convencional. En este punto *VoIP* sumaba el 1% del total del tráfico de voz. Durante 1998 tres fabricantes comenzaron a fabricar *switches* de capa 3 con QoS. En 1999 Cisco vende sus primeras plataformas corporativas para *VoIP*. Se utilizaba principalmente el protocolo H323 de señalización.

En el año 2000 *VoIP* representaba más del 3% del tráfico de voz. El mismo año Mark Spencer un estudiante de la Universidad de Auburn crea Asterisk, la primer central telefónica / conmutador basada en Linux con una PC hogareña con un código fuente abierto. Asterisk hoy ofrece una solución freeware para hogares/pequeñas empresas y soluciones IP-PBX corporativas.

En 2002 el protocolo SIP comienza a desplazar al H323.

En 2003 dos jóvenes universitarios - Jan Friis y Niklas Zenntrom - crean un softphone gratuito fácilmente instalable en cualquier PC que puede atravesar todos los firewalls y routers inclusive los corporativos. Ese producto es *Skype*, que se propaga con una velocidad increíble, y llega en Diciembre de 2005 a contar con 50 millones de usuarios.

III. Justificación

La transferencia de voz por medios seguros en una red es una solución útil para el paso de mensajes al estableces comunicaciones en cuestiones empresariales, sin embargo dichas transferencias de audio requieren un ancho de banda mayor, por lo que gestionar este tipo de inconvenientes con la calidad de servicios (QoS) disponible en los routers y *switches* Cisco puede reconocer el tráfico de datos importante y tratarlo de una forma especial, aunado al hecho de utilizar el conjunto de protocolos IPSec serán soluciones viables a los problemas antes mencionados en cuanto a la comunicación empresarial.

El diseño y configuración adecuada de redes requiere conocimientos y habilidades que son más propias de un ingeniero en computación, como el manejo de sesiones, gestión de servicios de red, estructuración de diferentes topologías, entre otras. Se considera que estos requisitos no son del dominio de otras carreras.

El presente proyecto puede servir de modelo para realizar implementaciones del protocolo VoIP sobre VPN's que utilicen otros protocolos de seguridad diferentes al utilizado y puede implementarse en ambientes escolares o empresariales para establecer comunicaciones.

IV. Objetivos

General

Diseñar una topología de red que permita el tráfico de VoIP, Voz sobre IP, sobre una red privada virtual (VPN) punto a punto asegurada con el conjunto de protocolos IPSec.

Particulares

I. Implementar una VPN IPSec punto a punto.
II. Implementar VoIP sobre la VPN.
III. Probar el funcionamiento de la implementación.

Capítulo I. Voz sobre IP

Se puede definir, de una manera simple, la VoIP como el envío de voz a través de una red por medio del encapsulamiento del tráfico de voz en paquetes IP. El trabajo de convertir la voz analógica en datos digitales comienza con el muestreo, se toman muestras de la onda de voz análoga cada determinado tiempo, luego esas muestras son digitalizadas después del otro extremo de la conversación de voz las señales digitalizadas pueden ser convertidas en ondas analógicas las cuales el oyente puede entender.

La integración de voz, datos y video va más allá de un cambio de infraestructura, también implica nuevas características que deben desarrollarse rápidamente y abre el desarrollo de aplicaciones a miles de proveedores de software independiente.

La figura 1 muestra como el modelo de conmutación de circuitos está entrando en un nuevo modelo por el cual existen estándares abiertos entre las tres capas. Una capa de infraestructura de paquetes llevará la voz (media), la capa de control de será separada de la capa de infraestructura, y la capa de aplicaciones de servicio, permitirá los nuevos servicios que serán creados por los proveedores de software independientes.

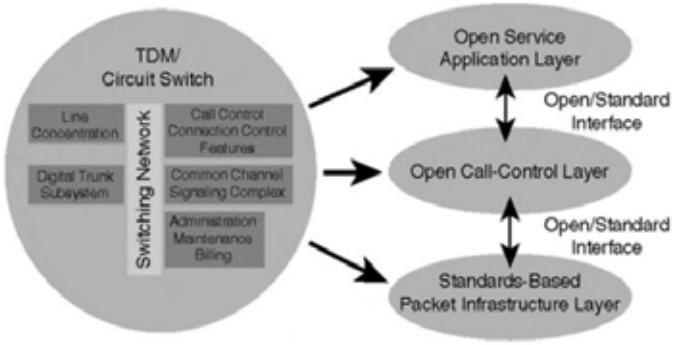

Figura 1 Modelo de Conmutación vs Modelo de Datos

- **Capa de infraestructura:** La capa de infraestructura reemplaza la infraestructura de conmutación, la cual podría ser IP, las aplicaciones que corran sobre IP no tienen que ser conocidas, IP solo transporta los datos de punto a punto sin ningún interés en la carga útil. Para proporcionar la adecuada priorización en una red IP congestionada, la red IP debe tener conocimiento de las aplicaciones.

  El protocolo de transporte en tiempo real (RTP) es utilizado en conjunto con un encabezado UDP/IP para proporcionar una marca de tiempo. RTP corre sobre UDP e IP y se conoce comúnmente como RTP/UDP/IP. RTP es actualmente la piedra angular para llevar el tráfico en tiempo real a través de redes IP. A menudo los paquetes RTP se conocen como flujos RTP. Esta nomenclatura es utilizada para describir el flujo del audio.

  En las redes IP es común que exista la perdida de paquetes, de hecho el TCP/IP fue hecho para utilizar los paquetes perdidos como un medio para controlar el flujo de paquetes. En TCP/IP sí un paquete es perdido este es retransmitido, en la mayoría de las aplicaciones en tiempo real la retransmisión de paquetes es muy malo debido a la naturaleza sensible al tiempo de la información.

  RTP contiene un campo que guarda el tiempo exacto en el que el paquete fue enviado, en relación con todo el flujo RTP. Esta información es conocida como la marca de tiempo RTP y es usado por el dispositivo que inicia/termina el flujo de audio. El dispositivo que termina utiliza la marca de tiempo RTP para determinar cuándo se espera un paquete, si el paquete estaba en orden, y si fue recibido cuando se esperaba. Toda esta información ayuda al dispositivo receptor a determinar la manera de ajustar su propia configuración para

enmascarar los problemas potenciales de la red tales como retardos, *jitter* y pérdida de paquetes.

Uno de los principales beneficios de las redes IP es el hecho de que las redes IP correctamente construidas son auto sanables, esto significa que debido a que son utilizados protocolos de ruteo dinámicos y existen varios destinos posibles, una red puede volver a converger sobre una mejor ruta, esto también significa que la voz, en paquetes IP puede tomar varias rutas hacia el mismo destino, cada paquete toma el mejor camino entre el emisor y el receptor.

El hecho de que la esta capa se basa en estándares abiertos permite que múltiples proveedores puedan ofrecer soluciones que sean interoperables. Un componente clave de tener una infraestructura de paquetes basada en estándares es la capacidad de tener estándares abiertos a la capa de control de llamada, estos estándares abiertos son proporcionados por protocolos tales como el H.323, SGCP, MGCP, SIP, etc. Que tienen interfaces definidas abiertas y son utilizados ampliamente en la infraestructura de paquetes. Uno de los trabajos del protocolo de control de llamada es indicarle al RTP dónde terminará y por dónde empezar. El control de llamada lleva acabo esta tarea mediante la traducción entre las direcciones IP y los planes de numeración telefónica.

- **Capa de Control:** El control de llamada es el proceso de hacer una decisión de ruteo acerca de donde la llamada necesita llegar y cómo hacer que la llamada suceda. Este nuevo modelo de separar los flujos RTP de la capa de control y de separar la capa de control de la capa de servicios es necesario para para asegurarse que los protocolos basados en estándares son utilizados. Las redes de datos son únicas ya que permite que múltiples protocolos puedan coexistir dentro de la red y se pueden adaptar a las necesidades particulares de la red. Existen varios protocolos de control de llamadas *VoIP*, todos resuelven la traducción de un número de teléfono a una dirección IP, entre ellos podemos encontrar el H.323, MGCP, SIP.
- **Capa de Servicio de Aplicaciones:** La capa más interesante de cualquier protocolo de red es la capa de aplicación, sin buenas aplicaciones la infraestructura de red es hecha en vano. Cuando se migra a una nueva infraestructura no es necesario llevar todas las características de la vieja infraestructura a la nueva, solo se requieren las características o aplicaciones que los clientes necesitan. Cuando se construye una red que tiene interfaces abiertas de la capa de infraestructura de paquetes a la capa de control y de la capa de control a la capa de aplicaciones, los proveedores ya no tienen que desarrollar aplicaciones ahora ellos pueden desarrollar sobre estas *APIs* estándar y tener acceso a toda la nueva infraestructura. Cuando una nueva infraestructura de paquetes es construida las oportunidades para nuevas aplicaciones son altamente viables.

Protocolos de control de llamadas

La meta de un protocolo de control de llamada en la red *VoIP* es permitir los flujos RTP fluyan directamente entre los puntos finales. Durante el proceso de establecimiento de una llamada cada punto final necesita conocer la dirección IP Y el puerto UDP a utilizar con el fin de recibir una llamada de teléfono al otro extremo de la conversación.

Algunos de los principales protocolos VoIP son H.323, *Simple Gateway Control Protocol* (SGCP), *Internet Protocol Device Control* (IPDC), MGCP y SIP.

- H.323 es la recomendación de ITU-T con la base instalada más grande, simplemente porque ha existido por más tiempo y no había otras opciones que existieran antes que este.
- SGCP fue desarrollado a partir de 1998 para reducir el costo de puntos finales (puertas de enlace) a través de tener centralizado el control de llamadas dentro de una puerta de enlace de control. IPDC es muy similar a SGCP, pero cuenta con más mecanismos para la operación, administración, gestión y el aprovisionamiento (OAM&P) que SGCP. OAM&P es clave para las redes de transporte ya que abarca la forma en que estas son mantenidas y desplegadas.
- A finales de 1998, el IETF fusiono IPDC y SGCP y se transformó en MGCP que es básicamente SGCP con algunas adiciones para OAM&P.
- SIP es un protocolo basado en los medios de comunicación que permite a los medios finales ser más inteligentes y permitir mejores servicios hacia la capa de control de llamadas.

  Una configuración básica de llamada SIP comienza cuando un cliente envía un mensaje de INVITE al servidor SIP, el servidor de destino, UAS, responde si está dispuesto a unirse a la sesión a la que ha sido invitado. El cliente de origen, UAC, envía el mensaje de recibido, mensaje ACK, al servidor de destino, en este punto el flujo RTP fluye directamente entre las puertas de enlace SIP. Por último el cliente que finaliza la llamada envía un mensaje BYE al servidor SIP, figura 2.

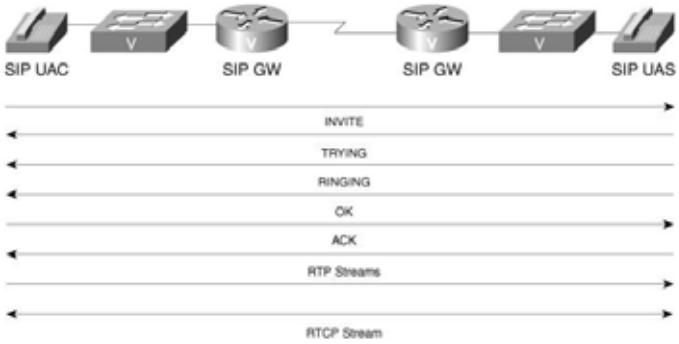

Figura 2. Llama SIP

H.323 a fondo

H.323 es una especificación para transmitir audio, video y datos a través de las redes IP, incluidas internet, del Sector de Normalización de las Telecomunicaciones de la UIT, ITU-T por sus siglas en inglés. Cuando se cumple con el H.323, los productos y aplicaciones de los diferentes proveedores pueden comunicarse unas con otras. El estándar H.323 de señalización de llamada de control, transporte y control multimedia, y el control de ancho de banda para las conferencias de punto a punto y multipunto. La serie H de las recomendaciones también específica el H.320 para la red

digital de servicios integrados (ISDN) y H.324 para el viejo servicio telefónico (POSTS) como mecanismos de transporte.

El estándar H.323 consiste de los siguientes componentes y protocolos:

Característica	Protocolo
Señalización de llamada	H.225
Media Control	H.245
Codecs de audio	G.711, G.722, G.723, G.728, G.729
Codecs de video	H.261, H.263
Compartimiento de datos	T.120
Transporte Media	RTP/RTCP

La figura 3 ilustra los elementos de un sistema H.323, estos elementos incluyen terminales, puertas de enlace, gatekeeper, y unidades de control multipunto, MCU.

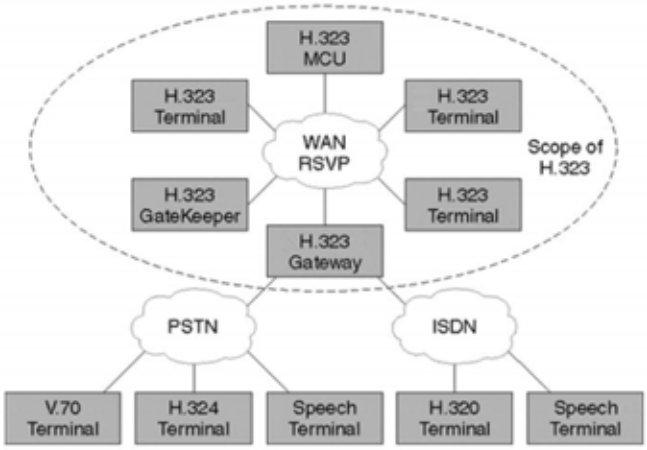

Figura 3 Elementos de una red H.323

También conocidos como puntos finales, las terminales proveen conferencias punto a punto y multipunto para audio y opcionalmente videos y datos. Las puertas de enlace interconectan Las redes PSTN o las redes ISDN para el funcionamiento con los puntos finales H.323. Los *gatekeeper*, controladores de acceso, proporcionan un control de admisión y los servicios de traducción de direcciones de las terminales o puertas de enlace. Los MCU's son dispositivos que permiten a dos o más terminales o puertas de enlace establecer una conferencia, ya sea con sesiones de audio y/o video.

Terminal

El siguiente elemento de red es definido, figura 4 en H.323 como terminal. Las terminales H.323 deben tener una unidad de sistema de control, transmisión de medios, audio códec, y una interfaz de red basada en paquetes. Opcionalmente pueden incluir códec de video y aplicaciones de datos.

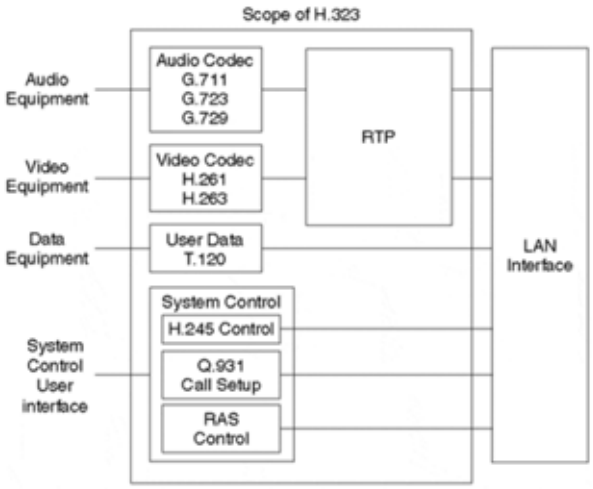

Figura 4 Terminal

Las siguientes funciones y capacidades están dentro del alcance de la terminal H.323:

- **Unidad de sistema de control:** Proporciona control de llamada tanto H.225 y H.245, intercambio de capacidades, mensajería, y señalización de los comandos para la operación correcta de la terminal.
- **Transmisión de medios:** Da el formato de la transmisión de audio, video, datos, flujo de control, y los mensajes dentro de la interfaz de red. La transmisión de medios también recibe audio, video, datos, control de flujo, y mensajes desde la interfaz de red.
- **Códec de audio:** Codifica la señal del equipo de audio para la transmisión y decodifica el código de audio entrante. Las funciones requeridas incluyen codificación y decodificación de voz G.711, la transmisión y recepción de los formatos a-law y μ-law. Opcionalmente pueden ser soportados la codificación y decodificación de G.722, G.723.1, G.728 y G.729.
- **Interface de red:** Una interfaz de red basada en paquetes capaz de realizar TCP de extremo a extremo y servicios UDP *unicast* y *multicast*
- **Códec de video:** Opcional, pero si se proporciona debe ser capaz de codificar y decodificar video de acuerdo al H.261 *Quarter Comment Intermediate Format*, QCIF.
- **Canal de datos:** Soporta aplicaciones como son bases de datos de acceso, transferencia de archivos, y conferencias audiográficas, que es la capacidad de modificar una imagen en común por múltiples usuarios simultáneamente, como se especifica en la recomendación T.120.

Puerta de enlace

La puerta de enlace H.323 refleja las características de una red de conmutación de circuitos, punto final SCN, y un punto final H.323. Es el encargado de traducir los formatos de transmisión entre audio, video y datos, así como los sistemas de comunicación y protocolos. Esto incluye el establecimiento de llamadas y el desmontaje tanto en la red IP como en el SCN.

La puerta de enlace no es necesaria al menos que la interconexión con la SCN sea requerida. Por lo tanto los puntos finales pueden comunicarse directamente sobre la red de paquetes sin necesidad de conectarse a la puerta de enlace. La puerta de enlace actúa como una terminal H.323 o MCU en la SCN, como se muestra en la figura 5.

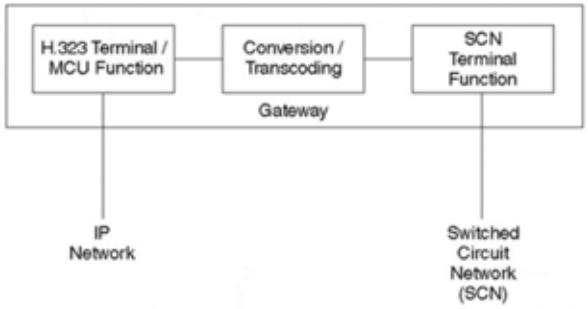

Figura 5 H.323 Gateway

Gatekeeper

Como una función opcional, el *gatekeeper* provee los servicios de control de pre-llamada y nivel-llamada a los puntos terminales H.323. Los *gatekeeper* están separados lógicamente de los otros elementos de la red en el ambiente H.323. Si más de un gatekeeper es implementado la intercomunicación se logra de una forma no especificada.

Sí un gatekeeper se presenta en un sistema H.323, debe realizar las siguientes funciones.

- **Traducción de direcciones:** Provee a las direcciones IP de los nodos finales alias H.323, como pc1@cisco.com, o direcciones E.164, números de teléfono estándar.
- **Control de admisión:** Provee acceso a H.323 usando los mensajes de *Admision Request/Admision Confirm/Admision Reject*, ARQ/ACF/ARJ.
- **Control del ancho de banda:** Consiste en la administración de los requerimientos de ancho de banda de los puntos terminales usando los mensajes de *Request/Bandwidth Confirm/Bandwidth Confirm/Bandwidth Reject*, BRQ/BCF/BRJ.
- **Zona de gestión:** Se proporciona para las terminales registradas, puertas de enlace y MCU's.

Los MCU

Un controlador multipunto, MC, soporta conferencias entre tres o más puntos terminales en una conferencia multipunto. MC's transmiten el conjunto de capacidades para cada punto terminal de la conferencia multipunto y pueden revisar las capacidades durante esta. La función MC puede residir en un terminal, Gateway, gatekeeper, o MCU.

El procesador multipunto, MP, recibe audio, video, y/o flujo de datos y los distribuye a los puntos terminales que participan en la conferencia multipunto.

El MCU es un punto terminal que soporta conferencias multipunto y, como mínimo, consiste de un MC y uno o varios MP's. Si soporta conferencias multipunto centralizadas, una MCU consiste de un MC y un MP de audio, video y datos.

H.323 Servidor Proxy

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

- Las terminales que no soportan el Protocolo de Reserva de Recursos, RSVP, pueden conectarse a través de accesos o LAN's con relativamente buena calidad de servicio hacia el proxy. Los pares proxys pueden entonces negociar un QoS adecuada para realizar un túnel a través de la red IP.
- Los proxys soportan el ruteo del tráfico H.323, separarlo del tráfico común de datos a través de la aplicación de enrutamiento, ASR.
- Un proxy es compatible con la translación de direcciones, habilitando los nodos H.323 para ser implementados en redes con direcciones privadas.
- Un proxy implementado sin un firewall o independiente de un firewall provee la seguridad afín de que solo el tráfico H.323 pasa a través de él. Un proxy implementado en conjunto con un firewall habilita al firewall a ser configurado para pasar todo el tráfico H.323 por el proxy como un nodo de confianza. Esto permite al firewall garantizar la seguridad de la red de datos y el servidor proxy proporciona la seguridad del tráfico H.323.

Suite de Protocolos H.323

El conjunto de protocolos H.323 consiste en varios protocolos, como se muestra en la figura 6. Este conjunto de protocolos soporta la admisión de llamadas, configuración, estado, desmontaje, flujo de medios, y mensajes en sistemas H.323. Estos protocolos son compatibles con ambos mecanismos de entrega de paquetes fiables y no fiables a través de la red de datos.

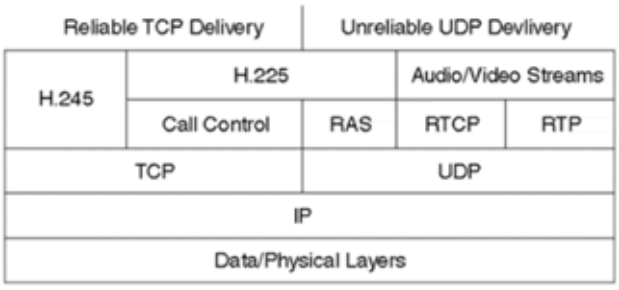

Figura 6 Capaz de la Suite de Protocolos H.323

Hoy en día la mayoría de implementaciones H.323 utilizan TCP como mecanismo de transporte para la señalización, la versión 2 de H.323 habilita el transporte básico UDP. Otros estándares se encuentran investigando el uso de mecanismos UDP para crear métodos de señalización escalables.

El conjunto de protocolos H.323 se divide en tres áreas de control:

- **Señalización de registro, admisión y estado, RAS:** Provee pre-llamada control en los *gatekeeper* H.323 basados en red.
- **Señalización de control de llamada:** Usado para conectar, mantener y desconectar llamadas entre los puntos finales.
- **Control de medios y transporte:** Proporciona el canal H.245 fiable que lleva el mensaje de control de medios. El transporte se produce con un flujo UDP no fiable.

Señalización de control de llamadas H.225

En redes H.323, el proceso de control de llamadas se encuentra basado en la recomendación H.225 de la Unión Internacional de Telecomunicaciones, ITU, la cual específica el uso y soporte de señalización de mensajes Q.931. Se proporciona un canal de llamada de control el cual es creado a través de la red IP en el puerto TCP 1720. Este puerto inicia los mensajes de control de llamada Q.931 entre dos puntos finales con el propósito de conectarlos, mantenerlos y desconectarlos de la llamada.

Los mensajes de control de llamada y de mantenimiento de conexión se mueven a los puertos efímeros después de la configuración inicial de la llamada. Pero el puerto 1720 es el puerto para las llamadas H.323. H.225 también especifica el uso de mensajes Q.932 para los servicios suplementarios.

Los siguientes mensajes Q.931 y Q.932 son lo más comúnmente usados en la señalización de mensajes en las redes H.323.

- ***Setup*:** Un mensaje de avance es enviado por la entidad H.323 que llama en un intento de establecer la conexión con la entidad H.323 a la que llama. Este mensaje es enviado al puerto H.225 1720 TCP.
- ***Call Proceeding*:** Un mensaje de regreso es enviado por la entidad llamada a la entidad que llama para avisar que el procedimiento de establecimiento de llamada se ha iniciado.
- ***Alerting*:** Un mensaje de regreso es enviado por la entidad llamada para avisar que el tono de inicio de llamada a comenzado.
- ***Connect*:** Un mensaje de regreso es enviado de la entidad llamada a la entidad que llama para indicar que ha contestado la llamada. El mensaje de conexión puede contener la dirección de transporte UDP/IP para el control de señalización H.245.
- ***Release Complete*:** Envida por el punto terminal que inicia la desconexión, lo que indica que la llamada está siendo liberada. Solo se puede enviar este mensaje si el canal de señalización de llamada está abierto o activo.
- ***Facility*:** Un mensaje Q.932 es utilizado para solicitar o conocer los servicios suplementarios. También es usado para indicar si una llamada debe ser directa o debe pasar a través de un gatekeeper.

La figura 7 muestra la señalización de mensajes para el establecimiento de una llamada. La interacción con el gatekeeper es limitado a los mensajes RAS para permisos de llamada, y posiblemente, a los mensajes de estado.

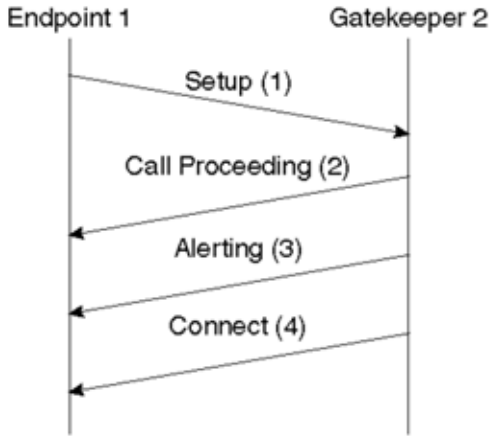

Figura 7 Mensajes de señalización de establecimiento de llamada

Se puede enrutar el canal de señalización de llamada en una red H.323 en dos formas. A través de GKRCS y de la señalización de llamada directa del punto terminal. En la señalización de llamada directa del punto terminal, los mensajes de señalización de llamada son enviados directamente entre los puntos terminales. Como se ilustra en la figura 8.

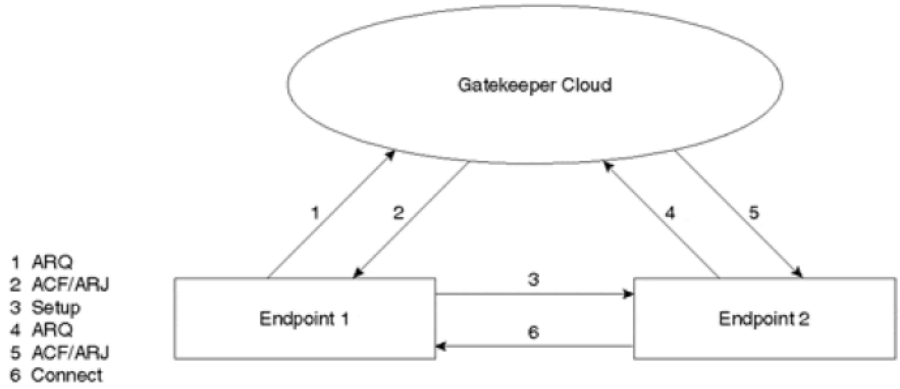

Figura 8 Señalización de llamada directa

En el método GKRCS, los mensajes de señalización de entre los puntos terminales son enrutados a través del *gatekeeper*, como se ilustra en la figura 9.

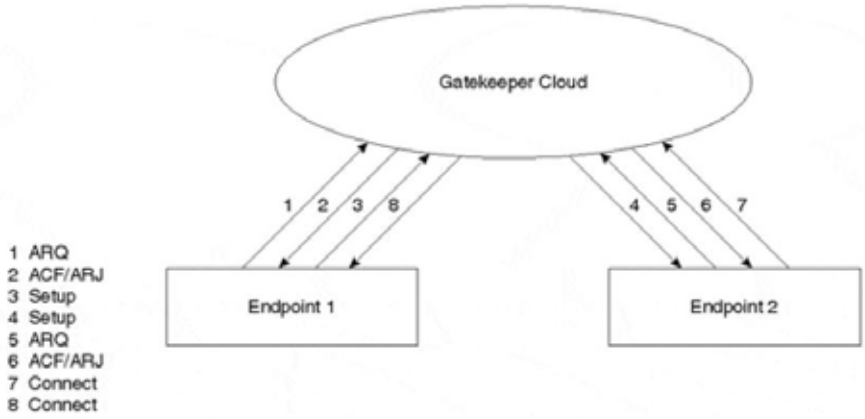

Figura 9 GKRCS

Se pueden ofrecer servicios suplementarios a través del método GKRCS si el canal de señalización de llamada se deja abierto durante la llamada. Los gatekeepers también pueden cerrar el canal de señalización de llamadas después de que el establecimiento de la llamada ha sido completado.

Transporte y control de medios (H.245 y RTP/RTCP)

H.245 maneja los mensajes de control de extremo a extremo entre las entidades H.323. Los procedimientos H.245 establecen canales para la transmisión de audio, video, datos, y el canal de control de información. Un punto terminal establece un canal H.245 por cada llamada con el punto terminal participante. El canal de control confiable es creado sobre IP usando el puerto TCP asignado dinámicamente en el mensaje de señalización final de llamada.

El intercambio de capacidades, la apertura y el cierre de los canales lógicos, los modos preferentes, y los mensajes de control toman lugar sobre este canal de control. El control H.245 también permite transmisión y recepción de intercambio de capacidades por separado así como la función de negociación, tales como la determinación de que códec utilizar.

Si se utiliza la señalización de llamada por Ruteo Gatekeeper, se puede controlar el enrutamiento del canal de dos formas. Se puede usar el Control Directo H.245, que se produce directamente entre los puntos finales participantes. O, se puede usar el Control de Ruteo *Gatekeeper* H.245, que se produce entre cada punto final y su gatekeeper.

Se pueden utilizar los siguientes procedimientos y mensajes para habilitar la operación de control H.245.

- **Intercambio de Capacidades:** Consiste en mensajes que aseguran el intercambio de capacidades entre dos punto, también conocidos como terminales. Estos mensajes indican a las terminales transmitir y recibir capacidades para audio video, y datos al terminal participante. Para audio, el intercambio de capacidades incluye codecs de transcodificación de voz, tales como la serie-G G.729 a 8 kbps , G.728 a 16 kbps , G.711 a 64 kbps , G.723 a 5,3 o 6,3 kbps o G.722 a 48 , 56 y 64 kbps. También incluye ISO series

IS.11172-32 con 32-, 44.1-, y 48 kHz frecuencia de muestreo, e IS.13818-3 con 16-, 22.05-, 24-, 32-,44.1-, y 48 kHz frecuencia de muestreo, y GSM *full-rate*, *half-rate* y *enhaced full-rate* codecs de audio de voz.

- **Terminación Maestro-Esclavo:** Procedimientos son usados para determinar que extremo es el maestro y cuál es el esclavo para una llamada en particular. La relación es mantenida durante la duración de la llamada y es usada para resolver conflictos entre los puntos finales. Las reglas maestro-esclavo son usadas cuando ambos extremos piden acciones similares al mismo tiempo.
- **Round-Trip Delay:** Procedimientos son usados para determinar el retraso entre el punto final de origen y el de destino. El mensaje *RoundTripDelayRequest* mide el retraso y verifica que el protocolo de la entidad remota H.245 este vivo.
- **Señalización Lógica del Canal:** Abre y cierra el canal lógico que transporta audio, video e información. El canal es establecido antes de la transmisión para asegurarse que las terminales están listas y capaces de recibir y decodificar información. Los mismos mensajes de señalización establecen ambos canales unidireccional y bidireccional. Después de que el canal lógico es establecido, el puerto UDP para el canal RTP se hace pasar desde el punto final de origen hasta el de destino. Además, cuando se utiliza el modelo de controlador de acceso de llamada enrutada, este es el punto en el que el controlador de acceso puede desviar la transmisión de tráfico RTP proporcionando la dirección de UDP / IP real del punto extremo de terminación.

La siguiente figura, figura 10, muestra el flujo de llamada entre dos puntos finales que comparten el mismo gatekeeper usando la señalización directa al punto final.

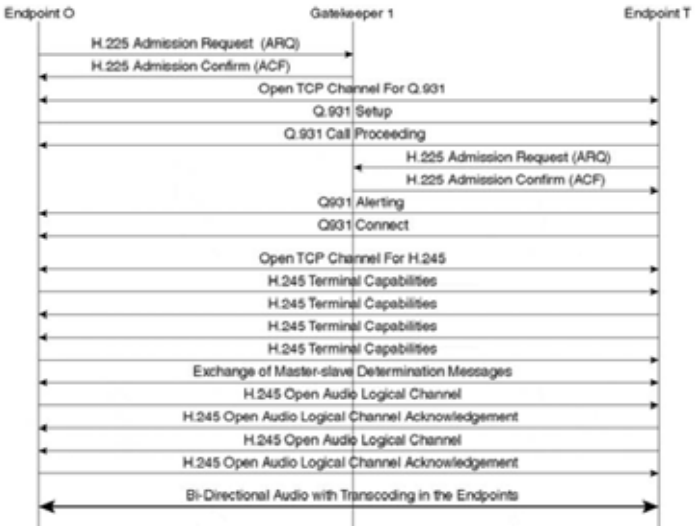

Figura 10 GKRCS

SCCP, Skinny Client Control Protocol

Es un protocolo de red propietario originalmente desarrollado por la empresa Selsius Systems.

La tecnología SCCP es actualmente propiedad de *Cysco Systems*. SCCP es un protocolo ligero para la señalización de sesiones que trabaja con el CCM. SCCP se utiliza para la comunicación entre dispositivos IP y el CCM. Ejemplos de clientes SCCP incluyen la serie CISCO 7900 de teléfono IP, el sophone Cisco IP Communicator. CCM actúa como un proxy de señalización para eventos de llamadas iniciadas sobre otros protocolos como pueden ser el H.323, SIP, MGCP.

Un cliente SCCP utiliza TCP/IP para comunicarse con otras aplicaciones dentro de un clúster. Utiliza RTP sobre UDP para soportar los flujos de audio en tiempo real con otros clientes Skinny o con terminales H.323. SCCP es un protocolo basado en el estímulo y es diseñado como un protocolo de comunicaciones para terminales de hardware y otros sistemas embebidos, con importantes limitantes de CPU y de memoria.

Códecs

Los Códecs, codificadores decodificadores, son los encargados de tomar una onda análoga de voz y convertirla en 0´s y 1's. Los teléfonos CISCO soportan el códec G.711, EL CODEC G.711 no soporta la compresión de voz, es decir no reduce el ancho de banda requerida para la voz.

El códec G.711 convierte las ondas análogas en binario usando la modulación por impulsos codificados (PCM). Las LAN's de alta velocidad comúnmente utilizan este códec ya que los 64 kbps requeridos para la carga útil de voz que utiliza el códec G.711 son insignificantes sobre el ancho de banda de la LAN.

En las WAN's si se utiliza el códec G.711 se puede alcanzar el ancho de banda disponible con pocas llamadas. Por lo tanto normalmente se utiliza el códec G.729. Solo requiere 8 kbps de ancho de banda para la carga útil de voz. La primera generación de teléfono IP soportan el códec G.723 que solo requiere 6.3 kbps de ancho de banda para la carga útil de voz, sin embargo el G.723 sufre de más degradación de voz que el G.729. Los teléfonos CISCO utilizan una variante del códec G.729 que se llama G.729a que tiene como característica de reducir la carga de procesamiento necesario para comprimir las muestras de voz.

Beneficios de VoIP

Entre los beneficios que se encuentran al utilizar *VoIP* son:

- Ahorro de costos.
- Ahorro en costos de infraestructura.
- Nuevas aplicaciones.

Uno de los factores clave para la combinación de las redes de voz y datos es el ahorro de costos. El ahorro de costos puede variar de acuerdo a la localización geográfica, en países distintos a Estados Unidos una comparación de costos, minuto a minuto entre *VoIP* y PSTN tradicional, donde el costo por minuto puede ser alrededor de $1, justifica el gasto para la implementación de *VoIP*.

Hoy en día muchas empresas consideran muy costoso trasladar un teléfono, debido a factores como los costos de mano de obra y el costo para volver a configurar el interruptor, debido a que estos costos no se presentan en una infraestructura IP, donde mover un teléfono IP conservando el mismo número es lo mismo a mover una laptop de oficina a oficina, debido a que el perfil del teléfono IP está configurado y a la red IP no le importa donde se encuentre físicamente, aprovechando la infraestructura de una red IP se ahorran costos.

Otro beneficio de *VoIP* es la capacidad de tener solo un departamento de Sistemas de Información (IS) que de soporte a la red de voz y datos.

Varios de los beneficios de *VoIP* se derivan del uso de IP como mecanismo de transporte.

Calidad de Servicio

Calidad de Servicio (QoS) se refiere tanto a la clase de servicio (CoS) y al tipo de servicio (ToS). El objetivo básico de ToS y CoS es lograr el ancho de banda y la latencia necesaria para una aplicación en particular.

CoS permite a un administrador de red agrupar los diferentes flujos de paquetes, cada uno con requisitos de latencia y ancho de banda diferentes. ToS es un campo dentro de una cabecera IP que habilita CoS. Actualmente un campo ToS utiliza tres bits, que permiten ocho grupos de flujo de paquetes, o CoS (0-7). Las nuevas solicitudes de comentarios (RFC's) permitirán seis bits en un campo ToS que por consecuencia permitirá más Cos.

Calidad de Servicio en VoIP

Comúnmente las redes separan físicamente el flujo de voz, video y datos. Estos tipos de tráfico viajan sobre medios separados, por ejemplo líneas dedicadas o cables de fibra óptica. Hoy, sin embargo, los diseñadores de redes buscan aprovechar las redes de datos existentes para transmitir voz y video, logrando así importantes ahorro de costos mediante la reducción de equipos, mantenimiento e incluso de personal.

Hoy en día las redes convergentes presentan un gran reto. Múltiples aplicaciones compiten por el ancho de banda y algunas aplicaciones, por ejemplo voz son más intolerante al retraso, algunas veces llamado latencia, que otras aplicaciones tales como la transferencia de archivos FTP. La falta de ancho de banda representa la mayoría de problemas en calidad.

Entre los problemas que se presentan por la falta de ancho de banda se pueden encontrar los siguientes.

- **Retraso:** Es el tiempo requerido por un paquete para viajar desde su origen hasta su destino.
- ***Jitter*:** Es el resultado de la llegada irregular de paquetes. Un ejemplo es una conversación de VoIP en la que el paquete 1 llega seguido por el paquete 2 20 milisegundos después, luego el paquete 3 llega después de 70 ms. Y el paquete 4 llega

50 ms después detrás del paquete 3. Esta variación en los tiempos de llegada es conocida como *jitter*. Que desde la perspectiva del oyente puede parecer perdida de paquetes.

- **Perdidas:** Routers y switches contienen buffers, para almacenar paquetes cuando el enlace de red, la conexión de red física, carece de suficiente ancho de banda para transmitir los paquetes en el momento. Los paquetes perdidos se producen cuando un enlace esta congestionado y el buffer esta sobrecargado. Algunos tipos de tráfico, como el de internet, retransmiten paquetes perdidos. Sin embargo paquetes de voz y video se pierden definitivamente. Estos tipos de tráfico que utilizan UDP para la transmisión, carecen de la capacidad para retransmitir paquetes peridos.

Capitulo II. Cisco Call Manager

En este capítulo vamos a hablar acerca del rol de los *CallManager's* en las redes de *VoIP*, como un grupo de *CallManager's* trabajan juntos y de cómo los Cisco Call Manager (CCM) sirven como un reemplazo como un reemplazo de las PBX en un entorno de telefonía IP.

CCM es un software que se ejecuta en plataformas de servidores CISCO. El CCM es el encargado de tomar las decisiones de desvió de llamadas, controla los teléfonos IP y puede soportar otras funciones como son las llamadas en conferencia y la transferencia de llamadas, en pocas palabras el CCM es el cerebro de la telefonía IP.

La figura 11 representa el siguiente escenario. Un teléfono IP de CISCO se descuelga. EL teléfono IP le notifica al servidor CCM que el auricular esta descolgado usando el SCCP. El servidor CCM al ver esta condición de descolgado, instruye al teléfono IP para ejecutar el tono de marcación. La persona que llama marca digitando en el teléfono IP y SCCP envía estos dígitos al servidor CCM.

El servidor CCM contiene un plan de marcado, un conjunto de instrucciones para llegar a diversos números de teléfono. Después que el CCM examina los dígitos de marcado y determina cual plan de marcado de entrada usar, el servidor CCM señala a la IP del teléfono de destino que este está recibiendo una llamada. Después que el teléfono de destino se descuelga, un flujo RTP se establece directamente entre los teléfonos.

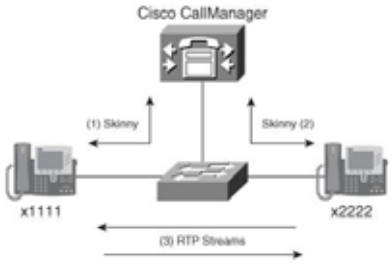

Figura 11 Flujo de Llamada

Para lograr el nivel de disponibilidad de un entorno PBX, se pueden tomar múltiples servidores CCM y agruparlos lógicamente. Estas agrupaciones de CCM's son llamadas clúster. Cada uno de los servidores CCM en el clúster necesita la misma información de base de datos, ya que en cualquier momento un servidor puede ser llamado como una copia de seguridad de otro servidor. Para mantener estas bases de datos sincronizadas se designa un único servidor del clúster como Editor. La nueva información en la base de datos solo puede ser escrita por el Editor. El servidor Editor envía las actualizaciones a los servidores suscritos, estos servidores suscritos tienes una copia de la base de datos solo de lectura. Este proceso de copia de información de la base de datos del servidor Publisher a los servidores suscritos se denomina replicación. Esta replicación de la base de datos incluye tanto información como registro y datos de acceso.

Los clúster de CCM's también intercambian datos en tiempo de ejecución, usando una topología lógica mallado completo, estos datos en tiempo de ejecución incluyen tanto información como detalles de las llamadas en progreso, Gateway y el registro de los teléfonos IP, así como información de los recursos DSP.

Un ejemplo de datos en tiempo de ejecución es un teléfono IP registrándose con un CCM. El CCM permite a los demás CCM's en el clúster saber acerca del registro. Entonces el teléfono IP envía un mensaje *keepalive* a su CCM primario de que se ha registrado en el cada 30 segundos. Para la redundancia el teléfono IP envía también un mensaje de conexión TCP aún CCM de respaldo, por lo que el teléfono se puede conectar en caso de falla del CCM primario al de respaldo. También se puede configurar el teléfono IP con un tercer CCM con el que se podrá conectar en caso que el primario y el de respaldo fallen.

Topologías de CCM

Dependiendo de las necesidades de una empresa se pueden seleccionar uno de los cuatro tipos de topologías.

- **En sitio:** Los teléfonos IP y los CCM se localizan en el mismo sitio.
- **Procesamiento de llamada centralizado:** Los teléfonos IP están en sitios diferentes y todos los CCM's en un solo sitio.
- **Procesamiento de llamada distribuido:** Tanto los teléfonos IP como los CCM's se encuentran en diferentes sitios.
- **Clustering sobre una WAN:** Los teléfonos IP y los CCM's se encuentran en múltiples sitios, con todos los CCM's lógicamente asignados al mismo clúster.

En Sitio

Una implementación de telefonía IP en un solo lugar, como se muestra en la figura 12, usa la LAN de alta velocidad de ese lugar, el PSTN es usado para hacer llamadas al exterior. En este caso el ancho de banda dedicado a la voz no es una consideración importante en este diseño, y el G.711 es típicamente el CODEC a elegir. Típicamente la implementación de un solo sitio consiste en un solo grupo por lo tanto todos los teléfono IP se registran en este mismo grupo por lo cual el plan de marcado se simplifica.

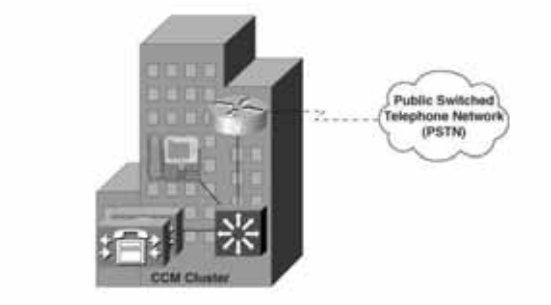

Figura 12 Implementación en Sitio

Si la red de datos existente utiliza un diseño de alta disponibilidad, entonces los componentes de telefonía IP también pueden disfrutar de alta disponibilidad, ya que estos componentes se conectan a la red de datos existente.

Modelo de Procesamiento de Llamadas Centralizado

A veces, las empresas desean ampliar su red de telefonía IP más allá de la sede central, llegando a las oficinas remotas, Figura 13. Sin embargo, muchas veces el tamaño relativamente pequeño de estas oficinas remotas no justifica la compra de servidores CCM. Un modelo de procesamiento de llamadas centralizado permite que los teléfonos IP ubicados en los sitios remotos se registren en el clúster de CCM's ubicado en el sitio central. El sitio central no solo contiene clúster de CCM's si no también contiene DSP's que los teléfonos IP remotos utilizan para funciones que incluyen conferencias y transcodificación, la conversión entre los diferentes CODECS. Un modelo de implementación centralizada utiliza normalmente el CODEC G.729, que solo requiere 8kbps de ancho de banda para la carga útil de voz, a través de la WAN IP para la conservación de ancho de banda.

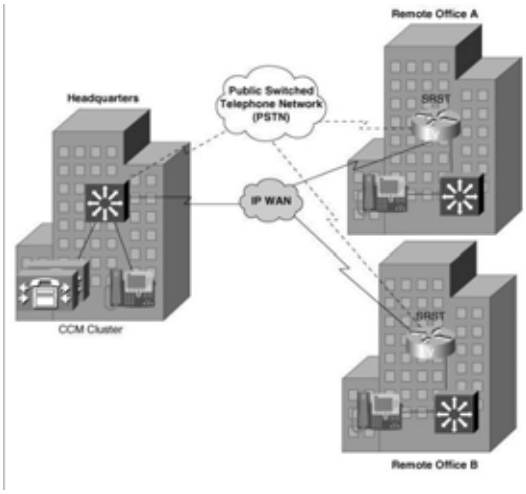

Figura 13 Modelo de Procesamiento de Llamadas Centralizado

El mantenimiento en los sitios remotos es mínimo ya que no hay servidores CCM en estos sitios. Sin embargo hay que tener en cuenta que la WAN IP puede presentar fallos y volverse inaccesible, debido a esto los teléfonos IP que pertenecen al clúster ubicado en la sede central pierden

conectividad con su CCM. Para dar solución a este tipo de fallo en la WAN IP, se puede utilizar el *Cisco Survivable Remote Site Telephony* (SRST) en estos sitios como se muestra en la figura 5.

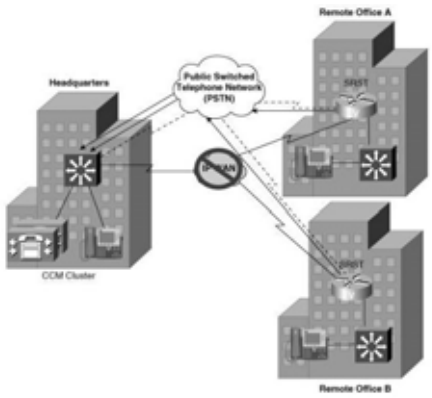

Figura 14 Survivable Remote Site Telephony

SRST permite a un router Cisco IOS intervenir y hacerse cargo de las tareas de procesamiento de llamadas de los teléfonos IP en los sitios remotos en caso de una falla de la WAN. A pesar de que un enrutador SRST no proporciona todos los tonos disponibles en un servidor de CCM, un enrutador SRST no solo soporta funciones básicas, permite que los teléfonos IP en el sitio remoto llamarse entre ellos, también llamar fuera de la PSTN.

Modelo de Procesamiento de Llamadas Distribuido

Empresas con múltiples ubicaciones remotas pueden optar por un modelo de procesamiento de llamadas distribuido, se puede definir como la implementación opuesta al modelo de procesamiento de llamadas centralizado, ya que cuenta con clústers de CCM's en cada una de las ubicaciones remotas como se muestra en la figura 6.

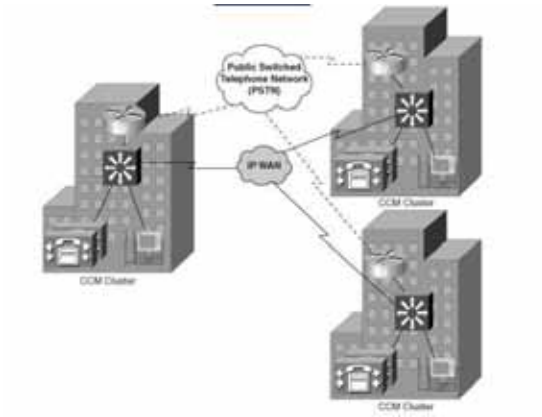

Figura 15 Modelo de Procesamiento de Llamadas Distribuido

Una de las ventajas de este modelo es que cada sitio contiene su propio clúster de CCM's, por lo que son mínimamente afectados por fallas en la IP WAN. Sin embargo existe la posibilidad de que el ancho de banda para la IP WAN se sature debido a demasiadas llamadas de voz. Por lo tanto un modelo de implementación de distribuida a menudo utiliza un *gatekeeper* para realizar un

seguimiento del número de llamadas que son realizadas entre los sitios. Conforme el uso de banda ancha se va acercando a su máxima capacidad el gatekeeper puede denegar intentos de llamada adicionales. El gatekeeper es el encargado de decidir si una llamada puede o no cruzar la IP WAN.

Clustering Sobre una WAN

La opción final para implementar servidores CCM a través de múltiples sitios geográficos es el modelo de clúster sobre una red WAN. Este modelo ofrece el plan de marcación simplificada del modelo de implementación centralizada y la alta disponibilidad del modelo de implementación distribuida, tal como se muestra en la figura 7.

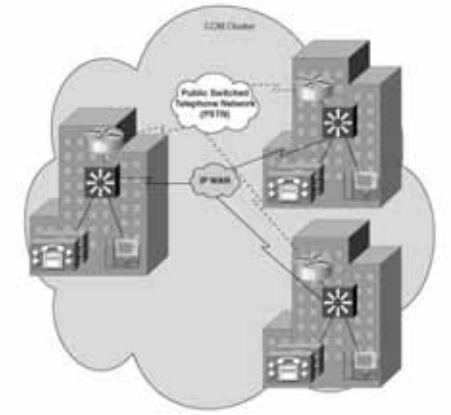

Figura 16 Clustering Sobre una WAN

Capítulo III. Red Privada Virtual

La expresión VPN a menudo se asocia con la conectividad de la empresa, cuando trabajadores remotos acceden a la red corporativa, pero actualmente el concepto está ganando popularidad entre los usuarios caseras y las pequeñas organizaciones. Con la VPN, dos o más computadoras o redes remotas pueden conectarse entre sí, de forma segura, para formar una red local virtual que utiliza una infraestructura pública como Internet, como medio para transmitir datos internos.

Se denomina VPN porque no se trata de una red física, pero tiene todas las características de una red de área local (LAN, *Local Area Network*). Este tipo de estructuras benefician a las personas y a las organizaciones, pues les permiten establecer conexiones de red de confianza y utilizar herramientas cooperativas y convencionales, tales como compartir impresoras y archivos, realizar conferencias en red y demás, desde cualquier punto donde haya acceso a internet.

Además de proporcionar conectividad, las redes privadas virtuales tienen un impacto muy importante en la seguridad: pueden mantener los datos privados, a pesar de estar utilizando puntos de conexión a internet seguros, tales como proveedores de servicio de red desconocidos, o acceso inalámbrico en sitios públicos.

Tipos de VPN's

De una forma simple, una VPN conecta dos puntos finales a través de una red pública para establecer una conexión lógica. La conexión lógica se puede establecer de tanto en la capa 1 como en la capa 2 del modelo OSI, por lo cual los diferentes modelos de conexión de VPN's se pueden clasificar en VPN's de capa 2 y VPN's de capa 3. Ejemplos de de VPN's de capa 2 son ATM y Frame Relay, mientras que ejemplos de VPN's de capa 3 son GRE, L2TP, MPLS e IPSec.

VPN's de Capa 2

Este tipo de VPN's trabajan en la capa de del modelo OSI, son punto a punto y establecen la conexión entre los sitios a través de un circuito virtual. El circuito virtual es configurado extremo-a-extremo y es usualmente llamado circuito virtual permanente (PVC). Un circuito virtual punto a punto dinámico también es posible y es conocido como circuito virtual conmutado (SVC), son usados con menos frecuencia debido a su complejidad. ATM y *Frame Relay* son de las tecnologías VPN's de capa 2 más populares, los proveedores de ATMA y *Frame Relay* pueden ofrecer conexiones privadas sitio-a-sitio a empresas configurando un PVC a través de una red compartida.

VPN's de Capa 3

Las conexiones entre sitios pueden definirse de capa 3 sí la cabecera de entrega es de capa 3 del modelo OSI. Las VPN's de capa 3 pueden ser punto a punto para conectar dos sitios tal como son GRE e IPSec, o pueden establecer una conexión muchos-a-muchos a varios sitios usando MPLS VPN's.

GRE Túnel

Encapsulación de Enrutamiento Genérico (GRE) originalmente desarrollado por Cisco y estandarizado como RFC 1701. Un GRE túnel entre dos sitios que tienen accesibilidad IP puede ser descrito como una VPN, ya que los datos privados entre los sitios se encapsulan en la cabecera de entrega de GRE.

Es posible conectar varios sitios de una empresa usando túneles GRE a través de internet. Aunque rara vez son implementadas debido a la falta de mecanismos de seguridad asociados con GRE.

MPLS VPN's

Conmutación Multiprotocolo por Etiquetas originalmente conocido como conmutación de etiquetas y posteriormente estandarizado a través de la IETF como MPLS. Un principio común entre las tecnologías para implementar VPN's es la encapsulación de los datos privados con una cabecera de entrega, las MPLS VPN's usan etiquetas para encapsular los datos originales, o carga útil, para formar una VPN entre los sitios.

IPSec VPN's

Una de las principales preocupaciones para las personas que utilizan cualquier tipo de VPN es la seguridad de los datos cuando estos viajan a través de una red pública.

La encriptación de los datos es una forma de protegerlos. La encriptación de datos se puede lograr implementando equipos que puedan encriptar y desencriptar en cada sitio. IPSec es un conjunto de protocolos desarrollados bajo el auspicio de la IETF para lograr servicios seguros a través de redes IP. Una VPN implementada a través de la Internet puede significar importantes ahorros para una empresa comparado con una línea dedicada para VPN.

Los servicio de IPSec permiten la autenticación, integridad, control de accesos y confidencialidad. Con IPSec, el intercambio de información entre dos sitios remotos puede ser encriptada y verificada. Tanto clientes de acceso remoto y VPN's punto a punto pueden implementarse usando IPSec.

VPN's de Acceso Remoto

Las VPN's se también se pueden clasificar en VPN's site-to-site y VPN's de accesos remoto. Frame Relay, ATM, GRE y MPLS VPN, se pueden considerar sitio a sitio, ya que la información relevante para la configuración entre los sitios se conoce de antemano por ambos lados y más importante aún son de tipo estático y por lo tanto no cambia dinámicamente. Por otro lado, supongamos que un trabajador remoto necesita acceso a los datos de la empresa por medio de la VPN a través de la Internet. La información necesaria para establecer la conexión a la VPN así como la dirección IP del trabajador remoto cambian dinámicamente dependiendo de la localización de este por lo tanto no se conoce la información del otro lado de la VPN. Este tipo de VPN puede ser clasificada como una VPN de acceso remoto.

Las redes de acceso telefónico proporcionan una solución de acceso local universal, son muy costosas, las conexiones de acceso remoto VPN proporcionan una mejor solución ya que permiten aprovechar las últimas tecnologías de acceso de última milla como son el cable y DSL.

Dos de los métodos de acceso remoto para VPN más comunes *son Layer 2 tunneling protocol* (L2TP) e IPSec. L2TP es un estándar IETF (RFC 2661) para transportar *frames* PPP sobre IP. L2TP provee a los usuarios de acceso telefónico con una conexión virtual a una puerta de enlace empresarial sobre una red IP, que puede ser la Internet. La figura 3 muestra el modelo L2TP.

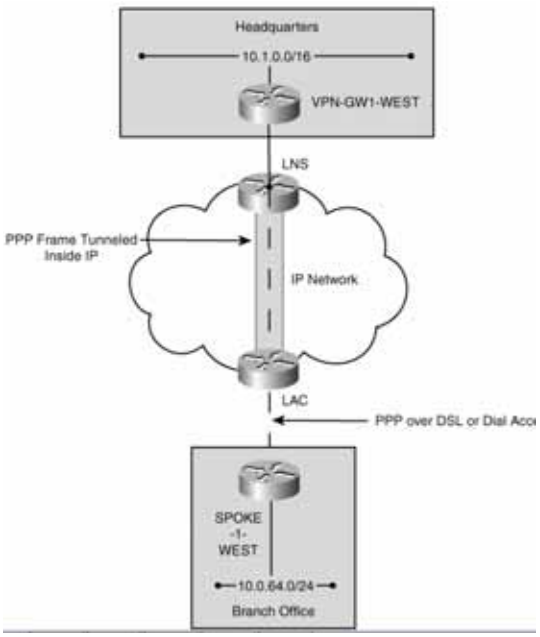

Figura 17 VPN de Acceso Remoto L2TP 1

El usuario remoto inicia una sesión PPP con el servidor de acceso, conocido como concentrador de acceso local (LAC) a través de una llamada telefónica local. El LAC autentifica al usuario remoto y determina en cual servidor de red local (LNS) terminara el usuario. El túnel L2TP es establecido entre el LAC y el LNS una vez que el LNS ha autentificado al usuario, una interfaz virtual para la terminación de PPP se crea en el LNS análoga a una conexión de marcado directo a la LNS.

IPSec es otra tecnología VPN que también puede ser usada para conectar usuarios de forma remota. IPSec también se puede implementar el modelo de cliente de acceso remoto donde permite al cliente usar una dirección IP asignada dinámicamente, también permite que los administradores de la red definir una política que es mandada al cliente para simplificar la gestión de las operaciones de la red. IPSec por sí sola no proporciona estos atributos, para lograrlo implementando la extensión IKE. El proceso de configuración de modo IKE asigna atributos de conexión con el cliente. Los atributos asignados típicos incluyen.

- Dirección IP privada.
- Servidor DNS privado.
- Servidor WINS privado.
- Nombre de Dominio privado.

La dirección IP privada generalmente es asignada desde un pool de conexiones configurado en el concentrador. Luego, un proxy IPSec es creado para proteger el tráfico desde la dirección privada asignada hacia un rango de direcciones protegidas por el concentrador. El concentrador anuncia el pool de direcciones a otros dispositivos de la red de tal manera que un camino de retorno es proporcionado al cliente. Normalmente el cliente dirige todo el tráfico del usuario al concentrador cuando la división de los túneles no está permitida.

El modelo de cliente de acceso remoto simplifica el proceso de aprovisionamiento mediante la automatización de la distribución de políticas a los clientes usando el IKE en modo de configuración global. Las políticas de protección pueden ser definidas y gestionadas de una forma central de tal manera que el administrador de la red no requiera configurar cada punto final remoto. Se pueden encontrar dos desventajas en este modelo. Primera, la conexión IPSec solo puede ser iniciada desde el cliente hacia el servidor. Segunda, la conexión usa una sentencia simple de proxy IPSec que no soporta multicast.

IPSec

Un error común de acerca de IPSec es que es un único protocolo para proveer servicios de seguridad para el tráfico IP. IPSec es una colección de seguridad definidos por el grupo de trabajo IPSec en el IETF. La arquitectura IPSec y los componentes principales de IPSec se definen en el RFC2401 como sigue.

- **Protocolos de seguridad:** Cabeceras de autenticación, AH, y encapsulación de seguridad de la carga útil, ESP.
- **Manejo de llaves:** ISAKMP, IKE, SKEME.
- **Algoritmos:** Para la encriptación y la autenticación.

El objetivo de IPSec es el de proveer servicios de seguridad para los paquetes IP en la capa de red. Estos servicios incluyen control de accesos, integridad de datos, autenticación, confidencialidad de datos y protección contra la replicación.

ESP y AH son dos protocolos IPSec usados para proveer esta seguridad a los datagramas IP. Para entender más a fondo estos protocolos es necesario entender los dos modos de IPSec, el de transporte y el de túnel, y los servicios que proporciona cada uno.

IPSec en Modo de Transporte

En este modo la cabecera IPSec (AH o ESP) es insertada entre la cabecera IP y la cabecera del protocolo de capa superior, figura 10.

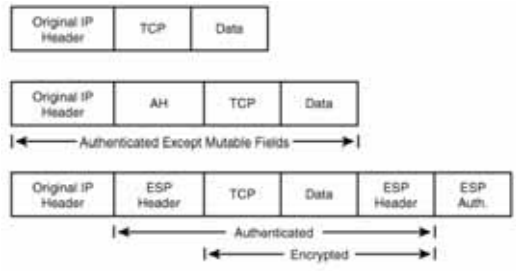

Figura 18 Paquete IP en IPSec Modo Transporte

En este modo, la cabecera IP es la misma que la del paquete original excepto por el campo del protocolo IP, el cual es cambiado por ESP(50) o AH(51), y el checksum de la cabecera IP, que es recalculado. IPSec asume que el punto destino es alcanzable. En este modo la dirección IP de destino en la cabecera IP no es cambiada por el punto de origen IPSec.

Desde el punto de vista de una VPN IPSec, este modo es el más usado cuando el tráfico entre dos hosts debe ser protegido.

IPSec en Modo de Túnel

El servicio de VPN IPSec utiliza el modo de transporte y la encapsulación GRE entre las puertas de enlace de la VPN de cada sitio. En el modo de túnel, la IP del paquete original es encapsulada en otro datagrama IP, y la cabecera IPSec (AH o ESP), es insertada entre los encabezados interiores y exteriores.

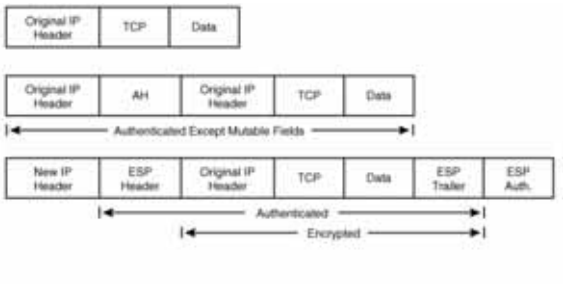

Figura 19 Paquete IPSec en Modo de Túnel

Cabecera de Seguridad de Encapsulación

ESP provee de confidencialidad, integridad de datos, autenticación del origen de los datos y servicios de antirepetición. Provee estos servicios encriptando la carga útil original y encapsulando los paquetes entre la cabecera y la cola, tal como se muestra en la figura 20.

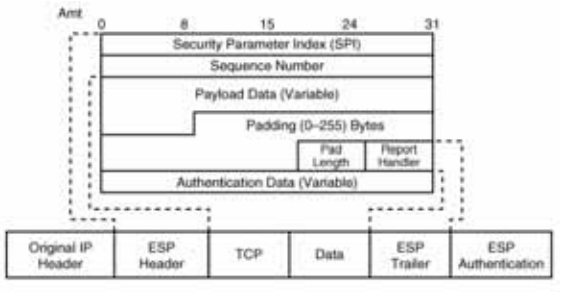

Figura 20 Paquete IP Protegido por ESP

La cabecera puede contener una nueva cabecera IP en modo túnel o la cabecera IP del paquete original en el modo transporte como se muestra en la figura 21 y 22 respectivamente.

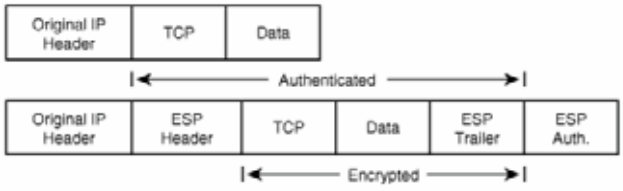

Figura 21 Paquete Protegido por ESP en Modo Transporte

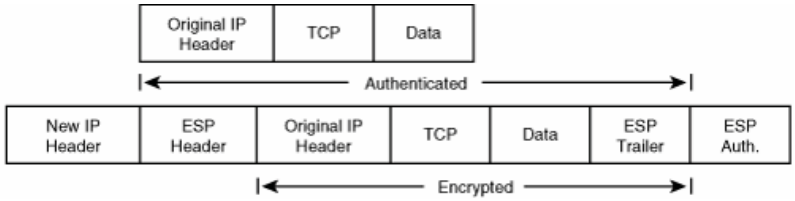

Figura 22 Paquete IP Protegido por ESP en Modo Túnel

Cabecera de Autenticación AH

AH proporciona integridad sin conexión, autenticación de datos, y opcionalmente protección de repetición, pero a diferencia de ESP, este no provee confidencialidad, figura 23.

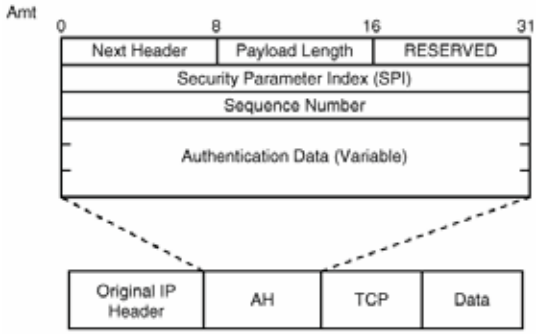

Figura 23 Paquete IP Protegido por AH

AH es un protocolo IP, identificado con un valor de 51 en la cabecera IP. El siguiente campo del encabezado indica que sigue del encabezado AH. En modo transporte, este puede ser el valor del protocolo de la capa siguiente a proteger, por ejemplo UDP o TCP, figura 24. En modo túnel este valor es 4, figura 25.

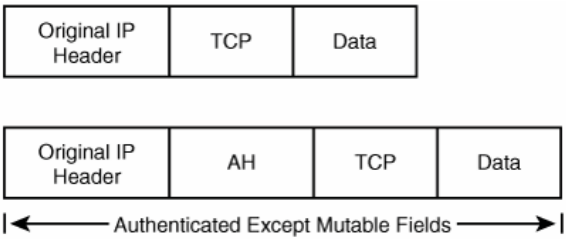

Figura 24 Paquete IP Protegido por AH en modo Transporte

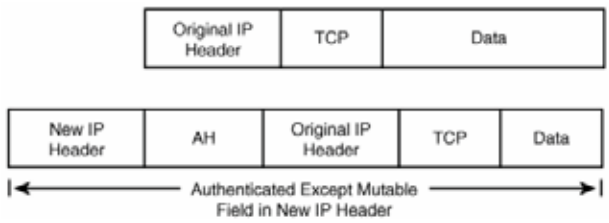

Figura 25 Paquete IP protegido por AH en Modo Túnel

Capítulo IV. NAT

NAT es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles. Consiste en convertir, en tiempo real, las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

El tipo más simple de NAT proporciona una traducción una-a-una de las direcciones IP. La RFC 2663 se refiere a este tipo de NAT como NAT Básico, también se le conoce como NAT una-a-una. En este tipo de NAT únicamente, las direcciones IP, las sumas de comprobación (*checksums*) de la cabecera IP, y las sumas de comprobación de nivel superior, que se incluyen en la dirección IP necesitan ser cambiadas. El resto del paquete se puede quedar sin tocar (al menos para la funcionalidad básica del TCP/UDP, algunos protocolos de nivel superior pueden necesitar otra forma de traducción). Es corriente ocultar un espacio completo de direcciones IP, normalmente son direcciones privadas IP, detrás de una única dirección IP (o pequeño grupo de direcciones IP) en otro espacio de direcciones (normalmente público).

NAT es como el recepcionista de una oficina grande. Imagine que le indica al recepcionista que no le pase ninguna llamada a menos que se lo solicite. Más tarde, llama a un posible cliente y le deja un mensaje para que le devuelva el llamado. A continuación, le informa al recepcionista que está esperando una llamada de este cliente y le solicita que le pase la llamada a su teléfono.

El cliente llama al número principal de la oficina, que es el único número que el cliente conoce. Cuando el cliente informa al recepcionista a quién está buscando, el recepcionista se fija en una tabla de búsqueda que indica cuál es el número de extensión de su oficina. El recepcionista sabe que el usuario había solicitado esta llamada, de manera que la reenvía a su extensión.

Entonces, mientras que el servidor de DHCP asigna direcciones IP dinámicas a los dispositivos que se encuentran dentro de la red, los routers habilitados para NAT retienen una o varias direcciones IP de Internet válidas fuera de la red. Cuando el cliente envía paquetes fuera de la red, NAT traduce la dirección IP interna del cliente a una dirección externa. Para los usuarios externos,

todo el tráfico que entra a la red y sale de ella tiene la misma dirección IP o proviene del mismo conjunto de direcciones.

Su uso más común es permitir utilizar direcciones privadas (definidas en el RFC 1918) para acceder a Internet. Existen rangos de direcciones privadas que pueden usarse libremente y en la cantidad que se quiera dentro de una red privada. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado. Esto es necesario debido al progresivo agotamiento de las direcciones IPv4. Se espera que con el advenimiento de IPv6 no sea necesario continuar con esta práctica.

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino. Esta combinación de números define una única conexión.

La mayoría de los NAT asignan varias máquinas (hosts) privadas a una dirección IP expuesta públicamente. En una configuración típica, una red local utiliza unas direcciones IP designadas "privadas" para subredes (RFC 1918). Un ruteador en esta red tiene una dirección privada en este espacio de direcciones. El ruteador también está conectado a Internet por medio de una dirección pública asignada por un proveedor de servicios de Internet. Como el tráfico pasa desde la red local a Internet, la dirección de origen en cada paquete se traduce sobre la marcha, de una dirección privada a una dirección pública. El ruteador sigue la pista de los datos básicos de cada conexión activa (en particular, la dirección de destino y el puerto). Cuando una respuesta llega al ruteador utiliza los datos de seguimiento de la conexión almacenados en la fase de salida para determinar la dirección privada de la red interna a la que remitir la respuesta.

Todos los paquetes de Internet tienen una dirección IP de origen y una dirección IP de destino. En general, los paquetes que pasan de la red privada a la red pública tendrán su dirección de origen modificada, mientras que los paquetes que pasan a la red pública de regreso a la red privada tendrán su dirección de destino modificada. Existen configuraciones más complejas.

Para evitar la ambigüedad en la forma de traducir los paquetes de vuelta, es obligatorio realizar otras modificaciones. La mayor parte del tráfico generado en Internet son paquetes TCP y UDP, para estos protocolos los números de puerto se cambian, así la combinación de la información de IP y puerto en el paquete devuelto puede asignarse sin ambigüedad a la información de dirección privada y puerto correspondiente. Los protocolos que no están basados en TCP y UDP requieren de otras técnicas de traducción Los paquetes ICMP normalmente se refieren a una conexión existente y necesitan ser asignado utilizando la misma información de IP. Para el ICMP al ser una conexión existente no se utiliza ningún puerto.

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan

en una tabla, para recordar qué dirección y puerto le corresponde a cada dispositivo cliente y así saber dónde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla en un determinado puerto y dirección se puede acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina **NAT inverso** o **DNAT** (Destination NAT).

NAT tiene muchas formas de funcionamiento, entre las que destacan:

- **Estática:** Conocida también como NAT 1:1, es un tipo de NAT en el que una dirección IP privada se traduce a una dirección IP pública, y donde esa dirección pública es siempre la misma. Esto le permite a un host, como un servidor Web, el tener una dirección IP de red privada pero aun así ser visible en Internet. Para ello usa la técnica llamada Redirección de puertos (en inglés *port forwarding*).
- **Dinámica:** Es un tipo de NAT en la que una dirección IP privada se mapea a una IP pública basándose en una tabla de direcciones de IP registradas (públicas). Normalmente, el router NAT en una red mantendrá una tabla de direcciones IP registradas, y cuando una IP privada requiera acceso a Internet, el router elegirá una dirección IP de la tabla que no esté siendo usada por otra IP privada. Esto permite aumentar la seguridad de una red dado que enmascara la configuración interna de una red privada, lo que dificulta a los hosts externos de la red el poder ingresar a ésta. Para este método se requiere que todos los hosts de la red privada que deseen conectarse a la red pública posean al menos una IP pública asociadas.
- **Sobrecargado**: La más utilizada es la NAT de sobrecarga, conocida también como PAT (*Port Address Translation* - Traducción de Direcciones por Puerto), NAPT (*Network Address Port Translation* - Traducción de Direcciones de Red por Puerto), NAT de única dirección o NAT multiplexado a nivel de puerto.
- **Solapamiento**: Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red, el enrutador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evitan los conflictos de direcciones entre las distintas redes.

Problemas de NAT con VoIP

Los protocolos de VoIP convencionales solo manejan la señalización de la conexión telefónica. El tráfico de voz es manejado por otro protocolo y para empeorar las cosas el puerto por donde el audio es enviado se elige al azar. El router configurado con NAT puede ser capaz de manejar las señalizaciones de tráfico, pero no tiene forma de saber que el tráfico de voz está relacionado con la señalización y por lo tanto el tráfico de voz se debe pasar por el mismo dispositivo por donde el tráfico de señalización pasa, como resultado se obtiene que el tráfico de voz no es traducido correctamente.

En un primer momento, tanto para el que llama como para el que recibe la llamada, parece que todo funciona correctamente. El que recibe la llamada vera el ID de el que llama mientras que el que llama escuchara un tono de timbre de realimentación. Cuando el que es llamado descuelga

el teléfono tanto el timbre como el tono de timbre de realimentación se detendrán como debía esperarse. Sin embargo la persona que llama no escuchara al que es llamado, audio unidireccional, y puede que la persona llamada no escuche al que llama, no habrá audio.

Se pueden presentar problemas con la calidad del audio, se pueden presentar problemas para recibir llamadas ya que los puertos para la señalización de las llamadas así como los puertos para la media de RTP y los flujos de RTCP no se encuentran direccionados.

Desarrollo del Proyecto

El proyecto consta de implementar una VPN IPSec *site-to-site* que se conectara a través de la internet, también contara con soporte para realizar llamadas VoIP, donde el servidor CCM será configurado en un extremo de la VPN, router A, y será el encargado de dar el soporte de VoIP a través de la VPN, esta implementación contará con la capacidad de conectarse a internet por medio de NAT lo que permitirá a los equipos que se encuentran de lado de los extremos de la VPN conectarse a internet por medio de PAT y no podrán ser accesados por equipos que no pertenezcan a la VPN, el router B solo cuenta con la configuración necesaria para ser parte de la VPN punto a punto,nuestra arquitectura quedara como se muestra en la figura 11. Cada extremo de la VPN contara con su propio DHCP.

En nuestra implementación utilizaremos el Cisco IP Communicator para simular los teléfonos IP dentro de nuestros equipos.

La configuración completa de nuestros routers se encuentran en los entregables A y B, el entregable A muestra la configuración del router el cual implementaba el servicio de telefonía así como la implementación del extremo de la VPN que le corresponde, el entregable B muestra la configuración del router solo con la implementación del extremo de la VPN que le corresponde. También como entregables se encuentran las capturas del tráfico mientras se realizaba la llamada, capturadas con *wireshark*, los cuales se anexan al cd, para la laptop *Vaio* el entregable es ACAP y para la laptop *Compaq* es el entregable BCAP.

A continuación se presentan las características de los equipos que se utilizaron para la implementación de nuestra arquitectura.

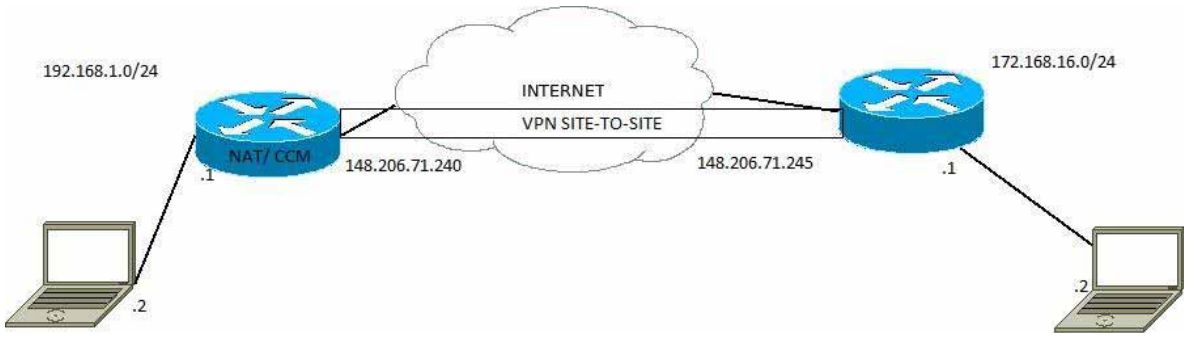

Figura 26 Arquitectura Proyecto

Hardware

- 2 Router Cisco 2811
- Laptop Sony Vaio
    - 8GB RAM
    - Procesador Intel Core I5 qA
- Laptop Compaq
    - 4GB RAM
    - Procesador Intel Celeron

Software

- Cisco IOS c2800nm-adventerprisek9-mz.124-15.T1
- Cisco.IP.Communicator.v.8.6
- Wireshark 1.10.5
- Windows 7

Cisco IP

Es un software basado en los teléfonos IP. El Cisco IP Communicator permite al usuario llevar su teléfono IP con el de un lado a otro. El Cisco IP Communicator ofrece las siguientes funciones y características figura 20:

- No requiere software de proveedores de servicios de telefonía, TSP.
- Soporte para los codecs G.711, G.729a, SCCP, iSAC, G.722, G.729a, G.729ab, G.729b, G711a.
- Soporta SCCP y SIP.
- Cinco teclas programables.
- Ocho botones de marcación dial/speed.
- Compatibilidad con XML.

Figura 27 Cisco IP Communicator.

Router Cisco 2811

El router Cisco 2811 es parte de la serie Cisco 2800 de servicios integrados, proporciona los siguientes soportes.

- Alto rendimiento para servicios concurrentes como voz y seguridad.
- Mayor protección de la inversión a través de un mayor rendimiento e inversión de la modularidad.
- Mejora de la ranura del módulo de red.
- Seguridad:
  - Cifrado on-board.
  - Soporte de hasta 1500 túneles VPN.
  - Soporte de antivirus a través de NAC.
  - Prevención de intrusiones.
- Voz:
  - Soporte de llamadas analógicas y digtales.
  - Soporte para buzón de voz.
  - Soporte opcional para CCME, para el procesamiento de llamadas locales para un máximo de 36 teléfonos IP.
  - Soporte opcional para SRST para el procesamiento de llamadas locales para un máximo de 36 teléfonos IP.

Cisco IOS c2800nm-adventerprisek9-mz.124-15.T1

Este IOS de Cisco cuenta con las siguientes características:

- **K9**: Contiene el protocolo de encriptación 3DES.
- **mz:** La versión de IOS corre desde la RAM y se encuentra comprimida.
- **124-15.T1:** Es una versión de IOS 124 release 15 y es una imagen e tipo T versión 1.
- **adventerprise:** Por ser una versión Enterprise contiene todas las funcionalidades, figura 20.

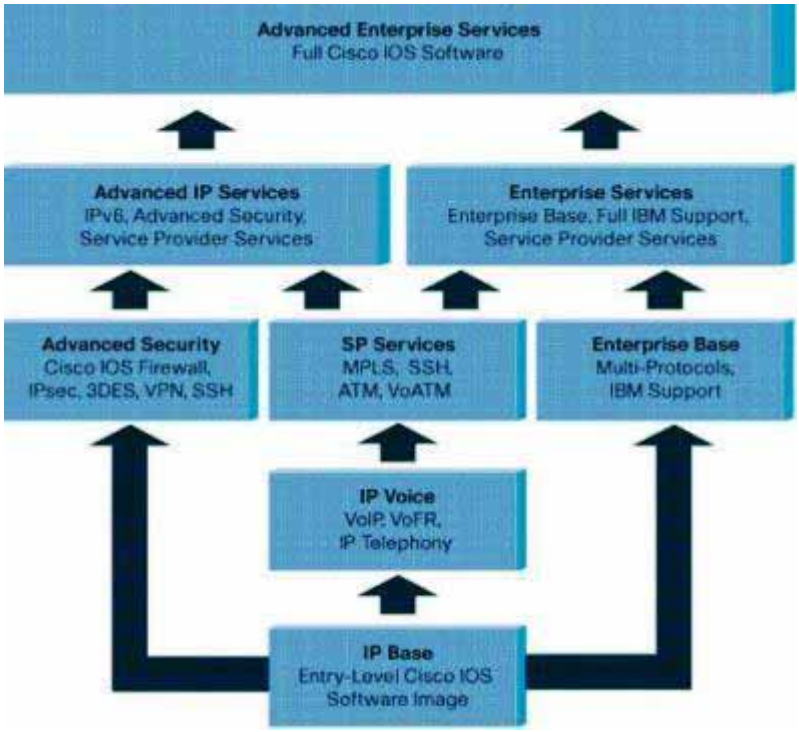

Figura 28. IOS Cisco.

IPSEC Site to Site

#Habilitamos IPSEC

Router(config)#crypto isakmp enable

#Se establece una nueva política isakmp

Router(config)#crypto isakmp policy 1

#Se utiliza un método de autenticación compartido

Router(config-isakmp)#authentication pre-share

#Se utiliza una encriptación simétrica

Router(config-isakmp)#encryption aes

#Se utiliza el algoritmo hash sha para la integridad de datos

Router(config-isakmp)#hash sha

#Se define el grupo helman

Router(config-isakmp)#group 2

Router(config-isakmp)#exit

#Se crea la clave que se usara para autentificar al otro extremo de la vpn

Router(config)#crypto isakmp key 0 address 11.0.0.1 0.0.0.0

#Se establece el protocolo para la protección de datos

Router(config)#crypto ipsec transform-set yasser esp-aes esp-sha-hmac

#El tiempo después del cual expirara la clave

Router(config)#crypto ipsec security-association lifetime seconds 86400

#Se establece una lista de acceso para el tráfico de la VPN

Router(config)#ip 36ccess-list extended ramzy

#Se establecen las redes que podrán tener acceso a la vpn

Router(config-ext-nacl)#permit ip 12.0.0.0 0.255.255.255 10.0.0.0 0.255.255.255

Router(config-ext-nacl)#exit

#Se crea un crypto map.

Router(config)#crypto map auda 100 ipsec-isakmp

% NOTE: This new crypto map will remain disabled until a peer

and a valid access list have been configured.

#Se liga la ACL con el crypto map

Router(config-crypto-map)#match address ramzy

#Se liga el otro extremo con el crypto map

Router(config-crypto-map)#set peer 11.0.0.1

#Se liga el grupo al crypto map

Router(config-crypto-map)#set pfs group2

#Se liga el transform set

Router(config-crypto-map)#set transform-set yasser

Router(config-crypto-map)#ex

Router(config)#int fa 0/1

#Se liga el crypto map a una interface

Router(config-if)#crypto map auda

Servicio de Telefonía

```
#configuramos el servicio de telefonÃa
telephony-service
#Definimos el número de teléfonos
      max-ephones 5
#Define el número de línea
      max-ephones 5
#ip encargada del servicio de telefonia sobre el puerto 2000
      ip source-address 10.0.1.1 port 2000
      exit
#Configuramos una línea
ephone-dn 1
```

#Configuramos el número de la línea

number 1111

#Configuramos el teléfono físico

ephone 1

#Le Asignamos la mac-address del teléfono.

mac-address 30F9.EDA1.EB49

#Establecemos el tipo de telefono

type CIPC

#Asignamos una línea al botón.

button 1:1

PAT

Enable

configure terminal

#Configuramos la dirección IP para la interface de salida

interface fastEthernet 0/0

ip address 192.168.121.1 255.255.255.0

#Habilitamos la interfaz

no shutdown

exit

#Configuramos la dirección IP para la interface de entrada

interface fastEthernet 0/1

ip address 10.0.0.1 255.255.255.0

#La habilitamos

no shutdown

exit

#Creamos una ruta estática y la direccionamos a la interfaz de salida

ip route 0.0.0.0 0.0.0.0 fastEthernet 0/0

#Creamos una lista de acceso con la red a la cual vamos aplicar PAT

access-list 100 permit ip 10.0.0.0 0.0.0.255 any

#Ligamos la lista de acceso con la interface de salida

ip nat inside source list 100 interface fastEthernet 0/0 overload

#Declaramos la interface de salida como salida de nat

interface fastEthernet 0/0

ip nat outside

exit

#Declaramos la interface de entrada con entrada de nat.

interface fastEthernet 0/1

ip nat inside

exit

Resultados y Análisis de Resultados

Tras la implementación de nuestra arquitectura realizada en el laboratorio de redes obtuvimos los siguientes resultados.

La figura 29, contiene el resultado al ejecutar el comando show crypto ipsec sa, que muestra el número de paquetes encriptados y decriptados en el router A al momento de ejecutarlo.

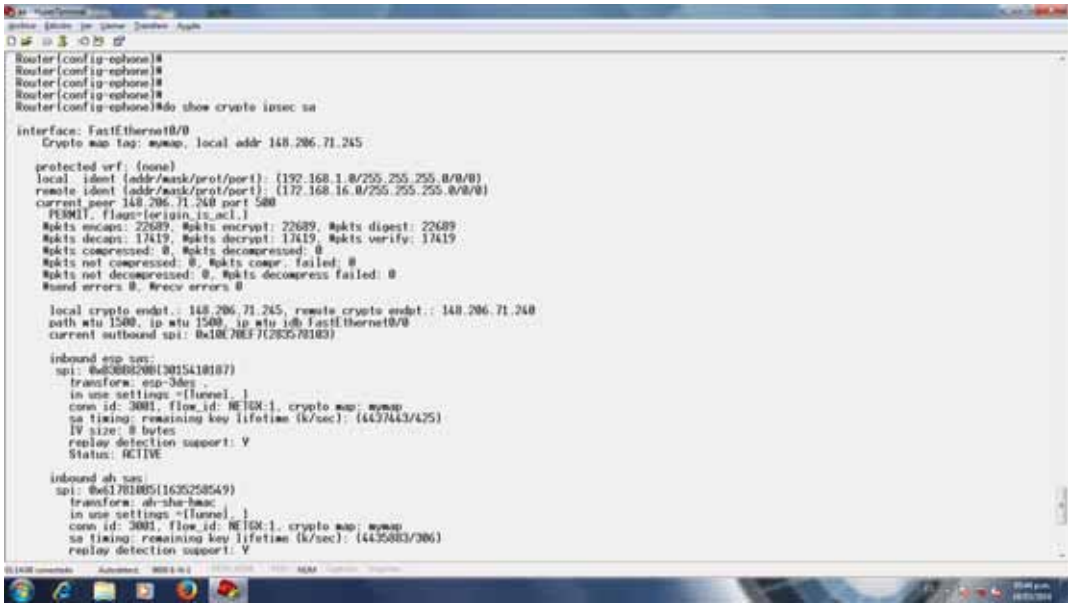

Figura 29 show crypto ipsec sa router A

La figura 30, muestra los paquetes encriptados y desencriptados por el router B al momento de ejecutar el comando show crypto ipsec sa.

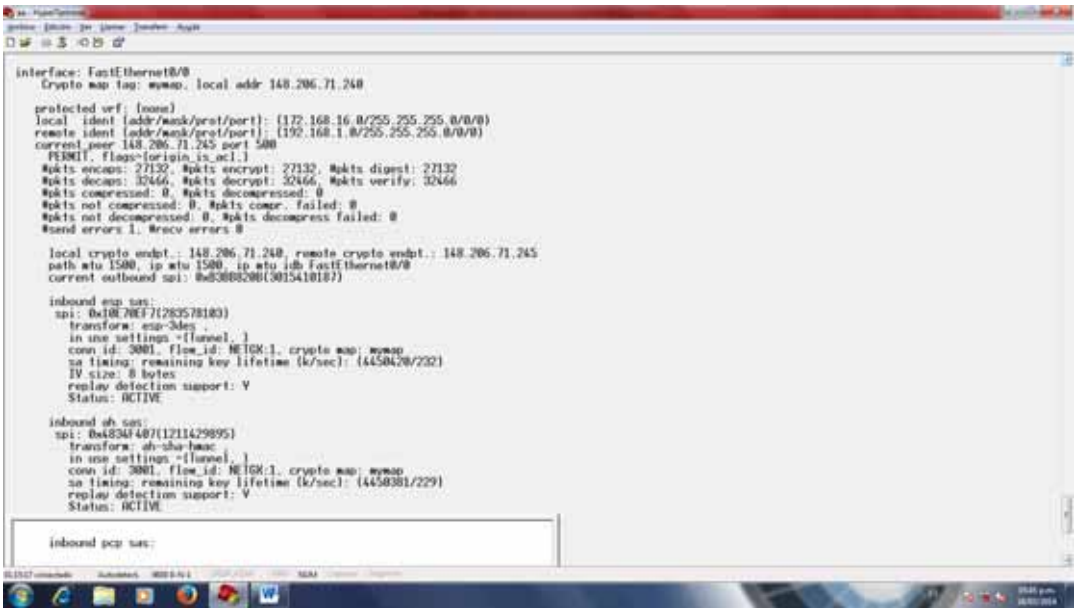

Figura 30 show crypto ipsec sa router B

Como se puede observar en la figura 23 y en la figura 24 se muestran los paquetes que fueron encriptados y desencriptados por los routers, el número de paquetes en nuestro caso depende de la duración de la llamada, se puede observar que son diferentes los números de paquetes encriptados y desencriptados, esto debido a que el router encripta los paquetes que van de salida y desencripta los paquetes que entran, por lo tanto se puede observar que el router A emitió más paquetes de voz que los que recibío, esto también se ve reflejado en el router B donde hay más paquetes desencriptados.

Vamos a analizar los campos que nos interesan de la salida del comando show crypto ipsec sa del router A.

#Aquí se puede observar la ranura de salida que se encarga de encriptar y desencriptar los paquetes, en nuestro caso es por el FastEthernet 0/0.

interface: FastEthernet0/0

#Se puede observar que el mapa crypto que fue utilizado en está interface es el mapa mymap, y la dirección IP que le corresponde a la interfaz de red que es la 148.206.71.245.

Crypto map tag: mymap, local addr 148.206.71.245

protected vrf: (none)

#En esta parte se visualiza el segmento de red que corresponde a nuestro lado de la VPN que es el 192.168.1.0/24

local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

#Ahora podemos observar que el segmento de red que corresponde al otro lado de la VPN es el 172.168.26.9/24

remote ident (addr/mask/prot/port): (172.168.16.0/255.255.255.0/0/0)

#El otro extremo al cual se conecta nuestra VPN tiene la dirección IP 148.206.71.240 y realizan la conexión por el Puerto 500.

current_peer 148.206.71.240 port 500

PERMIT, flags={origin_is_acl,}

#En esta sección se muestra el número de paquetes de salida que son encapsulados, encriptados y aceptados para poder viajar a través de internet, este número cambia de acuerdo al número de paquetes que son enviados que provienen de nuestro extremo de la VPN.

#pkts encaps: 34570, #pkts encrypt: 34570, #pkts digest: 34570

#Aquí se muestra el número de paquetes que fueron desencapsulados, desencriptados y verificados para accesar a nuestro segmento de la VPN, al igual que el campo anterior el número cambia de acuerdo al número de paquetes que provienen del otro extreme de nuestra VPN.

#pkts decaps: 40020, #pkts decrypt: 40020, #pkts verify: 40020

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

Ahora observaremos la salida del comando show crypto ipsec sa en el router B.

#Aquí se puede observar la ranura de salida que se encarga de encriptar y desencriptar los paquetes es la interface FastEthernet 0/0.

interface: FastEthernet0/0

#La dirección IP de la interface de salida es la 148.206.71.240.

Crypto map tag: mymap, local addr 148.206.71.240

protected vrf: (none)

#Se puede ver que el segmento de red de este lado de la VPN es el 172.168.16.0/24.

local ident (addr/mask/prot/port): (172.168.16.0/255.255.255.0/0/0)

#El segmento de red del otro lado de la VPN corresponde al 192.168.1.0/24.

remote ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0)

#El otro extreme al cual se conecta nuestra VPN es el 148.206.71.245 por el puerto 500.

current_peer 148.206.71.245 port 500

PERMIT, flags={origin_is_acl,}

#El número de paquetes de salida que fueron des encriptados, encapsulados y validados.

#pkts encaps: 34566, #pkts encrypt: 34566, #pkts digest: 34566

#El número de paquetes de entrada que fueron desencriptados, desencapsulados y verificados.

#pkts decaps: 40016, #pkts decrypt: 40016, #pkts verify: 40016

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 1, #recv errors 0

Gracias al comando show crypto ipsec sa se puede confirmar que se ha creado una VPN punto a punto, también se puede verificar el número de paquetes de entrada y de salida a nuestro punto de la VPN.

Para ver el tráfico de voz utilizaremos el software wireshark, su función principal es el de capturar el tráfico que viaja por una interfaz de red de una computadora en nuestro caso analizaremos el tráfico que se establece en una llamada de voz entre las computadoras que tienen instaladas el software Cisco IP Communicator.

En la figura 31 y en la figura 32, se puede observar como la señalización para el control de la llamada realizada entre los extremos, que cuentan con las direcciones IP 192.168.1.2 para el extremo A y la dirección IP 172.168.16.2 para el extremo B, y el gatekeeper que en nuestro caso tiene la dirección IP 192.168.1.1 y se comunican entre sí utilizando el protocolo SKINNY, para después establecer una conexión entre los extremos de la llamada y formar el canal RTP que es por donde viaja la voz.

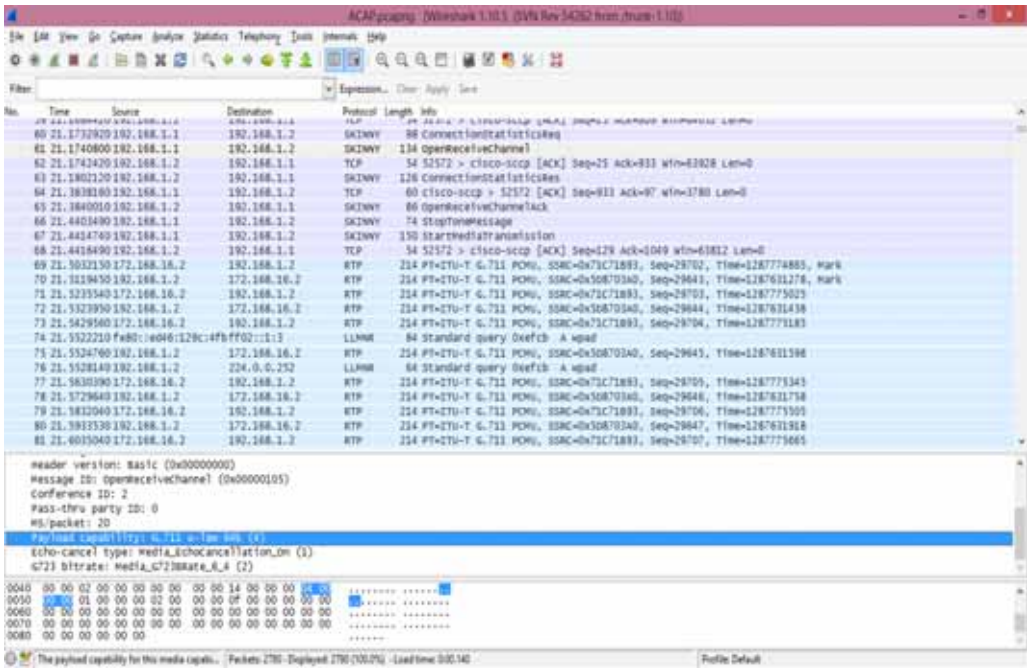

Figura 31 Captura Extremo A.

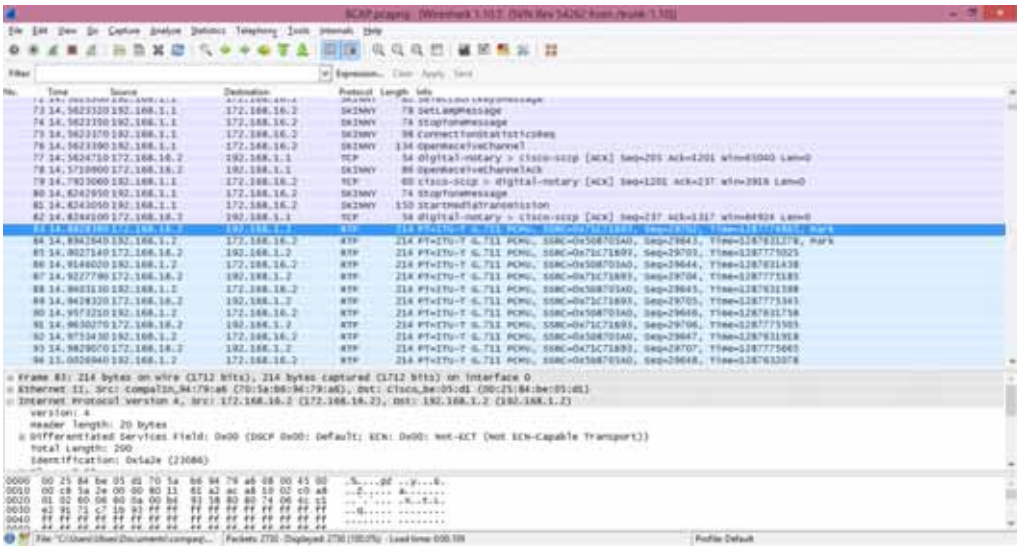

Figura 32 Captura de Tráfico Extremo B

Comenzaremos analizando el tráfico correspondiente al protocolo SKINNY. Al dar doble click sobre algún renglón que contenga el protocolo SKYNNI se mostrara una ventana con los detalles de ese paquete donde, entre otras cosas se puede ver el mensaje de señalización que es enviado, el puerto por el cual es enviado (puerto 2000), el protocolo que es utilizado, la dirección IP de destino y la dirección IP de origen entre otras cosas, tal como se muestra en la figura 33.

Figura 33 Detalle del Paquete SKINNY.

Para observar todas las señalizaciones de control de llamada realizadas por el protocolo SKINNY debemos seleccionar el menú *Telephony -> VoIP Calls* donde se nos mostrara una ventana con todas las llamadas que fueron realizadas durante la captura de tráfico, donde se nos mostrara la marca de tiempo en el inicio de la llamada, la marca de tiempo del fin de llamada, la dirección IP del que inicia la llamada, que en nuestro caso se muestra la dirección IP que pertenece al equipo en el que se realiza la captura de tráfico, el identificador de quien realiza la llamada, el identificador de quien recibe la llamada, el protocolo utilizado, el número de paquetes correspondientes a la señalización de la llamada, el estado de la llamada, en nuestro caso completada, y los comentarios, figura 34.

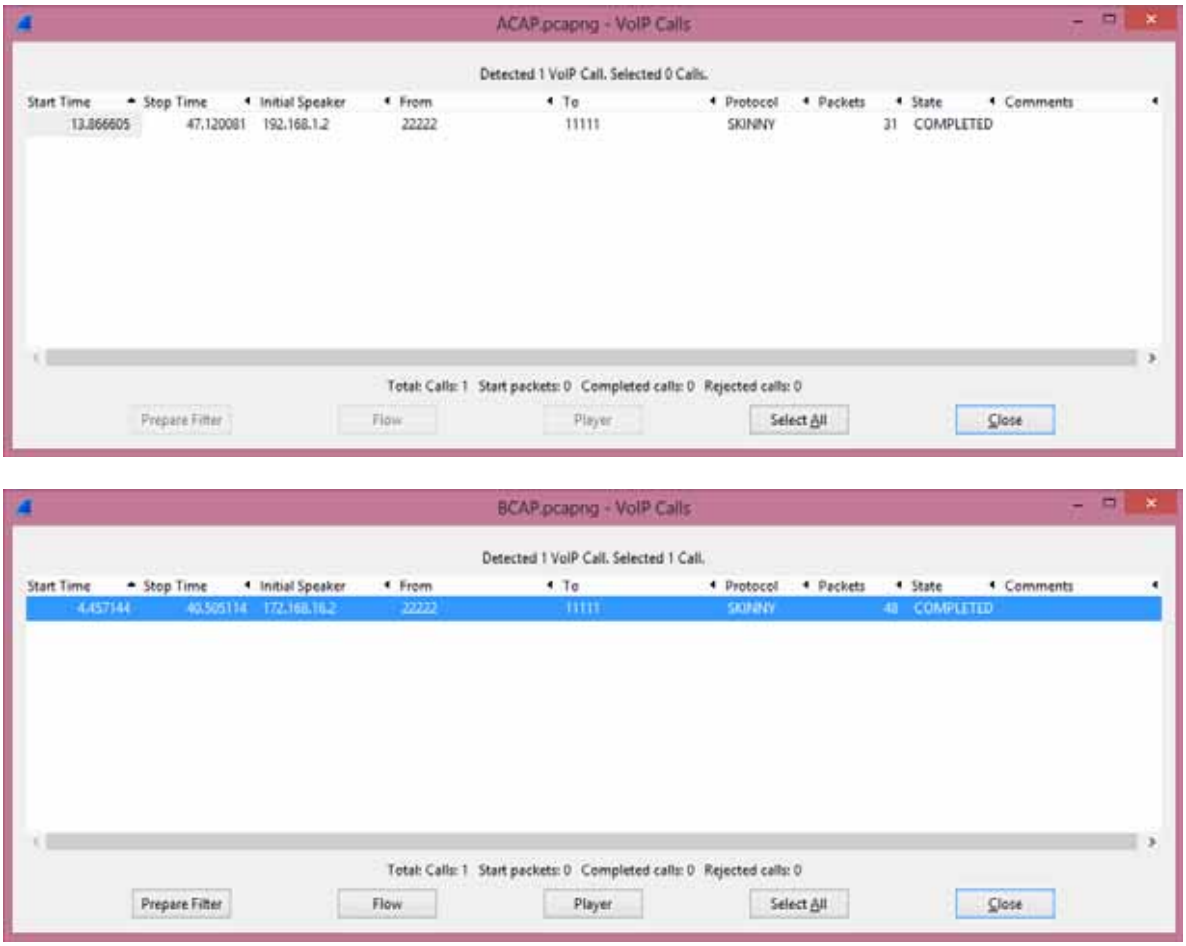

Figura 34 Detalle de la Llamada.

Damos click en flow donde se nos mostraran todas las señalizaciones que existieron en nuestra llamada, figura 35.

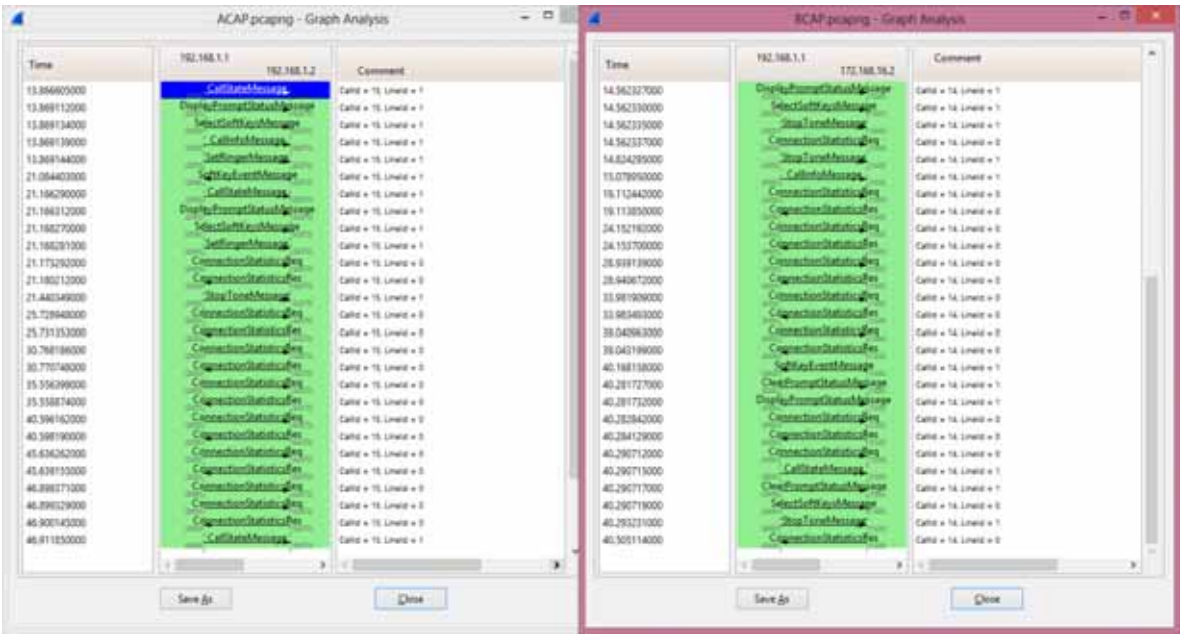

Figura 35 Señalización de la llamada.

Como se puede observar en la figura 36, la señalización de la llamada se da entre el Gatekeeper y ambos extremos de la llamada, y va desde el establecimiento de la llamada hasta la finalización de esta.

Para ver el flujo RTP seleccionamos un paquete RTP y vemos su detalle, figura 36.

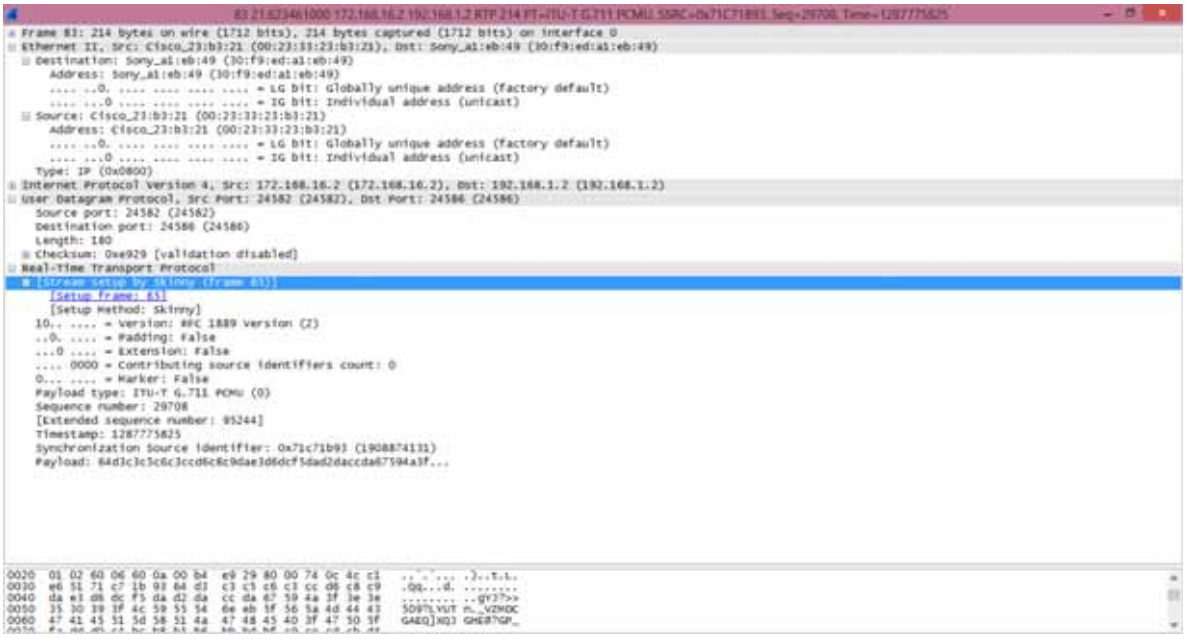

Figura 36 Detalle Paquete RTP

En el detalle se puede observar que el flujo RTP fue establecido por el protocolo SKINNY, se puede observar la dirección IP de origen, la dirección IP destino, y que viaja a través de UDP, también

podemos observar que el tipo que se trata es ITU-T G.711 PCMU (0), es decir usa el códec de audio G.711 estandarizado por ITU, una frecuencia de muestreo de 0, y comprime y descomprime PCMU. Una vez que se establece el canal RTP este es directo entre los extremos de la llamada.

Para observar el flujo RTP seleccionamos el menú *Telephony->RTP->Show All Streams*, donde nos mostrara una ventana con los flujos RTP que se establecieron mientras se capturaba el tráfico, figura 37, sí se selecciona un flujo y se oprime el botón *Find Reverse* podemos saber cuál es el flujo de reversa que corresponde al flujo que estamos seleccionando, es decir se crea un flujo de voz de entrada y otro de salida.

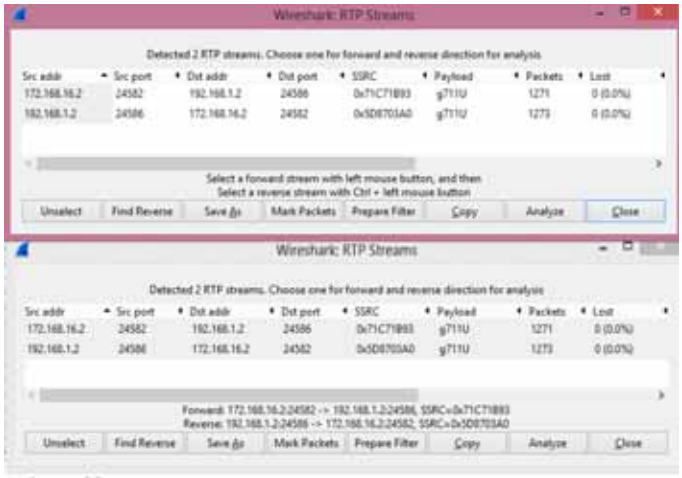

Figura 37 Flujos RTP

Una vez que están seleccionados los dos flujos de entrada y de salida podemos dar click en el botón *Analyze*, el cual mostrara el análisis estadístico de los flujos RTP de entrada y de salida, figura 38.

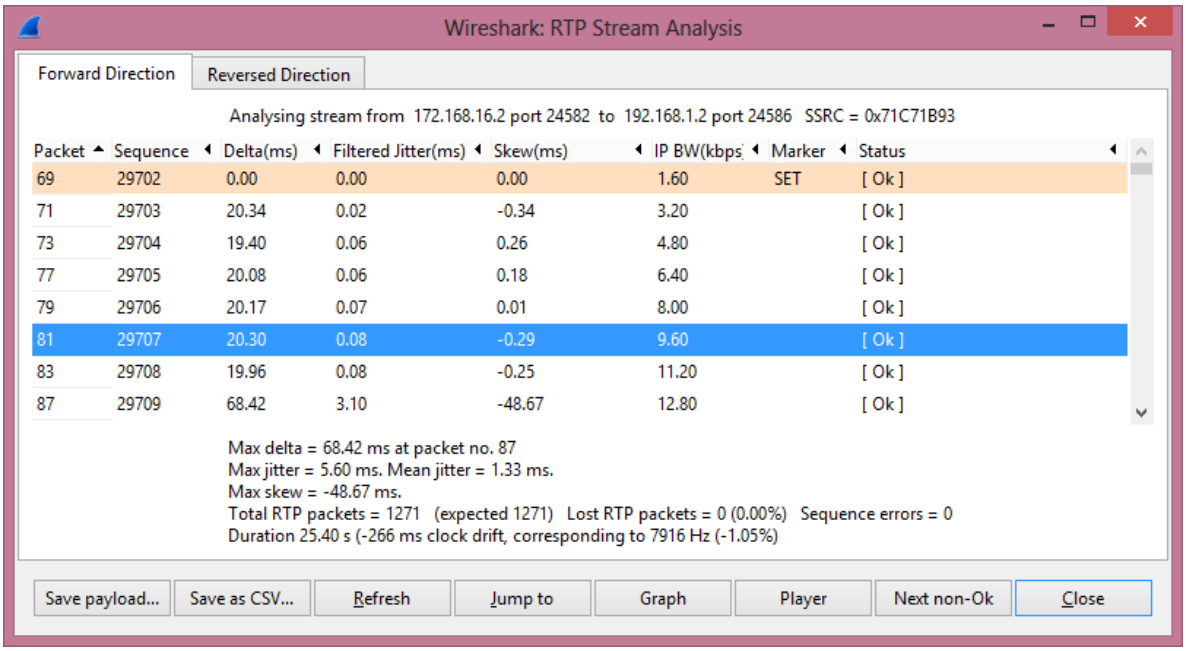

Figura 38 Análisis del Flujo RTP

Para recuperar el audio de la llamada se oprime el botón *Player* donde mostrara una pantalla donde se puede reproducir la llamada figura 39.

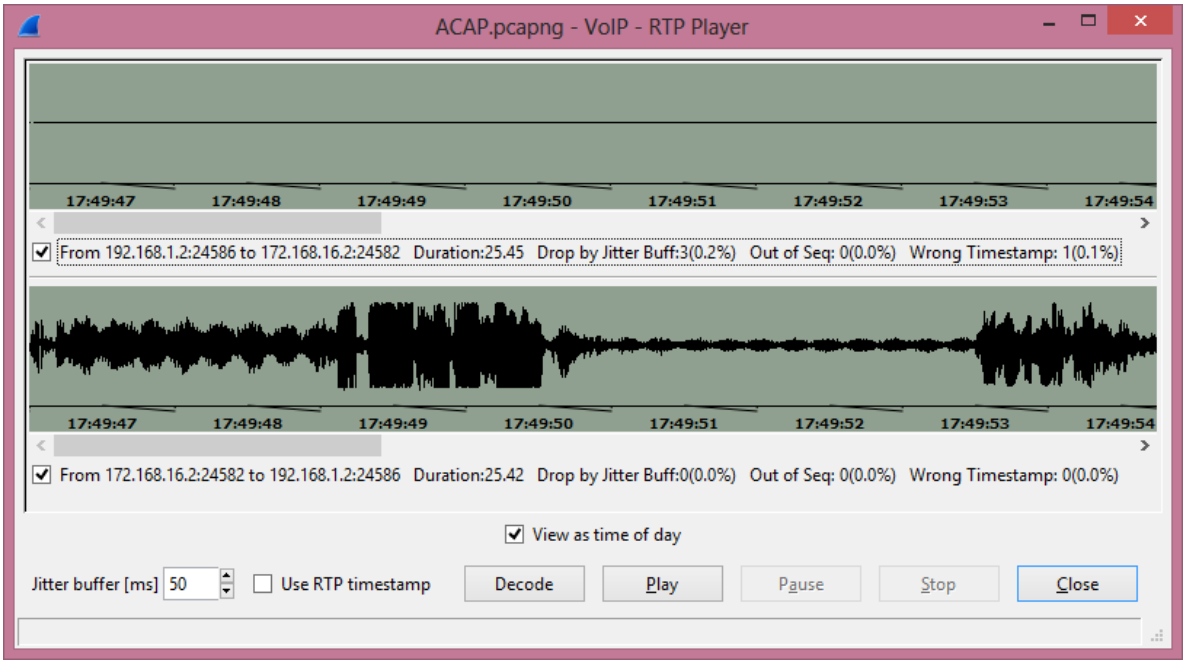

Figura 39 Reproductor de Audio

Conclusiones.

Tras haber realizado el proyecto se puede concluir que la implementación de VoIP significa un ahorro en cuanto a infraestructura ya que se aprovecha internet para implementarla solo hace falta tener el hardware adecuado dependiendo de la topología a implementar y establecer la políticas de calidad necesarias para tener llamadas de alta calidad, la implementación de VoIP a grandes escalas representa un reto ya que se tiene que lidiar con las limitaciones de las redes IP en cuanto a conservar un ancho de banda adecuado para la transferencia de datos y el ancho de banda necesario para poder dar servicio de telefonía a todos los participantes involucrados.

En cuanto a los problemas que se presentan al momento de implementar VoIP en conjunto con Nat y la VPN después de haber buscado varias soluciones se prefirió negar la traducción de direcciones para el tráfico entre los segmentos de red involucrados en la VPN que son los mismos a los que se le proporciona el servicio de telefonía por lo cual se puede establecer una comunicación directa entre los dos extremos de la VPN lo que hace posible prestar el servicio de telefonía sin las complicaciones que NAT representa a la VoIP, y sin preocuparnos por la seguridad de los paquetes que viajan a través de internet ya que viajan encriptados gracias a los protocolos IPSec con los cuales fue implementad nuestra VPN.

Se optó implementar la VPN punto-a-punto por qué es un modelo simple y cuando no se implementa a grandes escalas, la configuración se torna sencilla ya que solo conectamos dos segmentos de red a nuestra VPN.

Gracias a la encriptación proporcionada por los protocolos de IPSec se puede asegurar la confidencialidad de la llamada, debido a la encriptación que se implementó, las llamadas no puede ser interceptada ni decodificadas. Esto es un elemento muy importante para que las empresas u organizaciones opten por este tipo de esquema y dejar a un lado la telefonía tradicional que no proporciona la seguridad en los datos.

Bibliografía

- Jonathan Davidson and James Peters, *Voice Over IP Fundamentals*, Indianapolis, IN: Cisco Press, 2000.
- Kevin Wallace, *Voice Over IP First-Step*, Indianapolis, IN: Cisco Press, 2006.
- Richard Deal, *The Complete Cisco VPN Configuration Guide*, Indianapolis, IN: Cisco Press, 2006.
- Vijay Bollapragada, Mohamed Khalid, Scott Wainner, *IPSec VPN Design*, Indianapolis, IN: Cisco Press, 2005.
- Jazib Frahim, Omar Santos, *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance,* Indianapolis, IN: Cisco Press, 2006.
- Diane Teare, *Campus Network Design Fundamentals,* Indianapolis, IN: Cisco Press, 2006.
- David Barnes, Basir Sakandar, *Cisco LAN Switching Fundamentals,* IN: Cisco Press, 2006.
- http://www.voipvoip.com/customer-care/voip-router.html (08/04/2014).

- http://www.voip-info.org/wiki/view/NAT+and+VOIP(08/04/2014).
- http://www.cisco.com/c/en/us/products/routers/2811-integrated-services-router-isr/index.html (08/07/2014).
- http://www.cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-110/13329-x-release.html (08/07/2014).

Entregable A.

Configuración del router A que contiene el servicio de telefonía. La configuración del router se muestra al ejecutar el comando show run.

Building configuration...

Current configuration : 2108 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Router

!

boot-start-marker

boot system tftp c2800nm-advipservicesk9-mz.124-17.bin 192.168.1.2

boot system flash

boot system rom

boot-end-marker

!

!

no aaa new-model

```
!
!
ip cef
no ip dhcp use vrf connected
!
ip dhcp pool VOIP
   network 192.168.1.0 255.255.255.0
   default-router 192.168.1.1
   option 150 ip 192.168.1.1
!
!
!
!
voice-card 0
 no dspfarm
!
!
!
!
!
!
!
!
!
!
!
!
```

```
!
!
!
!
!
!
!
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 5
 lifetime 900
crypto isakmp key cisco address 148.206.71.240
!
!
crypto ipsec transform-set 50 ah-sha-hmac esp-3des
!
crypto map mymap 10 ipsec-isakmp
 set peer 148.206.71.240
 set security-association lifetime seconds 1800
 set transform-set 50
 match address 101
!
!
!
!
```

interface FastEthernet0/0

ip address 148.206.71.245 255.255.255.0

ip nat outside

ip virtual-reassembly

duplex auto

speed auto

crypto map mymap

!

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0

ip nat inside

ip virtual-reassembly

duplex auto

speed auto

!

interface Serial0/3/0

no ip address

shutdown

no fair-queue

clock rate 125000

!

interface Serial0/3/1

no ip address

shutdown

clock rate 125000

!

ip forward-protocol nd

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

!

!

ip http server

no ip http secure-server

ip nat inside source list 100 interface FastEthernet0/0 overload

!

access-list 100 deny   ip 192.168.1.0 0.0.0.255 172.168.16.0 0.0.0.255

access-list 100 permit ip 192.168.1.0 0.0.0.255 any

access-list 101 permit ip 192.168.1.0 0.0.0.255 172.168.16.0 0.0.0.255

!

!

!

!

control-plane

!

!

!

!

!

!

!

!

!

```
telephony-service
 max-ephones 5
 max-dn 5
 ip source-address 192.168.1.1 port 2000
 max-conferences 8 gain -6
!
!
ephone-dn  1
 number 11111
!
!
ephone-dn  2
 number 22222
!
!
ephone  1
 mac-address 30F9.EDA1.EB49
 type CIPC
 button  1:1
!
!
!
ephone  2
 mac-address 705A.B694.79A6
 type CIPC
 button  1:2
```

!

!

!

line con 0

line aux 0

line vty 0 4

login

!

scheduler allocate 20000 1000

!

end

Entregable B.

El siguiente entregable contiene la configuración del router B, que solo contiene la configuración para conectarse a la VPN. La configuración del router se muestra al ejecutar el comando show run.

Building configuration...

Current configuration : 1914 bytes

!

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Router

!

boot-start-marker

boot system tftp c2800nm-advipservicesk9-mz.124-17.bin 192.168.1.3

boot system flash:

boot system rom

boot-end-marker

!

!

no aaa new-model

memory-size iomem 10

!

!

ip cef

no ip dhcp use vrf connected

!

ip dhcp pool SINVOIP

network 172.168.16.0 255.255.255.0

default-router 172.168.16.1

!

!

!

!

voice-card 0

no dspfarm

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

!

crypto isakmp policy 10

encr aes

authentication pre-share

group 5

lifetime 900

crypto isakmp key cisco address 148.206.71.245

!

!

crypto ipsec transform-set 50 ah-sha-hmac esp-3des

!

crypto map mymap 10 ipsec-isakmp

set peer 148.206.71.245

set security-association lifetime seconds 1800

set transform-set 50

match address 101

!

!

!

!

interface FastEthernet0/0

ip address 148.206.71.240 255.255.255.0

ip nat outside

ip virtual-reassembly

duplex auto

speed auto

crypto map mymap

!

interface FastEthernet0/1

ip address 172.168.16.1 255.255.255.0

ip nat inside

ip virtual-reassembly

duplex auto

speed auto

!

interface Serial0/0/0

no ip address

shutdown

clock rate 125000

!

interface Serial0/0/1

no ip address

shutdown

clock rate 125000

!

interface Serial0/1/0

no ip address

shutdown

clock rate 125000

!

interface Serial0/1/1

no ip address

shutdown

clock rate 125000

!

ip forward-protocol nd

ip route 0.0.0.0 0.0.0.0 FastEthernet0/0

!

!

ip http server

no ip http secure-server

ip nat inside source list 100 interface FastEthernet0/0 overload

!

access-list 100 deny ip 172.168.16.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 172.168.16.0 0.0.0.255 any

access-list 101 permit ip 172.168.16.0 0.0.0.255 192.168.1.0 0.0.0.255

!

!

!

!

control-plane

!

!

!

!

!

!

!

!

!

!

line con 0

line aux 0

line vty 0 4

login

!

scheduler allocate 20000 1000

!

end

Entregable ACAP.

Captura del tráfico de datos al momento de la llamada dentro de la laptop Vaio, se encuentra dentro del cd con el nombre del archivo ACAP.pcapng, se tiene que contar con wireshark para poder visualizarlo, una vez abierto con el wireshark se puede recuperar el flujo de voz.

Entregable BCAP.

Captura del tráfico de datos al momento de la llamada dentro de la laptop Compaq, se encuentra dentro del cd con el nombre del archivo BCAP.pcapng, se tiene que contar con wireshark para poder visualizarlo, una vez abierto con el wireshark se puede recuperar el flujo de voz.