Universidad Autónoma Metropolitana

Unidad Azcapotzalco

División de Ciencias Básicas e Ingeniería

Licenciatura en Computación

Proyecto de Integración de Ingeniería en Computación

Implementación de VoIP en una VPN

Alumno

Muñoz Salgado Luis Roberto

Asesor

M. en C. Arturo Zúñiga López

Trimestre 17-P

28-agosto-2017

Yo, Arturo Zúñiga López, declaro que aprobé el contenido del presente Reporte del 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, Luis Roberto Muñoz Salgado, doy mi autorización a la Coordinación de Servicios de Información de la Universidad Autónoma Metropolitana, Unidad Azcapotzalco, para publicar el presente documento de la Biblioteca Digital, así como en el Repositorio Institucional de la UAM Azcapotzalco.

Firma

Resumen

En el presente trabajo se implementó la comunicación de voz por medio de una red de datos IP, haciendo un enfoque particular en los fundamentos de la tecnología VoIP, así como los protocolos requeridos y los estándares necesarios para implementar voz sobre IP en una VPN.

La Voz sobre IP, también conocida como VoIP, Telefonía IP o telefonía de Internet. Se trata de la tecnología que permite la conexión de conversaciones de voz sobre Internet o red de computadoras. Es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN (sigla de Public Switched Telephone Network, Red Telefónica Pública Conmutada). Existen diversos estándares de comunicación de voz por IP, que están disponibles para uso generalizado y sistemas exclusivos. H.323 y SIP pertenecen a la primera categoría, mientras que Skype utiliza su propio sistema exclusivo.

Las VPN son redes artificiales que utilizan Internet como medio de transmisión junto a un protocolo de túnel garantizando confidencialidad, bajo costo, autenticación y que la información recibida sea la enviada, son algunas de las características de VPN, además de su sistema de cifrado de mensajes. Para implementar una red privada virtual es necesario una políticas de seguridad, servidor de acceso y autenticación, administración de direcciones y soporte para múltiples protocolos, para poder compartir datos, aplicaciones y recursos.

En la implementación del proyecto utilizaremos NAT (Network Address Translation). NAT es un mecanismo que permite que múltiples dispositivos compartan una sola dirección IP pública de Internet, ya que en nuestro proyecto tendremos conectados dos router al internet con ip publicas.

Tabla de contenido

Tabla de Ilustraciones

I Introducción

La mayoría de nosotros estamos familiarizados con el "sistema telefónico conmutado público" (PSTN), que nos permite establecer contacto con personas de todo el mundo al marcar una secuencia de números. VOIP ofrece una alternativa, que funciona mediante la redirección de señales de voz digitalizadas a través de redes IP, como intranet de empresa o, en algunos casos, la Internet pública.

El sistema PSTN no ha cambiado mucho en más de 100 años. Se han producido muchos cambios tecnológicos y mejoras, como el marcado por tonos y los ID de llamada, pero, en lo que concierne al usuario, sigue siendo cuestión de marcar.

VoIP no es una tecnología particularmente nueva. Existen documentos y patentes que datan de décadas atrás y hay software VoIP disponible desde 1991. El principio fundamental es bastante sencillo. Un micrófono recoge el sonido de voz y la tarjeta de sonido lo digitaliza. El audio digitalizado se comprime con un códec de audio. Esto se hace eliminando los datos innecesarios, a la vez que se mantiene la legibilidad del audio, a fin de que el flujo, sea lo suficientemente compacto para enviarse por la red en tiempo real. Los sonidos se codifican en el lado del emisor, se envían a través de la red y, a continuación, se decodifican en el lado del receptor, donde se reproducen por los altavoces o auriculares.

Dentro de la gran diversidad de usos del Internet, el principal y medular es la comunicación de equipos, ¿Cómo podemos asegurarnos de conectar terminales remotos? ¿Cómo podemos acercar computadoras para facilitar el trabajo? Tenemos las redes locales que permiten compartir archivos, recursos, información en general de forma rápida, y como bien dice, local.

Explicaremos cómo funcionan las Redes Virtuales Privadas, o VPN, los tipos de redes virtuales, protocolos empleados a grandes rasgos, mecanismos de seguridad, el software utilizado para facilitar la implementación de éstas, y las principales y potenciales aplicaciones en el ámbito doméstico/, empresarial e industrial.

Teniendo en cuenta los dos conceptos pasados el de VoIP y el de VPN, nuestro proyecto implementara una red virtual donde podremos pasar VoIP para realizar un servicio de telefonía IP a través de internet.

II Antecedentes

La tecnología IP comenzó a principios de la década de los 1990, aunque la mala calidad de voz y el impulso que en aquellos momentos estaba tomando la RDSI hicieron que no pasase de un mero experimento. Durante esa década se produjo el boom de internet, lo que hizo que todos los esfuerzos, tanto de las empresas como de los operadores fuesen dirigidos a potenciar su uso y las aplicaciones de navegación Web y correo electrónico fueron las que más éxito tuvieron, lo que junto el despliegue de las redes móviles dejaron la voz relegada en un tercer plano.

La voz sobre redes IP VoIP (Voice over IP) inicialmente se implementó para reducir el ancho de banda mediante compresión vocal, aprovechando los procesos de compresión diseñados para sistemas celulares en la década de los años 80. En consecuencia, se logró reducir los costos en el transporte internacional. Luego tuvo aplicaciones en la red de servicios integrados sobre la LAN e Internet. Con posterioridad se migró de la LAN (aplicaciones privadas) a la WAN (aplicaciones públicas) con la denominación IP-Telephony.

En marzo de 1997 la compañía MCI de Estados Unidos lanza su proyecto llamado VAULT, esta nueva arquitectura de red permite interconectar y combinar las redes tradicionales de telefonía con redes de datos. El sistema “empaqueta” las conversaciones (es decir, las transforma en bloques de información manejables por una red de datos) y las envía vía Internet.

A finales del año 1997 el VoIP forum del IMTC (International Multimedia Telecommunications Consortium) llega a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP. Debido a la ya existencia del estándar H.323 del ITU-T (International Telecommunication Union), que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323 fuera la base del VoIP. De este modo, el VoIP debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP. El VoIP tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, y estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

En el año 1998 se comenzaron 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). También se comenzó a fabricar Switches de Layer 3 con QoS.

En el año 1999 Cisco vende sus primeras plataformas corporativas para VoIP. Se utilizaba principalmente el protocolo H.323 de señalización. El marco de voz con el software integrador Cisco IOS ofrece la integración completa y sin fisura de voz, video y datos. Permite a los clientes corporativos y a los proveedores de servicio manejar grandes redes y servicios basados en VoIP. En enero de 1999, 3Com lanzó con éxito las capacidades de VoIP, construido en parte sobre la base del servidor de Microsoft Windows NT y en la plataforma Total Control multi-servicio, un sistema avanzado basado en DSP (Digital Signal Processor).

En el año 2000 VoIP representaba más del 3% del tráfico de voz. Ese 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 el año 2000 VoIP representaba más del 3% del tráfico de voz.

En el año 2002 el protocolo SIP (Session Initiation Protocol) que es un protocolo de señalización desarrollado por la IETF (Internet Engineering Task Force), empieza a desplazar al protocolo H.323.

Todo apunta hacia el triunfo de la telefonía IP, tanto en el segmento residencial como en el empresarial, y las predicciones del mercado apuntan a que hacia el año 2010 un 25% de las llamadas telefónicas lo serán sobre redes basadas en IP.

III Justificación

La integración de voz, datos y equipos IP le ha permitido a compañías interactuar e intercambiar éstos tipos de comunicaciones de manera mucho más fácil, aumentando en consecuencia la productividad de sus fuerzas laborales y las interacciones con sus consumidores, proveedores y otros agentes en la cadena de valor.

A pesar de sus muchas ventajas y papel muy influyente en las comunicaciones unificadas, VoIP todavía tiene algunos problemas y problema de seguridad es uno de ellos. Sin embargo, como la PSTN es caro y no tan rápido como VOIP, por lo que es necesario que las empresas para cambiar a sistemas de un teléfono VoIP de negocio para asegurar mejores resultados rápidamente. VoIP sigue siendo el 'futuro de la comunicación'

La seguridad de VoIP tiene una solución en forma red privada virtual. Red Privada Virtual también conocido como VPN es una red segura para el uso de un número limitado de personas, tales como empleados de una empresa, que operan en una amplia zona.

Hay muchas ventajas de utilizar VPN. Por ejemplo, se le permite cambiar los sistemas de telefonía VoIP desde cualquier lugar. Gracias a esta característica, se puede navegar por los sitios web que se limitan estrictamente a un único país. Por ejemplo, un sitio web chino que es sólo para los chinos no estará disponible fuera de China. Sin embargo, a través de la VPN se puede navegar por este sitio web tan fácilmente como pasar por las restricciones regionales, tales como firewalls y otra de filtrado web.

Las VPN permite a otros seguir el rastro de sus actividades en la red. Por esta razón, se convierte en un guardia de seguridad para la transferencia de datos en línea. Tambien mejora la calidad de sus procesos de VoIP de forma rentable. Un punto a favor de estas llamadas tendrá una mejor calidad.

IV Objetivos

General

Diseñar una topología de red que permita el tráfico de VoIP, sobre una red privada virtual(VPN) de Acceso Remoto.

Particulares

I. Implementar una VPN de Acceso Remoto
II. Implementar VoIP sobre la VPN.
III. Probar el funcionamiento de la implementación.

Capitulo I. Voz Sobre IP

Voz sobre Protocolo de Internet, también llamado Voz sobre IP, Voz IP, VoIP (por sus siglas en inglés, Voice over IP), siendo un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN.

Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local.

Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía IP.

• VoIP es el conjunto de normas, dispositivos, protocolos, en definitiva la tecnología que permite comunicar voz sobre el protocolo IP.

• Telefonía IP es el servicio telefónico disponible al público, realizado con tecnología de VoIP.

Protocolos

Existen varios protocolos comúnmente usados para VOIP, estos protocolos definen la manera en que por ejemplo los CODECS5 se conectan entre si y hacia otras redes usando VoIP. Estos también incluyen especificaciones para CODECS de audio.

H.3236

El estándar H.323 proporciona una base para realizar la transmisión de voz, datos y vídeo sobre redes no orientadas a conexión y que además no ofrecen un grado de calidad del servicio, como son las basadas en IP, incluida Internet, de manera tal que las aplicaciones y productos conforme a ella puedan interoperar, permitiendo la comunicación entre los usuarios sin necesidad de que éstos se preocupen por la compatibilidad de sus sistemas. La LAN sobre la que los terminales H.323 se comunican puede ser un simple segmento o un anillo, o múltiples segmentos (es el caso de Internet) con una topología compleja, lo que puede resultar en un grado variable de rendimiento.

H.323 es la especificación establecida por la UIT en 1996, fijó los estándares para la comunicación de voz y vídeo sobre redes de área local, con cualquier protocolo, que por su propia naturaleza presentan una gran latencia y no garantizan una determinada calidad del servicio. Para la conferencia de datos se apoya en la norma T.120 , con lo que en conjunto soporta las aplicaciones multimedia. Los terminales y equipos conforme a H.323 pueden tratar voz en tiempo real, datos y vídeo, incluida videotelefonía.

El estándar contempla el control de la llamada, gestión de la información y ancho de banda para una comunicación punto a punto y multipunto, dentro de la LAN, así como define interfaces entre la LAN y otras redes externas, como puede ser la RDSI. Es una parte de una serie de especificaciones para videoconferencia sobre distintos tipos de redes, que incluyen desde la H.320 11a la H.324, estas dos válidas para RDSI y RTC, respectivamente.

La norma H.323 que hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los cuales el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica.

Características principales de H.323

En 1996 la UIT realizó una recomendación denominada H.323 y bajo la cual agrupó a un conjunto de estándares y protocolos para las comunicaciones en tiempo real sobre redes que no garantizaban la calidad de servicio como lo es la Internet. H.323 está orientado a la comunicación de dispositivos multimedia dentro de una red LAN, con la posibilidad de interactuar con la PSTN o ISDN. Con H.323 es posible transmitir voz, datos, video o alguna combinación de estos.

Este protocolo funciona sobre varias topologías de red y el software requerido para que el protocolo funcione de manera obligatoria es el software de voz, mientras que el software orientado a la transmisión de datos y video es opcional. Al ser H.323 un protocolo que agrupa a varios más, necesita de otros protocolos y equipos que gestionen la comunicación entre los diferentes dispositivos y redes de telefonía.

Las características que ofrece este estándar, en cuanto a comunicaciones multimedia, son:

- Interoperabilidad entre distintos fabricantes. Sin embargo, precisamente debido a su complejidad, H.323 intenta acotar todas las posibilidades de la comunicación, de las capacidades y de la funcionalidad de cada elemento de la red, incluso las posibles ampliaciones de sí mismo, de forma que en la comunicación exista.

- Independencia de la red. H.323 hace referencia a redes de paquetes que no provean calidad de servicio, pero no especifica ningún protocolo de red en concreto.

- Independencia de la plataforma y de la aplicación. Siempre que se cumplan los requisitos y procedimientos descritos en las especificaciones, podrá hacer uso de H.323 cualquier plataforma, hardware o sistema operativo deseado.

- Soporte para multiconferencias. Aunque H.323 permite mantener multiconferencias sin el uso de unidades especializadas, las MCUs (Multipoint Control Units) proporcionan una arquitectura más robusta y flexible para el mantenimiento de multiconferencias.

- Gestión del ancho de banda. El tráfico de audio y de vídeo resulta costoso en cuanto a recursos de ancho de banda, y podría colapsar la red. H.323 permite la gestión del ancho de banda, pudiendo limitar el número de conexiones H.323 simultáneas, así como especificarles el ancho de banda disponible a aplicaciones y terminales H.323.

- Soporte para transmisión en MULTICAST. MULTICAST es un método de transporte que permite enviar un solo paquete hacia un conjunto de destinos sin replicación (frente a UNICAST, que utilizaría múltiples transmisiones punto a punto, y a BROADCAST, que enviaría el paquete a todas los destinos), haciendo un uso mucho más eficiente del ancho de banda.

- Soporte para el establecimiento de conferencias entre distintas redes multimedia. H.323 establece mecanismos para unir sistemas basados en comunicaciones LAN con sistemas RDSI, así como con las redes PSTN, tanto en audio como en videoconferencias.

- Seguridad. Mediante H.235, se establecen procedimientos de autenticación, integridad de los paquetes, privacidad (mediante mecanismos de encriptación) y no repudio (es decir, medios de protección contra la afirmación de no haber participado en una conferencia).

- Establecimiento de llamada rápido (FAST CALL). H.323 también establece mecanismos para que la llamada quede establecida con un mínimo de dos paquetes.

- Intercambio de requerimiento de calidad de servicio. Un destino puede especificar una calidad de servicio deseada para sus flujos de audio y vídeo
- Capacidades para la redundancia de la red. Mediante servidores de direccionamiento alternativos (“ALTERNATE GATEKEEPERS”) la red podrá soportar la caída de estos equipos críticos, sin pérdida de comunicación.

- Descripción genérica de capacidades. Mediante esta especificación ASN.1, pueden describirse CÓDECS y formatos de audio o vídeo genéricos, sin perturbar las capacidades de comunicación dentro de los estándares más habituales.

- Gestión del direccionamiento entre dominios administrativos. Se establecen flexibles mecanismos de escalado para el establecimiento de llamadas entre grandes redes internacionales, mediante la definición, entre los GATEKEEPERS encargados del direccionamiento de la red, de los llamados elementos de borde o border elements.

- Terminales simples SET (Simple Endpoint Type). Como la especificación H.323 puede resultar demasiado extensa para terminales sencillos, la especificación H.341 recoge los mecanismos mínimos para asegurar la comunicación en redes H.323 de terminales con una funcionalidad básica.

- Servicios suplementarios. Dentro de los servicios asociados a conferencias, H.323 añade numerosas posibilidades, entre las cuales se destacan: o Transferencia de llamada: permite que una conferencia establecida entre A y B pase a establecerse entre B y C.

Arquitectura del protocolo H.323.

Para la arquitectura H.323 que se aprecia en la figura, complementan básicamente equipos Terminales, Gateways, para su interconexión con los recursos PSTN), Gatekeepers que es (Control de admisión, registro y ancho de banda) y MCUs (Multiconference Control Units).

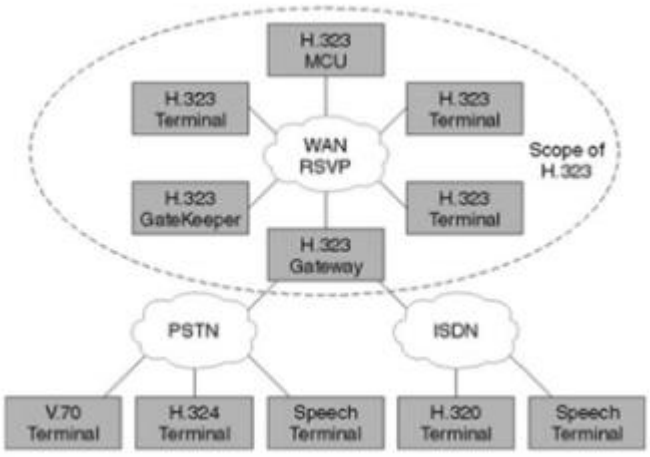

Figura 1: Elementos de una red H.323

Dentro de H.323 se incluyen todo un conjunto de protocolos perfectamente integrados.

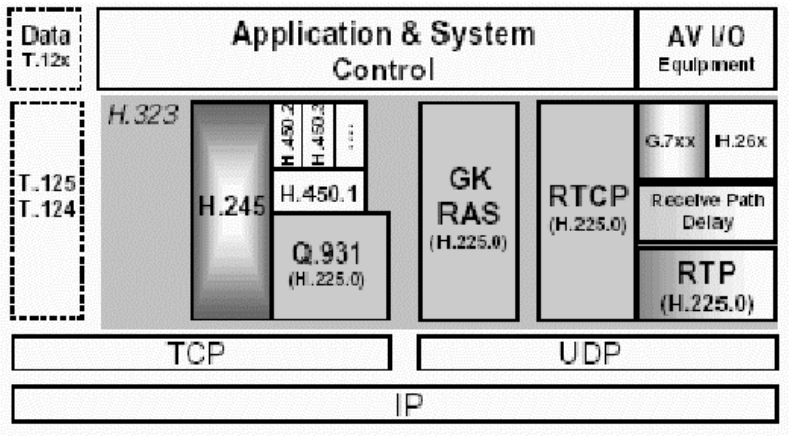

Figura 2: Conjunto de protocolos integrados a H.323

Función de señalización de la llamada

La función de señalización está basada en la recomendación H.225, que especifica el uso y soporte de mensajes de señalización. Las llamadas son enviadas sobre TCP por el puerto 1720. Sobre este puerto se inician los mensajes de control de llamada entre dos terminales para la conexión, mantenimiento y desconexión de llamadas. Los mensajes más comunes de Q.931/Q.932 usados como mensajes de señalización H.323 son:

- Setup. Es enviado para iniciar una llamada H.323 para establecer una conexión con una entidad H.323. Entre la información que contiene el mensaje se encuentra la dirección IP, puerto y alias del llamante o la dirección IP y puerto del llamado.
- Call Proceeding. Enviado por el GATEKEEPER a un terminal advirtiendo del intento de establecer una llamada una vez analizado el número llamado.
- Connect. Indica el comienzo de la conexión.
- Release Complete. Enviado por el terminal para iniciar la desconexión.

• Facility. Es un mensaje de la norma Q.932 usado como petición o reconocimiento de un servicio suplementario.

Función de control H245

Es un conjunto de mensajes ASN.1 que se usan para establecer y controlar una llamada. Las características mas revelantes que se intercambian son:

MasterSlaveDetermination (MSD). Este mensaje es usado para prevenir conflictos entre dos terminales que quieren iniciar la comunicación. Decide quién actuará de Master y quién de Slave.

TerminalCapabilitySet (TCS). Mensaje de intercambio de capacidades soportadas por los terminales que intervienen en una llamada.

OpenLogicalChannel (OLC). Mensaje para abrir el canal lógico de información contiene información para permitir la recepción y codificación de los datos. Contiene la información del tipo de datos que serán transportados.

CloseLogicalChannel (CLC). Mensaje para cerrar el canal lógico de información.

Canal H.225 RAS

El canal RAS (Registration Admission Status) es un fragmento del estándar H.225 y sirve para mantener una comunicación de señalización entre un punto final y el "GATEKEEPER". Funciona sobre el protocolo de transporte UDP y entre sus funciones destacamos:

- Localización del "GATEKEEPER".

- Registro de un punto final en el "Gatekeeper".

- Localización de un punto final a través del "Gatekeeper".

- Admisión de conexiones. - Reajustes en el ancho de banda.

Componentes de H.323

La norma H.323 hace uso de los procedimientos de señalización de los canales lógicos contenidos en la norma H.245, en los que el contenido de cada uno de los canales se define cuando se abre. Estos procedimientos se proporcionan para fijar las prestaciones del emisor y receptor, el establecimiento de la llamada, intercambio de información, terminación de la llamada y como se codifica y decodifica. Por ejemplo, cuando se origina una llamada

telefónica sobre Internet, los dos terminales deben negociar cual de los dos ejerce el control, de manera tal que sólo uno de ellos origine los mensajes especiales de control. Es importante determinar las capacidades de los sistemas, de forma que no se permita la transmisión de datos si no pueden ser gestionados por el receptor.

Terminal H.323

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo. Un terminal H.323 consta de las interfaces del equipo de usuario, el códec de video, el códec de audio, el equipo telemático, la capa H.225, las funciones de control del sistema y la interfaz con la red por paquetes.

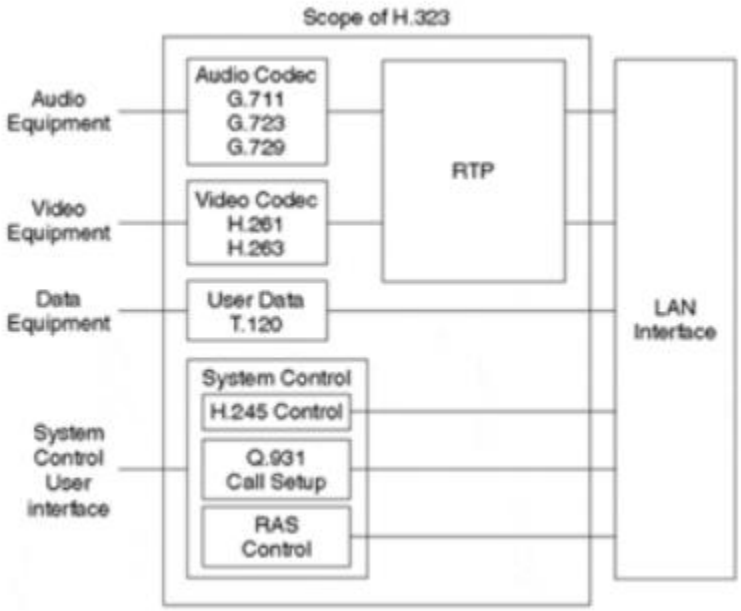

Figura 3: Terminal

Gatekeeper

El GATEKEEPER es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, GATEWAYS y MCUs. El

GATEKEEPER puede también ofrecer otros servicios a los terminales, GATEWAYS y MCUs, tales como gestión del ancho de banda y localización de los GATEWAYS.

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

El GATEKEEPER proporciona todas las funciones anteriores para los terminales, GATEWAYS y MCUs, que están registrados dentro de la denominada Zona de control H.323. Además de las funciones anteriores, el GATEKEEPER realiza los siguientes servicios de control.

Control de admisiones: El GATEKEEPER puede rechazar aquellas llamadas procedentes de un terminal por ausencia de autorización a terminales o gateways particulares de acceso restringido o en determinadas franjas horarias.

Control y gestión de ancho de banda: Para controlar el número de terminales H.323 a los que se permite el acceso simultáneo a la red, así como el rechazo de llamadas tanto entrantes como salientes para las que no se disponga de suficiente ancho de banda. Gestión de la zona: Lleva a cabo el registro y la admisión de los terminales y GATEWAYS de su zona. Conoce en cada momento la situación de los GATEWAYS existentes en su zona que encaminan las conexiones hacia terminales RCC.

Controlador Multipunto

Un controlador multipunto es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo. El Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

Procesador Multipunto

Un procesador multipunto es un componente de H.323 de hardware y software especializado, mezcla, conmuta y procesa audio, vídeo y / o flujo de datos para los participantes de una conferencia multipunto de tal forma que los procesadores del terminal no sean pesadamente utilizados. El procesador multipunto puede procesar un flujo medio único o flujos medio múltiples dependiendo de la conferencia soportada.

Proxy H.323

Proxy H.323 es un servidor que permite el acceso seguro a las redes tanto en una LAN como en una WAN, es decir de unas a otras confiando en la información que conforma la recomendación H.323.

El Proxy H.323 se comporta como dos puntos remotos H.323 que envían mensajes call – set up, e información en tiempo real a un destino del lado seguro del firewall.

Protocolo SIP

Una alternativa al H.323 surgió con el desarrollo del Session Initiation Protocol (SIP). SIP es un protocolo mucho mas lineal, desarrollado específicamente para aplicaciones de IP. Más eficientes que H.323. SIP toma ventaja de los protocolos existentes para manejar ciertas partes del proceso.

Uno de los desafíos que enfrenta el VoIP es que los protocolos que se utilizan a lo largo del mundo no son siempre compatibles. Llamadas VoIP entre diferentes redes pueden meterse en problemas si chocan distintos protocolos. Como VoIP es una nueva tecnología, este problema de compatibilidad va a seguir siendo un problema hasta que se genere un standard para el protocolo VoIP.

Componentes SIP

El Protocolo SIP soporta las funcionalidades establecer y finalizar las sesiones multimedia: localización, disponibilidad, utilización de recursos, y características de negociación.

Para poder implementar estas funcionalidades, existen varios componentes distintos en SIP. Y además elementos fundamentales, como son los agentes de usuario (UA) y los servidores.

User Agent (UA)

Consisten en dos partes distintas, el User Agent Client (UAC) y el User Agent Server (UAS).

Un UAC es una entidad lógica que genera peticiones SIP y recibe respuestas a esas peticiones.

Un UAS es una entidad lógica que genera respuestas a las peticiones SIP.

Los dos tipos se encuentran en todos los agentes de usuario, así permiten la comunicación entre diferentes agentes de usuario mediante comunicaciones de tipo cliente-servidor.

Servidores SIP Los Servidores SIP son de tres tipos:

- Proxy Server: Retransmiten solicitudes y deciden a qué otro servidor debe remitir, alterando los campos de la solicitud en caso necesario. Es una entidad intermedia que actúa como cliente y servidor con el propósito de establecer llamadas entre los usuarios. Este servidor tiene una funcionalidad semejante a la de un Proxy HTTP que tiene una tarea de encaminar las peticiones que recibe de otras entidades más próximas al destinatario.

  Existen dos tipos de Proxy Servers: Statefull Proxy y Stateless Proxy.

  i) Statefull Proxy: mantienen el estado de las transacciones durante el procesamiento de las peticiones. Permite división de una petición en varias, con la finalidad de la localización en paralelo de la llamada y obtener la mejor respuesta para enviarla al usuario que realizó la llamada.
  ii) Stateless Proxy: no mantienen el estado de las transacciones durante el procesamiento de las peticiones, únicamente reenvían mensajes.

- Registrar Server: es un servidor que acepta peticiones de registro de los usuarios y guarda la información de estas peticiones para suministrar un servicio de localización y traducción de direcciones en el dominio que controla.

- Redirect Server: es un servidor que genera respuestas de redirección a las peticiones que recibe. Este servidor reencamina las peticiones hacia el próximo servidor.

La división de estos servidores es conceptual, cualquiera de ellos puede estar físicamente una única máquina, la división de éstos puede ser por motivos de escalabilidad y rendimiento.

Funcionamiento de SIP

SIP (Session Initiation Protocol) Protocolo de inicio de sesión además es un protocolo de control desarrollado por el IETF, basado en una arquitectura de cliente-servidor muy similar al HTTP, con el que comparte muchos códigos de estado y sigue una estructura de petición-respuesta; estas peticiones son generadas por un cliente y enviadas a un servidor, que las procesa y devuelve la respuesta al cliente, además el par petición-respuesta recibe el nombre de transacción. Al igual que el protocolo HTTP, SIP proporciona un conjunto de solicitudes y respuestas basadas en códigos.

Métodos, Solicitudes y Respuestas de SIP

El Protocolo SIP utiliza Métodos, Solicitudes y respuestas correspondientes para establecer una sesión de llamada.

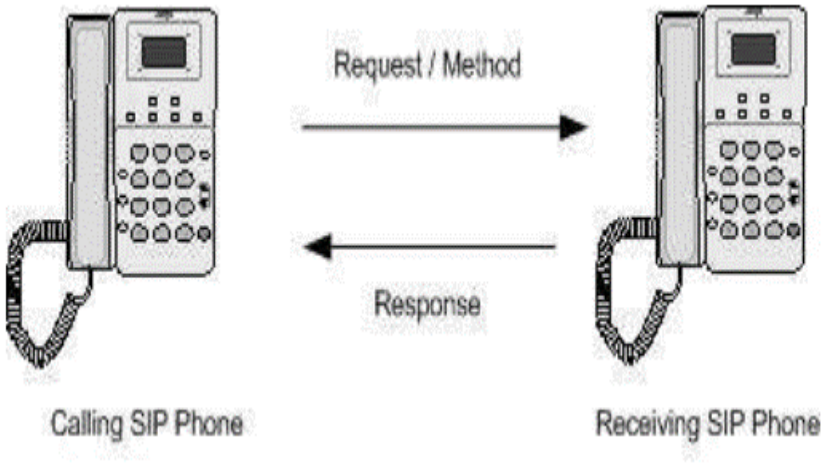

Figura 4: Solicitud y respuesta SIP.

Protocolo IAX

IAX (Inter-Asterisk Exchange protocol) es uno de los protocolos utilizado por Asterisk, un servidor PBX (central telefónica) de código abierto patrocinado por Digium. Es utilizado para manejar conexiones VoIP entre servidores Asterisk, y entre servidores y clientes que también utilizan protocolo IAX. El protocolo IAX ahora se refiere generalmente al IAX2, la segunda versión del protocolo IAX. El protocolo original ha quedado obsoleto en favor de IAX2.

Características importantes del protocolo IAX:

• Minimizar el ancho de banda usado en las transmisiones de control y multimedia de VoIP.

• Evitar problemas de NAT (Network Address Translation).

• Soporte para transmitir planes de marcación.

Una llamada IAX o IAX2 tiene tres fases:

A) Establecimiento de la llamada.

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

B) Flujo de datos o flujo de audio

Se mandan los frames M y F en ambos sentidos con la información vocal. Los frames M son mini-frames que contienen solo una cabecera de 4 bytes para reducir el uso en el ancho de banda. Los frames F son frames completos que incluyen información de sincronización. Es importante volver a resaltar que en IAX este flujo utiliza el mismo protocolo UDP que usan los mensajes de señalización evitando problemas de NAT.

C) Liberación de la llamada o desconexión

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

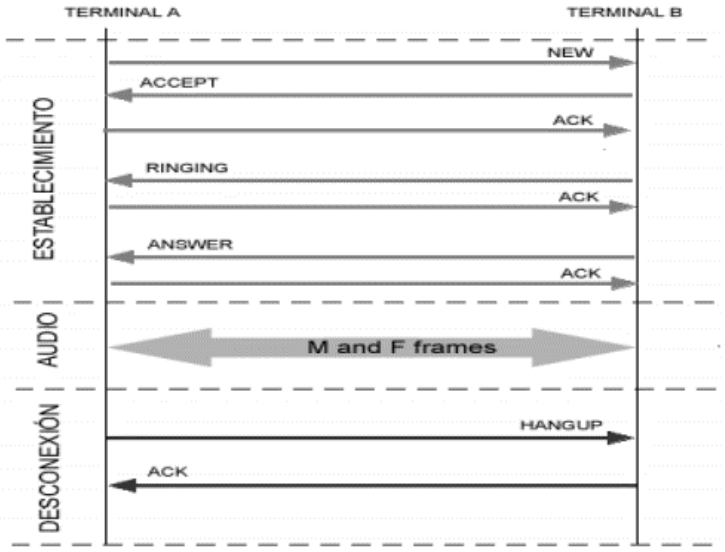

Figura 5: Protocolo IAX

Ventajas de la Telefonia IP, ¿Porque utilizar VoIP?

La primera ventaja y la más importante es el costo, una llamada mediante telefonía VoIP es en la mayoría de los casos mucho más barata que su equivalente en telefonía convencional.

Esto es básicamente debido a que se utiliza la misma red para la transmisión de datos y voz, la telefonía convencional tiene costos fijos que la telefonía IP no tiene, de ahí que esta es más barata. Usualmente para una llamada entre dos teléfonos IP la llamada es gratuita, cuando se realiza una llamada de un teléfono ip a un teléfono convencional el costo corre a cargo del teléfono ip.

Existen otras ventajas mas allá del costo para elegir a la telefonía IP:

- Con VoIP uno puede realizar una llamada desde cualquier lado que exista conectividad a internet. Dado que los teléfonos IP transmiten su información a trabes de internet estos pueden ser administrados por su proveedor desde cualquier lugar donde exista una conexión. Esto es una ventaja para las personas que suelen viajar mucho, estas personas pueden llevar su teléfono consigo siempre teniendo acceso a su servicio de telefonía IP.
- La mayoría de los proveedores de VOIP entregan características por las cuales las operadoras de telefonía convencional cobran tarifas aparte. Un servicio de VOIP incluye:
    - Identificación de llamadas.

    - Servicio de llamadas en espera
    - Servicio de transferencia de llamadas
    - Repetir llamada
    - Devolver llamada
    - Llamada de 3 líneas (three-way calling).
- En base al servicio de identificación de llamadas existen también características avanzadas referentes a la manera en que las llamadas de un teléfono en particular son respondidas. Por ejemplo, con una misma llamada en Telefonía IP puedes:
    - Desviar la llamada a un teléfono particular
    - Enviar la llamada directamente al correo de voz
    - Dar a la llamada una señal de ocupado.
    - Mostrar un mensaje de fuera de servicio

Desventajas de la Telefonía IP

Aun hoy en día existen problemas en la utilización de VoIP, queda claro que estos problemas son producto de limitaciones tecnológicas y se verán solucionadas en un corto plazo por la constante evolución de la tecnología, sin embargo algunas de estas todavía persisten y se enumeran a continuación.

- VoIP requiere de una conexión de banda ancha! Aun hoy en dia, con la constante expansión que están sufriendo las conexiones de banda ancha todavía hay hogares que tienen conexiones por modem, este tipo de conectividad no es suficiente para mantener una conversación fluida con VoIP. Sin embargo, este problema se vera solucionado a la brevedad por el sostenido crecimiento de las conexiones de banda ancha.

- VoIP requiere de una conexión eléctrica! En caso de un corte eléctrico a diferencia de los teléfonos VoIP los teléfonos de la telefonía convencional siguen funcionando (excepto que se trate de teléfonos inalámbricos). Esto es así porque el cable telefónico es todo lo que un teléfono convencional necesita para funcionar.

- Dado que VOIP utiliza una conexión de red la calidad del servicio se ve afectado por la calidad de esta línea de datos, esto quiere decir que la calidad de una conexión VoIP se puede ver afectada por problemas como la alta latencia (tiempo de respuesta) o la perdida de paquetes. Las conversaciones telefónicas se pueden ver distorsionadas o incluso cortadas por este tipo de problemas. Es indispensable para establecer conversaciones VOIP satisfactorias contar con una cierta estabilidad y calidad en la línea de datos.

- VOIP es susceptible a virus, gusanos y hacking, a pesar de que esto es muy raro y los desarrolladores de VOIP están trabajando en la encriptación para solucionar este tipo de problemas.

- En los casos en que se utilice un softphone la calidad de la comunicación VOIP se puede ver afectada por la PC, digamos que estamos realizando una llamada y en un determinado momento se abre un programa que utiliza el 100% de la capacidad de nuestro CPU, en este caso critico la calidad de la comunicación VOIP se puede ver comprometida porque el procesador se encuentra trabajando a tiempo completo, por eso, es recomendable utilizar un buen equipo junto con su configuración VoIP.

De todos modos, con la evolución tecnológica la telefonía IP va a superar estos problemas, y se estima que reemplace a la telefonía convencional en el corto plazo.

Codecs en la Telefonía IP, Codecs VoIP

Un Codec, que viene del ingles coder-decoder, convierte una señal de audio analógico en un formato de audio digital para transmitirlo y luego convertirlo nuevamente a un formato descomprimido de señal de audio para poder reproducirlo. Esta es la esencia del VoIP, la conversión de señales entre analógico-digital.

Tipos de codecs en la Telefonía IP

Los codecs realizan esta tarea de conversión tomando muestras de la señal de audio miles de veces por segundo. Por ejemplo, el codec G.711 toma 64,000 muestras por segundo. Convierte cada pequeña muestra en información digital y lo comprime para su transmisión. Cuando las 64,000 muestras son reconstruidas, los pedacitos de audio que se pierden entre medio de estas son tan pequeños que es imposible para el oído humano notar está perdida, esta suena como una sucesión continua de audio. Existen diferentes frecuencias de muestre de la señal en VOIP, esto depende del codec que se esté usando.

- 64,000 veces por segundo
- 32,000 veces por segundo
- 8,000 veces por segundo

Un codec G728A tiene una frecuencia de muestreo de 8,000 veces por segundo y esta el codec mayormente usado en VoIP. Tiene el balance justo entre calidad de sonido y eficiencia en el uso de ancho de banda.

Como Funcionan los Codecs VoIP

Los codecs operan usando algoritmos avanzados que les permiten tomar las muestras, ordenas, comprimir y empaquetar los datos. El algoritmo CS-ACELP (conjugate-structure algebraic-code-excited linear prediction) es uno de los algoritmos más comunes en VoIP. CS-ACELP ayuda a organizar el ancho de banda disponible.

El anexo B de este algoritmo CS-ACELP es el que crea la regla que dice "si ninguno está transmitiendo, no mandar ninguna información". Como aprendimos anteriormente la eficiencia creada por esta regla es una de las cosas más importantes en las que el intercambio de paquetes es superior a la conmutación de circuitos. Es el Anexo B en este algoritmo CS-ACEPL que es responsable de esta regla en las llamadas VoIP.

Capitulo 2. Cisco Call Manager

El software Cisco Call Manager es la solución de Cisco para las comunicaciones telefónicas IP. Es distribuible, escalable y una solución de procesamiento de llamadas de telefonía IP de gran disponibilidad para una empresa de gran tamaño debido al gran número de usuarios que puede soportar.

Cisco Call Manager proporciona a la empresa características y capacidad para los dispositivos de red de telefonia como son los teléfonos IP, VoIP Gateways y aplicaciones multimedia. También es posible ampliarlo con servicios adicionales como la mensajería, la conferencia multimedia, etc.

Hemos estado escuchando acerca de VoIP durante muchos años y aunque algunos nunca han trabajado con él, se ha convertido en el estándar de hoy en comunicaciones IP y Private Branch Exchange (PBX) o soluciones de centro de telefonía.

Vendedores populares como Siemens, Panasonic, Alcatel y muchos más que, hasta hace poco, no ofrecían soluciones de VoIP, vieron la nueva ola llegar y producir soluciones que permitirían a sus sistemas soportar VoIP. Sin embargo, estos productos "híbridos" **no son VoIP puro** y no admiten las características de VoIP PBX esperadas, tales como SIP Trunking con proveedores globales, selecciones de códec, protocolo de señalización de llamadas H.323 y más.

CME es un sistema de telefonía IP basado en software integrado en las siguientes versiones más avanzadas de Cisco IOS. Los nuevos paquetes de Cisco IOS son los siguientes y los **destacados** proporcionan funcionalidad CME:

1. Base de IP
2. Voz IP
3. Base de empresa
4. seguridad avanzada
5. Servicios SP
6. Servicios IP avanzados
7. Servicios empresariales
8. Servicios empresariales avanzados

Las capacidades de Cisco Call Manager son:

- Soporte de audio y video telefonía
- Hasta 30.000 teléfonos por clúster
- Corre sobre un appliance con sistema operativo endurecido

- Basado en base de datos Informix de IBM
- Sistema de Recuperación ante desastres (DRS) para respaldos y mecanismos de restauración

Flujo de Datos Cisco Call Manager

- Señalización y el control de la sesión fluye entre el Cisco Unified CM y el teléfono IP, y entre el Cisco Unified CM y el Gateway de la PSTN

- El flujo de audio es terminado en el Gateway PSTN, y se convierte el flujo en Time Division Multiplexing (TDM)

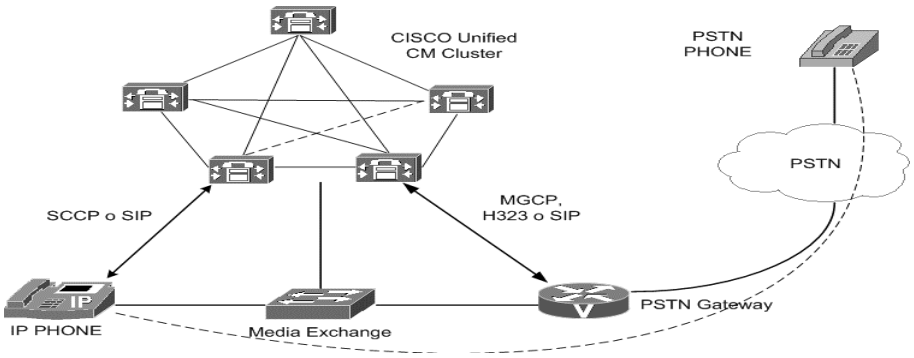

Figura 6: Flujo de llamada

Topología de llamada

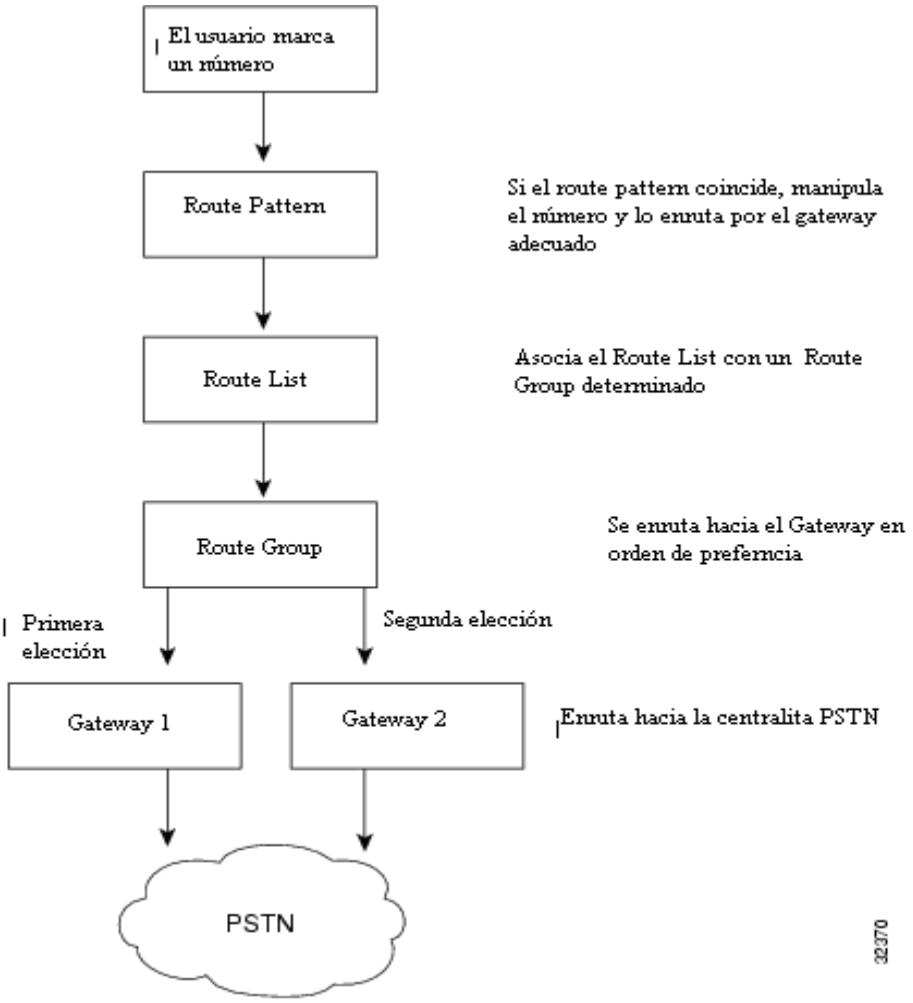

Figura 7:Topología de llamada

- Router PARTITIONS

- Dividen el conjunto de route patterns en subconjuntos de destinos alcanzables identificados por un nombre.
- Una partición contiene una lista de Route Patterns.
- Facilitan el enrutado de llamadas dividiendo el route plan en subconjuntos lógicos que se pueden basar en la organización, localización y tipo de llamada.

- SEARCH SPACES

- Es una lista ordenada de rutas de partición. Estas rutas se asocian a los dispositivos (teléfonos).

- Determinan las particiones que los dispositivos que hacen una llamada buscan para que esta llamada se realice

- ROUTE PATTERNS

- La llamada al destino se hace solo si se marca la secuencia correcta definida en el route pattern

- Se pueden usan caracteres especiales (x…) para hacer rangos

- Definir route patterns para diferentes tipos de llamadas: nacionales

Capitulo 3 Red Priva da Virtual (VPN)

La Red Privada Virtual (VPN), cuyo nombre deriva del inglés Virtual Private Network, es una tecnología de red que permite la extensión de una red local sobre una red pública o no controlada, como por ejemplo Internet, mediante un proceso de encapsulación y encriptación, en la cual los paquetes de datos viajan a distintos puntos remotos por medio de un "túnel" definido en una infraestructura pública de transporte.

POR QUÉ UNA VPN?

Las VPN son una salida al costo que puede significar el pagar una conexión de alto costo, para usar líneas alquiladas que estén conectadas a otros puntos que puedan hacer uso de la conexión a Internet o para hacer negocios con clientes frecuentes a través de la red.

Los datos son codificados o cifrados e inmediatamente enviados a través de la conexión, para de esa manera asegurar la información y la contraseña que se esté enviando. Cuando deseo enlazar mis oficinas centrales con alguna sucursal u oficina remota tengo tres opciones:

Modem: La mayor desventaja es el costo de la llamada, ya que sería por minuto conectado, además sería una llamada de larga distancia y la conexión no contaría con la calidad y velocidad adecuadas.

Línea Privada: Tendría que tender mi cable ya sea de cobre o fibra óptica de un punto a otro, en esta opción el costo es muy elevado porque si necesito enlazar mi oficina central con una sucursal que se encuentra a 200 kilómetros de distancia el costo sería por la renta mensual por kilómetro, sin importar el uso.

VPN: Los costos son bajos porque solo realizo llamadas locales, además de tener la posibilidad de que mis datos viajen encriptados y seguros, con una buena calidad y velocidad.

Las VPNs son una gran solución a distintos problemas, pero solo en el campo de la economía de los usuarios porque por ejemplo en el caso de que se realice una conexión entre dos sedes de empresas, una en Japón y la otra en Chile, sería muy costoso el realizar un cableado entre estos dos países, y un enlace inalámbrico satelital sería muy costoso. Es por ello que una red privada virtual es más económica porque solo se hace uso de Internet que es un conjunto de redes conectadas entre si.

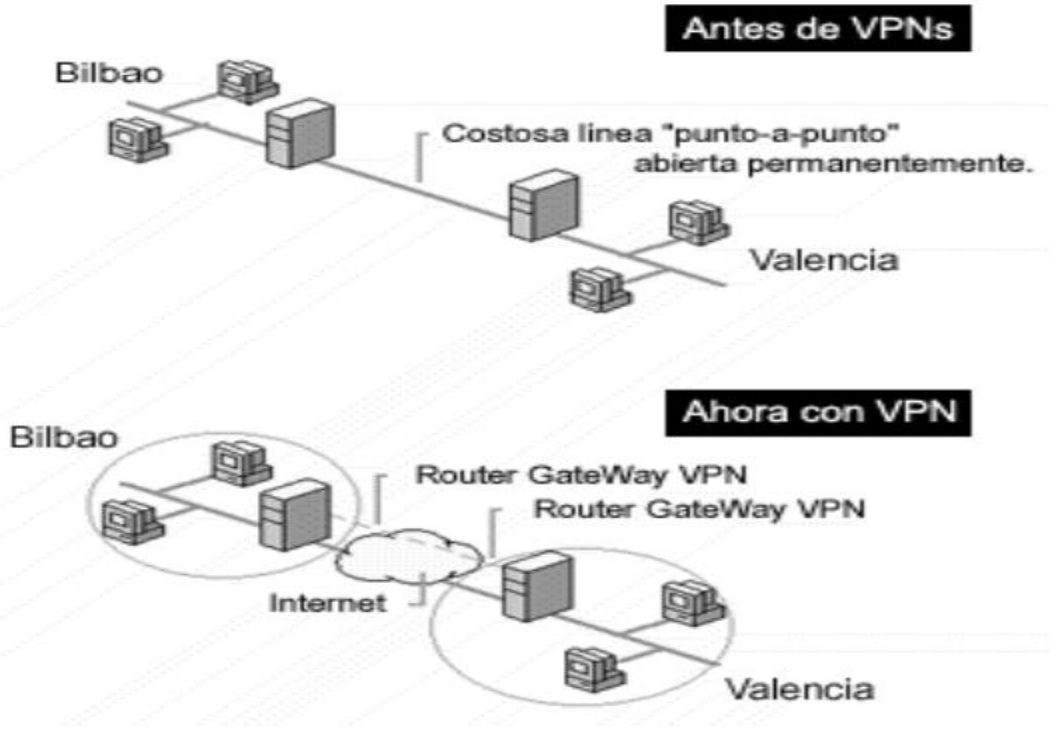

Figura 8: VPN antes y ahora.

COMPONENTES QUE CONFORMAN UNA VPN

Las VPN consisten hardware y software, y además requieren otro conjunto de componentes. Estos componentes son simples requisitos que garantizan que la red sea segura, este disponible y sea fácil de mantener. Son necesarios ya sea que un PSI proporcione la VPN o que usted haya decidido instalar una por si mismo.

- DISPONIBILIDAD Se aplica tanto al tiempo de actualización como al de acceso.

- CONTROL Suministra capacitación, experiencia, supervisión meticulosa y funciones de alerta que ofrece algunos proveedores de servicios administrados. Una consideración significativa es que sin importar que tan grande sea la organización, es probable que solo cuente con una VPN; puede tener otros puntos de acceso pero seguirá siendo una VPN corporativa.
- COMPATIBILIDAD Para utilizar tecnología VPN e Internet como medio de transporte, la arquitectura interna del protocolo de red de una compañía debe ser compatible con el IP nativo de Internet.

- SEGURIDAD Lo es todo en una VPN, desde el proceso de cifrado que implementa y los servicios de autenticación que usted elige hasta las firmas digitales y las autoridades emisoras de certificados que utilizan. Abarca el software que implementa los algoritmos de cifrado en el dispositivo de la VPN.

- CONFIABILIDAD Cuando una compañía decide instalar el producto VPN de un PSI, está a merced de este.

- AUTENTICACION DE DATOS Y USUARIOS Datos: Reafirma que el mensaje a sido enviado completamente y que no ha sido alterado de ninguna forma. Usuarios: clientes que se conectan a la VPN.

- SOBRECARGA DE TRAFICO En todo tipo de tecnologías existen sacrificios: velocidad contra desempeño, seguridad contra flexibilidad. Las VPN caben en la misma categoría cuando se hablan de tamaño de paquetes cifrados las sobre carga esta en juego, ya que si mandamos varios paquetes se incrementa el tamaño de estos y por lo tanto se afecta la utilización del ancho de banda.

Tipos de VPN´s

VPN Punto a punto

Esta basado en las conexiones desde un eje central (Sede principal de la empresa) o componente central VPN y los servidores de otras oficinas que estén remotas. Se conectan a internet solo utilizando internet de los proveedores de servicios, en definitiva es medida de ahorro en cables y conexiones físicas o denominados conexiones punto a puntos tradicionales, sobre todo si se encuentran ubicadas en diversos estados del país o incluso fuera de él.

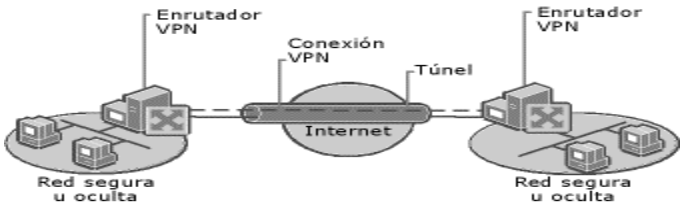

Figura 9:VPN Punto a Punto

VPN Interna (Over LAN):

Funciona como una **VPN** de uso normal solo con la diferencia que es centralizada en la misma **red local** (LAN), el objetivo de esta VPN es aislar todas las partes de la red y sus servicios entre sí con el propósito de tener más seguridad. Este tipo de VPN no es de uso frecuente, pero se recomienda para tener una conexión más segura para el acceso inalámbrico separando toda **red** física para que no haya ningún acceso que no haya sido autorizado y ninguna exposición de la información.

VPN de Acceso Remoto

En las redes empresariales es el más utilizado, teniendo como punto principal un Proveedor que se conecta a una red perteneciente a la compañía desde otros puntos lejanos, que pueden ser desde Hoteles, Aviones exclusivos, Oficinas Comerciales, Sucursales, etc. utilizando como sustento la de red pública que está a mayor disponibilidad, esto es, una conexión a Internet.

En esta ocasión, la forma de ingresar a esta Red Privada Virtual está dada por la asignación a cada Cliente de una forma de autenticación, que generalmente lleva este acceso la modalidad de Usuario y Contraseña, o bien a través del acceso en primera instancia a una Red de Área Local dentro de la empresa.

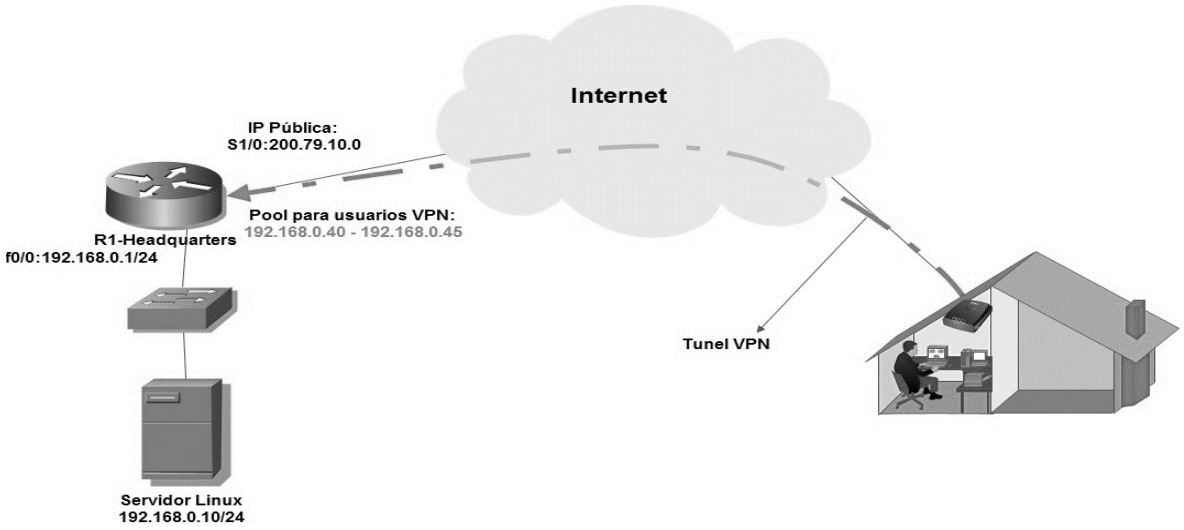

Figura 10:VPN de Acceso Remoto

IPSec

El conjunto de protocolos en el IPSec (Internet Protocol Security) tienen como finalidad hacer más seguras las comunicaciones dentro del IP, autenticando y cifrando cada paquete del flujo de datos. Es un protocolo diseñado por la IETF, que se definió en el RFC4301. También incluye protocolos para establecer la autenticación mutua entre agentes al inicio de la sesión y la negociación de llaves criptográficas durante la sesión. IPSec puede ser usado para proteger flujos de datos entre un par de hosts, ya sean servidores o clientes, entre un par de puertas de enlace (gateway) de seguridad, ya sean firewalls o ruteadores, o entre una puerta de enlace un hosts. IPSec es un esquema de seguridad en modo dual, de punto a punto, operante en la capa 3 del modelo OSI.

Componentes

Los protocolos que usa IPSec son:

IKE (Internet Key Exchange) para llevar a cabo una asociación de seguridad (SA, security asociation) al llevar las negociaciones de los protocolos y algoritmos, además de generar las llaves de cifrado y autenticación que serán usadas por IPSec.

Encabezado de Autenticación (AH authentication header) para proveer integridad y autenticación de origen de datos para los datagramas IP y para proveer protección contra los ataques de respuesta (reply attacks).

El encabezado de carga de seguridad de encapsulamiento (ESP encapsulating security payload) para proveer confidencialidad, autenticación de origen de datos, integridad sin conexión (conectionless), un servicio anti-respuesta, un tipo de secuencia parcial de integridad y una limitada confidencialidad de flujo de tráfico. ESP también soporta configuraciones de sólo cifrado y sólo autenticación, aunque esto se desaconseja. A diferencia del encabezado de autenticación ESP no protege el encabezado de paquete IP. En el modo de túnel, donde el paquete completo original es encapsulado con un nuevo encabezado de paquete, la protección que ofrece ESP abarca a todo el paquete, incluyendo el encapsulado, mientras que el encabezado exterior continua sin protección. Este encabezado opera directamente al principio del IP, usando el número 50 del IP. Observamos la forma del encabezado de carga seguridad en el cuadro 4 de la siguiente página.

0-7 bits	8-15 bits	16-23 bits	24-31 bits
Índice de parámetros de seguridad (*SPI*)			
Números de Secuencia.			
Carga útil de datos (variable)			
	Relleno (0-255 bytes)		
		Long. de relleno	Prox. encabezado
Autenticación de datos (variable)			

Figura 11: Encabezado de carga de seguridad.

Trama IPSec

La trama del conjunto de protocolos IPSec se compone de los encabezados de autenticación y el encabezado de próximo encabezado.

Encabezado de Autenticación (AH)

El encabezado de autenticación es parte del conjunto de protocolos Elipse. Este garantiza la integridad sin conexión (conectionless) y autenticación del origen de los paquetes IP. Además puede, opcionalmente, proteger contra los ataques de respuesta (reply attacks) usando la técnica de deslizamiento de ventanas (sliding windows) y descartando paquetes viejos. El encabezado de autenticación protege la carga IP y todos los campos de encabezados de un datagrama IP con excepción de los campos que vayan a modificarse durante su trayectoria.

En IPv4, los campos de encabezados variables y por lo tanto inautenticados, incluyen al campo (DSCP differentiated services code point) de apuntador de código de servicios diferenciados, tipo de servicios (TOS type of servicie), banderas, fragment offset, tiempo de vida (TTL time to live) y el encabezado de suma de verificación (Checksum).

El encabezado de autenticación trabaja directamente al principio del IP, usando el número de protocolo IP 51.

0-7 bits	**8-15 bits**	**16-23 bits**	**24-31 bits**
Prox. Encabezado	Long. carga útil	Reservado	
Índice de parámetros de seguridad (*SPI*)			
Número de secuencia.			
Autenticación de datos (variable)			

Figura 12: Encabezado de autentificación.

El encabezado de Próximo encabezado, que se muestra en el cuadro 5, es un campo de ocho bits que identifica el tipo de la próxima carga útil después del encabezado de autenticación (AH). El valor de este campo se escoge del conjunto de números de protocolo IP que se definió en el más reciente RFC de asignación de números del IANA (Internet Assigned Number Authority).

- La longitud de carga útil es el tamaño de del paquete del encabezado de autenticación.
- La parte de reserva se utilizará en el futuro, se llenará de ceros hasta entonces
- El índice de parámetros de seguridad (SPI) identifica a los parámetros de seguridad, los cuales en combinación con la dirección ip identifica la asociación de seguridad implementada en este paquete.
- El número de secuencia es un número monotónico incremental, usado para prevenir ataques de respuesta.
- La autenticación de datos contiene el valor de chequeo de integridad (ICV integrity check value) necesario para autenticar el paquete.

Arquitectura IPSec

La arquitectura de IPSec especifica la base en la cual todas las implementaciones serán construidas y define los servicios de seguridad proveídos por IPSec, cómo y dónde pueden ser usados, cómo serán los paquetes construidos y procesados, y la interacción de procesamiento de IPSec con las políticas de seguridad.

Esta arquitectura define hasta que nivel podrá ser definido y usado por el usuario de acuerdo a las políticas de seguridad, permitiendo que cierto tráfico sea identificado para recibir el nivel de protección deseable.

IPSec fue definido para proveer un alto nivel de seguridad criptográfica, para ambas versiones del IP. Componiéndose de los siguientes encabezados que proveen seguridad en el tráfico: el encabezado de autenticación AH (Autentication Header) y el encabezado de encapsulamiento de carga útil de seguridad ESP (Encapsulating Security Payload), incluyendo los protocolos que generan y administran las llaves de cifrado, IKE (Internet Key Exchange) e ISAKMP (Internet Security Key Association and Key Management Protocol). 27

IPSec maneja a través de las asociaciones de seguridad SA (Security Association) su esquema de interoperabilidad, controladas por el índice de parámetros de seguridad SPI (Security Parameter Index), que se norman por las políticas de seguridad SP (Security

Policy); las cuales se almacenan en bases de datos. También se define como dichas bases de datos se relacionarán con las distintas funciones de procesamiento de IPSec, y como distintas implementaciones del IPSec pueden coexistir.

Las políticas establecidas pueden tener dos vertientes, las estáticas y las dinámicas. Las políticas estáticas serán previamente establecidas y contendrán valores fijos, los cuales establecerán los parámetros que se negociarán; estableciendo canales seguros. O pueden ser dinámicas, en cuyo caso se podrán usar protocolos de administración de llaves como ISAKMP.

Protocolo del encabezado de autenticación

El encabezado de encapsulamiento de carga de seguridad, se define en el RFC 4303, tiene como objetivo principal proporcionar confidencialidad, especificando el modo de cifrar los datos que se desean enviar y como este contenido cifrado se incluye en un datagrama IP. Puede ofrecer servicios de antiréplica, integridad y autenticación del origen de los datos incorporando un mecanismo similar al a AH. El encabezado ESP se inserta después del encabezado IP y antes del encabezado del protocolo de capa superior (modo transporte) o antes del encabezado IP encapsulado (modo túnel).

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de llave simétrica. Típicamente se usan algoritmos de cifrado por bloques (DES), de modo que la longitud de datos a cifrar tenga que ser un múltiplo de tamaño de bloque (8 o 16 bytes, en la mayoría de los casos). Por esta razón existe un campo de relleno cuya finalidad es añadir caracteres de relleno al campo de datos para ocultar así su longitud real, y por lo tanto las características del tráfico.

El encabezado de autenticación de definió en el RFC 4302, es un encabezado de IPSec usado para proporcionar integridad en los datos, autenticación en el origen de los datos y opcionalmente servicios de anti-réplica en los datagramas IP. No proporciona ninguna garantía de confidencialidad.

Se suele situar justo antes de los datos, de forma que los proteja de posibles atacantes. Ha sido diseñado de forma muy versátil, de manera que puede incluirse antes que otros encabezados para asegurar que las opciones que acompañan al datagrama sean las correctas.

Métodos de autenticación

La autenticación en IPSec se logra a tráves de algoritmos de autenticación, tales como MD5, SHA-1, HMAC, RIPEMD-160.

Asociaciones de seguridad y políticas

Una SA es la forma básica de comunicación en IPSec refiriéndose a un contrato entre dos entidades que desean comunicarse en forma segura. Las SA determinan los encabezados de IPSec a utilizar, las transformaciones, las llaves y la duración de validez de dichas llaves. Las SA son de un solo sentido, cada entidad con IPSec tendrá una SA para el tráfico entrante y otra para el trafico saliente; además de que son específicas para cada encabezado. Cuando se implementa IPSec, se crea una base de datos de las SA denominada SAD donde se almacenan todas las SA de dicha implementación.

La manera que tiene las SA de identificarse de manera única, es a través de los SPI. Estos son entidades de 32 bits, por los cuales se comunican dos entidades de manera segura e indicarán los parámetros usados, tales como llaves y algoritmos.

Para el manejo de las SA's se establecen dos tareas principalmente: creación y eliminación; que a su vez se pueden ejecutar de manera manual o dinámica a través de un protocolo de intercambio de llaves como IKE. La creación de llaves se lleva a través de la negociación de los parámetros de las SA y la correspondiente actualización de la SAD. El manejo manual de llaves es obligatorio en toda implementación, el proceso de asignación del SPI y la negociación de parámetros es totalmente manual y permanecerán hasta que sean manualmente borrados. Para el manejo dinámico de las llaves se utiliza IKE.

Protocolo de intercambio

El conjunto de protocolos que forman IPSec están diseñados con capacidad de expansión que dan servicios de seguridad como el control de acceso, integridad, confidencialidad y autenticación. El mismo es capaz de proteger paquetes IP entre hosts y gateways, gaterías, hosts, etc. Este conjunto de protocolos puede ser implementado en IPv4 de manera opcional, y aunque en IPv6 se debería implementar de manera obligada, esto también puede no serlo.

Una de las características de IPSec es su posibilidad de acoplamiento a otras tecnologías, aunado al hecho de que es posible cambiar los algoritmos criptográficos estándar por otros más robustos. IPSec maneja una especificación de arquitectura que

deberá ser la base de todas las implementaciones, definiendo los servicios que esta proveerá, como se procesara la información y dónde, además de como se deben de definir las políticas de seguridad a usar en la misma. Ha sido diseñado para proveer seguridad criptográfica para ambas versiones del IP. Tiene dos encabezados que proveen la seguridad del tráfico de información (AH [authenticaction header] y ESP [encapsulating security payload]), protocolos que generan y administran las llaves (ISAKMP [internet security association and key managment protocol] e IKE [intenet key exchange].

El esquema de interoperabilidad de IPSec se maneja a través de SAs (Security Associations) las cuales son controladas por un SPI (Security Parameter Index), y regidas por un SPs (Security Policy) que se configuran previamente; tanto las SAs como las SPs se almacenan son almacenadas en sus respectivas bases de datos: SAD para las asociaciones de seguridad y SPD para las políticas. La arquitectura de IPSec también define la interacción que hay entre estas bases de datos con las diferentes funciones de procesamiento de IPSec (cifrado y descifrado) y define cómo varias implementaciones de IPSec pueden existir.

Los parámetros que se negocian para establecer los canales seguros se indican bajo las políticas preestablecidas dentro de un esquema de funcionamiento estático con valores fijos y previamente establecidos, o bien, en un esquema de funcionamiento dinámico utilizando un protocolo de administración de llaves como ISAKMP (Internet Security Association and Key Managment Protocol). Estas políticas determinan si dos entidades son capaces de comunicarse entre sí y cuál sería la transformación a usar en un caso dado.

IPSec proporciona los siguientes servicios de seguridad:

- Control de acceso
  Previene el uso no autorizado de recursos, garantizando que sólo acceden a la información y a los recursos los usuarios que tiene permiso para ellos.

- Integridad
  Implica que los datos no puedan ser modificados o corrompidos de manera alguna desde su transmisión hasta su recepción en una comunicación.

- Autenticación
  Definen mecanismos para garantizar la procedencia de la información, de modo que se puede verificar que realmente es el remitente autorizado quien lo envió.

- Protección a la réplica
  Asegura que una transacción sólo se pueda llevar a cabo una vez, a menos que se autorice una repetición de la misma. Nadie debería poder grabar una transacción para luego replicarla para aparentar múltiples transacciones del remitente original.

- Confidencialidad

Implica que la información sea accesible únicamente por las entidades, sistemas o personas autorizadas, asegurando la privacidad de la información al no ser consultada por terceras personas.

- Confidencialidad limitada en el flujo de tráfico

  Este servicio se refiere a ocultar las direcciones fuente y destino, la longitud del mensaje, o la frecuencia de la comunicación. En el contexto de IPSec, usando ESP en modo túnel, especialmente en un gateway de seguridad, puede proporcionar un cierto nivel de confidencialidad en el flujo de tráfico.

  IPSec proporciona un nivel de seguridad común y homogéneo para todas las aplicaciones, además de ser independiente de la tecnología física empleada. Cuando se implementa IPSec en un firewall o enrutador, éstos proporcionan una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza el perímetro.

  Por otro lado, al estar implementado en la capa de red, debajo de los protocolos TCP/UDP resulta "transparente" para las aplicaciones, es decir, no hay necesidad de realizar alguna configuración desde el punto de vista de usuario final ni del servidor. También IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable, resultando útil para los empleados que accedan a la red desde el exterior vía telefónica. Además, es posible asegurar una subred virtual dentro de una organización para las aplicaciones más sensibles.

  Facilita el comercio electrónico de negocio a negocio al proporcionar una infraestructura segura sobre la cual realizar transacciones usando cualquier aplicación, por ejemplo las extranets.

  Los algoritmos permitidos para la protección con IPSec, tanto los usados para autenticación como los usados para cifrado, idealmente desempeñan dos metas incompatibles: proveer máxima protección contra una gran variedad de ataques matemáticos, de análisis criptológico y de fuerza bruta; y por otro lado, requerir un procesamiento mínimo en el lado de cada participante dentro de la comunicación. Aunque los documentos de IPSec decretan algoritmos específicos para proveer un grado estándar, con seguridad interoperable, se pueden implementar algoritmos adicionales ya sea para dominio público o privado.

  Todos los algoritmos son algoritmos de bloque, empiezan en el inicio del mensaje y cada bloque es procesado uno a la vez. El tamaño del bloque es parte de la definición de cada algoritmo, donde el más común es de 8 bytes (64 bits). Cada bloque pasa de cierto modo por algún procesamiento repetitivo donde cada iteración de ese procesamiento es conocido como ciclo.

El número de ciclos es algunas veces considerado como una característica importante en la criptografía de un algoritmo. Cada ciclo, en turno, consiste de una función de ciclo, la cual es un procesamiento que constituye cada ciclo del cifrado. La función de ciclo puede ser simple y sencilla, o extremadamente compleja. Algunos algoritmos tienen múltiples funciones de ciclo que se pueden aplicar a uno o más ciclos. En muchos algoritmos, la llave secreta más completa no es usada como función hash o para cifrar cada bloque, sino para generar múltiples sub-llaves, o ciclos de llave donde a su vez cada ciclo puede incorporar una o más sub-llaves. Si cada bloque fuera cifrado o manejado por una función hash separadamente, se presentarían ataques más fáciles, ya que el contenido de algunas partes del paquete de Internet serían conocidas. En el caso de una función hash, el hash final se debe reflejar en todos los bits de todo el bloque de entrada, no solo en el último bloque. En el caso de un algoritmo de cifrado, si cada bloque es descifrado separadamente, sin hacer referencia a ningún otro bloque, los bloques previsibles pueden ser atacados más fácilmente una vez que la llave fue conocida y todo el bloque puede ser descifrado. Por esta razón, todo algoritmo de manera obligatoria en IPSec incorpora dentro de su definición un mecanismo de retroalimentación, es decir, el cifrado o autenticación de cada bloque tiene como una de sus entradas la salida calculada criptográficamente del bloque previo.
La seguridad de los algoritmos criptográficos dependerá de la complejidad de su criptografía y de su robustez. Sin embargo, un algoritmo criptográfico no es suficiente para garantizar la seguridad de las comunicaciones debido a que varios factores juegan un papel muy importante, como por ejemplo, la implementación en hardware o software, o bien, la generación de llaves secretas que deberán tener una apropiada longitud, complejidad y ser generadas, intercambiadas, administradas y almacenadas de una manera segura.

El protocolo IPSec ha sido diseñado en forma modular de modo que se puedan seleccionar determinados algoritmos para cifrado y autenticación sin afectar a otras partes de la implementación.

Sin embargo, han sido definidos algunos algoritmos de manera estándar para soportar todas las implementaciones y asegurar la interoperabilidad en el mundo global de Internet, como son AES (en etapa de evaluación) para sustituir a DES y 3DES, considerados actualmente para cifrado, así como MD5 y SHA-1 como funciones hash para autenticación. Además es perfectamente posible usar otros algoritmos que se consideren más seguros o más adecuados para un entorno específico, como por ejemplo IDEA o Blowfish.

Para los algoritmos de autenticación se utilizan las funciones hash (o primitivas hash), cuya funcionalidad es usada principalmente para resolver el problema de integridad y autenticidad del origen de los mensajes.

Una función hash o “función resumen” es un algoritmo que, aplicado a un mensaje determinado, crea una representación digital o hash de una longitud fija mucho menor que el mensaje original, pero substancialmente único a él, de tal manera, que no sea factible, dado solamente el hash, reconstruir el mensaje original, es decir, las funciones hash son de una sola dirección. Un simple ejemplo de una función hash sería contar el número de letras del mensaje, si es par asociamos un 0 y si es impar un 1. El principal inconveniente de este sistema es que pueden existir colisiones (dos mensajes diferentes producen la misma salida) por lo que conviene que las funciones tengan un rango de salida lo suficientemente grande (128 bits o más) para poder considerarlas libres de colisión.

Capítulo 4. Nat

Internet en sus inicios no fue pensado para ser una red tan extensa, por ese motivo se reservaron “sólo” 32 bits para direcciones, el equivalente a 4.294.967.296 direcciones únicas, pero el hecho es que el número de máquinas conectadas a Internet aumentó exponencialmente y las direcciones IP se agotaban. Por ello surgió la NAT o Network Address Translation (en castellano, Traducción de Direcciones de Red)

La idea es sencilla, hacer que redes de ordenadores utilicen un rango de direcciones especiales (IPs privadas) y se conecten a Internet usando una única dirección IP (IP pública). Gracias a este “parche”, las grandes empresas sólo utilizarían una dirección IP y no tantas como máquinas hubiese en dicha empresa. También se utiliza para conectar redes domésticas a Internet.

NAT como medio de seguridad

Este ahorro de direcciones es solo uno de los motivos de utilizar NAT. Implementando NAT crea una especie de Firewall entre tu red interna y las redes externas, o entre tu red interna e Internet. NAT solo permite conexiones que se originen dentro del dominio. En esencia, esto significa que un ordenador en una red externa no puede conectar contigo a no ser que tú hayas iniciado el contacto. Puedes conectarte a Internet, e incluso bajarte archivos, pero una persona en Internet no puede conectarse a tu IP e iniciar una conexión. Por supuesto, existen vulnerabilidades que podrían saltarse esta regla, pero ese es otro tema.

NAT es algunas veces confundido con los servidores Proxy, pero existen diferencias entre ellos. NAT es transparente para los ordenadores de origen y destino. Ninguno de ellos es consciente de que están interactuando con un tercer dispositivo, NAT en este caso. Un Proxy no es transparente. El ordenador de origen sabe que está haciendo una petición al Proxy y debe ser configurado para que lo haga.

Por otro lado, el ordenador de destino cree que el servidor Proxy es el ordenador de origen, y se comunica con el directamente.

¿Cómo funciona Nat?

En la NAT existen varios tipos de funcionamiento:

Estática

Una dirección IP privada se traduce siempre en una misma dirección IP pública. Este modo de funcionamiento permitiría a un host dentro de la red ser visible desde Internet. (Ver imagen anterior).

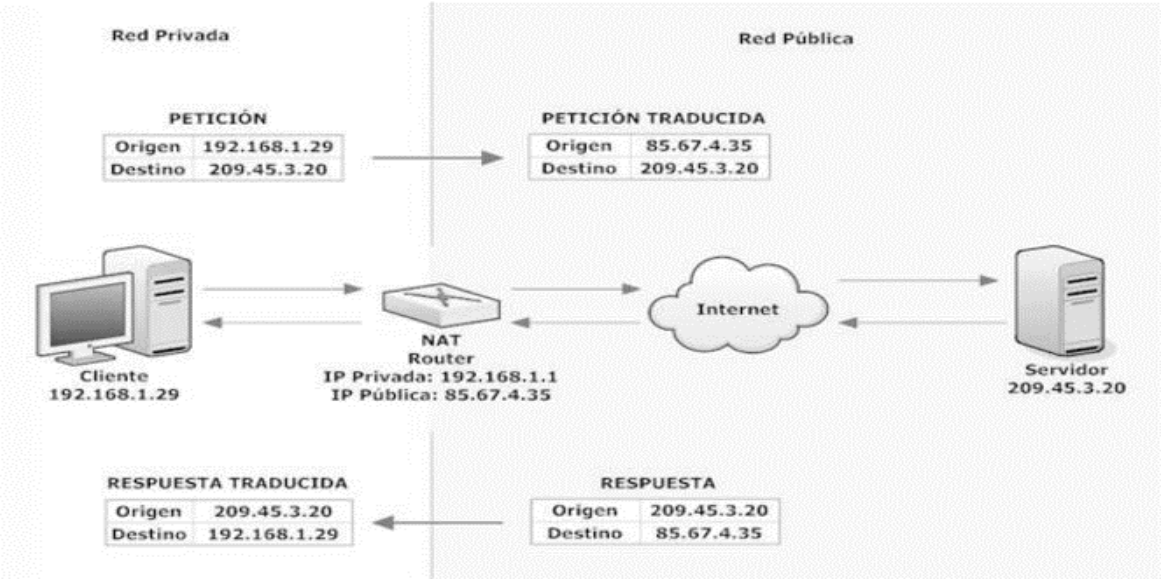

Figura 13: Funcionamiento de Nat

Dinámica

El router tiene asignadas varias direcciones IP públicas, de modo que cada dirección IP privada se mapea usando una de las direcciones IP públicas que el router tiene asignadas, de modo que a cada dirección IP privada le corresponde al menos una dirección IP pública.

Cada vez que un host requiera una conexión a Internet, el router le asignará una dirección IP pública que no esté siendo utilizada. En esta ocasión se aumenta la seguridad ya que dificulta que un host externo ingrese a la red ya que las direcciones IP públicas van cambiando.

Sobrecarga

La NAT con sobrecarga o PAT (Port Address Translation) es el más común de todos los tipos, ya que es el utilizado en los hogares. Se pueden mapear múltiples direcciones IP privadas a través de una dirección IP pública, con lo que evitamos contratar más de una dirección IP pública. Además del ahorro económico, también se ahorran direcciones IPv4, ya que aunque la subred tenga muchas máquinas, todas salen a Internet a través de una misma dirección IP pública.

Para poder hacer esto el router hace uso de los puertos. En los protocolos TCP y UDP se disponen de 65.536 puertos para establecer conexiones. De modo que cuando una máquina quiere establecer una conexión, el router guarda su IP privada y el puerto de origen y los asocia a la IP pública y un puerto al azar. Cuando llega información a este puerto elegido al azar, el router comprueba la tabla y lo reenvía a la IP privada y puerto que correspondan.

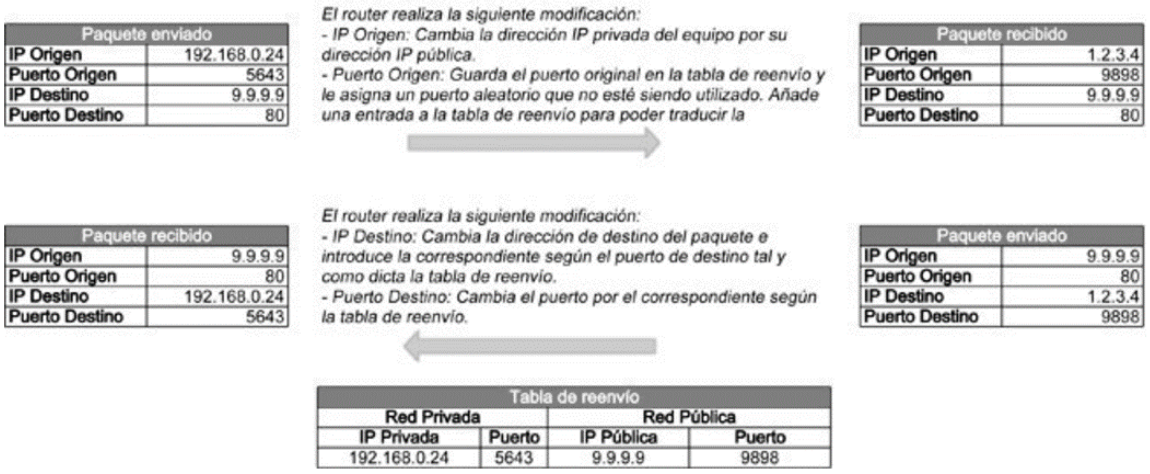

Figura 14: Funcionamiento de NAT Sobrecargado

NAT Tranversal

Como se mencionó anteriormente a veces se requiere comunicación entres IP's privadas esto se logra mediante técnicas NAT Traversal. A toda técnica que logre atravesar la barrera de los router NAT se les denomina NAT Traversal, sin importar la forma para lograrlo, es por eso que estás técnicas no están estandarizadas, pese a esto hay dos métodos que se diferencian:

- Uso de un servidor como vía de la comunicación: Lo que se hace en esta situación es generar dos conexiones, una entre el cliente 1 y el servidor, y la otra entre el

servidor y el cliente 2, este servidor contiene una IP pública conocida a priori por ambos clientes. Primeramente, ambos clientes hacen un handshake con el servidor, determinando así los puertos dentro del servidor a ser utilizados. Es así como se genera una "falsa comunicación" ya que el cliente 1 envía información al servidor, este la almacena y luego este mediante la aplicación la envía al cliente 2.

- Uso de un servidor para establecer la comunicación: En este caso el servidor solo es utilizado como pasarela de información. Primeramente, se establecen las conexiones respectivas entre ambos clientes y el servidor, y luego este les comunica el puerto e IP públicas de los clientes a los otros clientes, encaminando así los paquetes. Cabe mencionar que no se pierde el contacto con el servidor ya que este constantemente tiene que estar informando a los clientes sobre los estados de las conexiones y puertos de los otros clientes.

Ventajas y desventajas de NAT

Ventajas de la NAT

El uso de la NAT tiene varias ventajas:

- La primera y más obvia, el gran ahorro de direcciones IPv4 que supone, recordemos que podemos conectar múltiples máquinas de una red a Internet usando una única dirección IP pública.
- Seguridad. Las máquinas conectadas a la red mediante NAT no son visibles desde el exterior, por lo que un atacante externo no podría averiguar si una máquina está conectada o no a la red.
- Mantenimiento de la red. Sólo sería necesario modificar la tabla de reenvío de un router para desviar todo el tráfico hacia otra máquina mientras se llevan a cabo tareas de mantenimiento.

Desventajas de la NAT

Recordemos que la NAT es solo un parche, no una solución al verdadero problema, por tanto también tiene una serie de desventajas asociadas a su uso:

- Checksums TCP y UDP: El router tiene que volver a calcular el checksum de cada paquete que modifica. Por lo que se necesita mayor potencia de computación.
- No todas las aplicaciones y protocolos son compatibles con NAT. Hay protocolos que introducen el puerto de origen dentro de la zona de datos de un paquete, por lo que el router no lo modifica y la aplicación no funciona correctamente.

DESARROLLO DL PROYECTO

En este proyecto se implementar una VPN IPSec de acceso remoto que se conectara a través de internet, también contaremos con un soporte para realizar llamadas VoIP, para eso utilizaremos CCM que será configurada en un extremo de la VPN, donde tenemos el router A, el cual será el encargado de dar soporte de VoIP a travez de la VPN. También implementaremos NAT lo que permitirá a los equipos que se encuentren en la VPN conectarse al internet por medio de PAT y no podrán accesar equipos que no pertenezcan a las misma VPN, el router B solo cuenta con la configuración necesaria para tener salida al internet ya que es lo único que necesita para poder conectarse remotamente a la VPN, nuestro router A cuenta con la configuración DHCP para poder darles una ip a los equipos que se quieran conectar a la VPN.

En nuestra configuración utilizaremos el Cisco IP Communicator para simular los teléfonos IP dentro de nuestro equipo.

La configuración completa se encuentra en los entregables A y B. En el entregable A se encuentra la configuración del router A, el cual contiene la implementación del servicio telefónico, así como la implementación de la VPN IPSec de Acceso Remoto, el entregable B, muestra la configuración del router B, la cual nada mas cuenta con la salida de pc al internet. También como entregable se encuentran las capturas de trafico mientas se realiza la llamada, capturadas con wireshark.

También utilizaremos OracleVM VirtualBox para poder simular dos sistemas operativos Windows XP para poder instalar IP Communicator en cada uno de ellos y asi poder hacer llamadas entre sí.

A continuación, se muestra el diagrama que representa la implementación que se realizó.

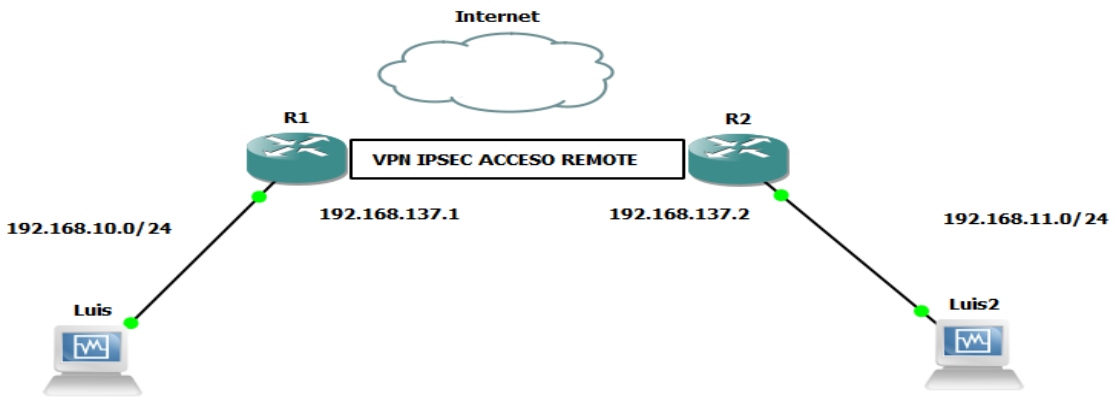

Figura 15: Arquitectura del proyecto.

Hardware

- HP Pavilion x360
    - Procesar Intel Core i5-6200U CPU 2.30GHz 2.40GHz
- Memoria RAM 8.00 GB

Software

- Cisco IOS c7200-advipservicesk9-mz.124-4.T1
- CiscoVPN
- Wireshark-win32-1.10.5
- GNS3-2.0.3
- Windows 10
- Cisco IP Communicator
- OracleVM VirtualBox

.

Cisco IP Commnicatar

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

- No requieres software de proveedores de servicio de telefonía, TSP.
- Soporte para los codecs G.711, G.729a, SCCP, iSAC, G.722, G.729a, G.729ab.
- Soporta SCCP y SIP.
- Cinco teclas programables.
- Ocho botones de marcación dial.
- Compatibilidad de XML.

Figura 16: . Cisco IP Communicator

Router Cisco c7200

El Router Cisco c7200 Proporciona los siguientes soportes.

- Alto rendimiento para servicios concurrentes como voy y seguridad.
- Mejora la ranura de Red.
- Seguridad:
  - Cifrado on-board..
  - Soporte de hasta 1500 túneles VPN.
  - Soporte de antivirus a través de NAC.
  - Prevención de instrucciones.
- Voz:
  - Soporte de llamadas analógicas y digitales.
  - Soporte para buzón de voz.
  - Soprte opcional para CCME, para el procesamiento de llamadas locales para un máximo de 36 telefonos IP.
  - Soporte opcional para SRST.

Cisco IOS c7200-advipservicesk9-mz.124-4.T1

Este ios de cisco cuenta con las siguientes caracteristicas:

- K9: Contiene el protocolo de encriptación de 3DES.
- Mz: la versión de IOS corre sobre RAM y se encuentra comprimida.
- 124-15.T1: es una versión de IOS 124 y es una imagen de tipo T versión 1.

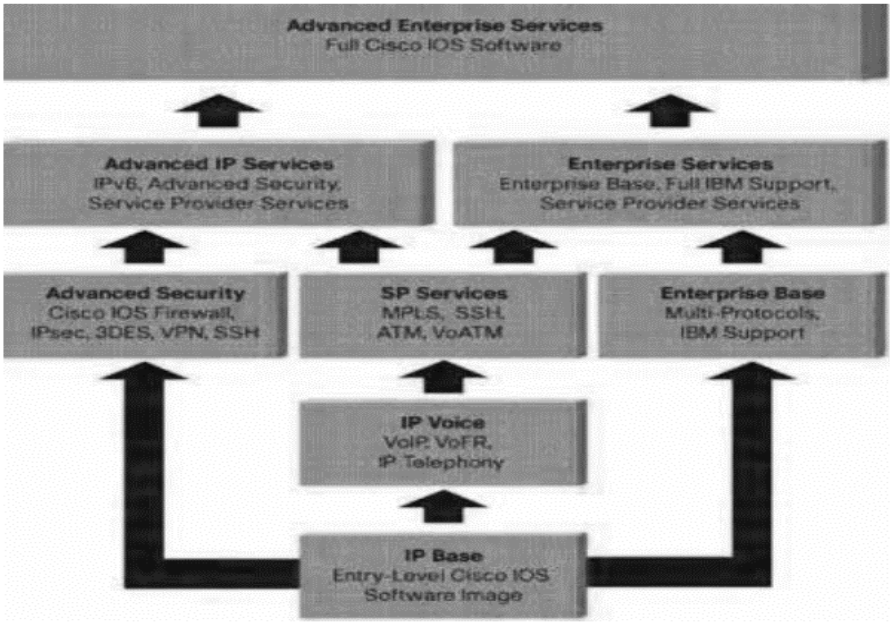

Figura 17: IOS Cisco

VPN de acceso remoto basada en IPSec

I. Crear un pool de direcciones

Se crea un pool de direcciones que permite 10 conexiones concurrentes

r1(config)# ip local pool vpn-pool 192.168.10.20 192.168.10.25

II. Configurar la autenticación

Activa la funcionalidad aaa (Authentication, Authorization y Accounting)

r1(config)# aaa new-model

Defina la lista de métodos de autenticación cuando un usuario hace login (local)

r1(config)# aaa authentication login USERS local

Establece los parámetros que restringen el acceso de los usarios a la red

r1(config)# aaa authorization network AUTH-LIST local

Se crea una cuenta de usuario que usarán los clientes VPN para autenticarse contra el servidor

r1(config)# username admin01 password admin01

III. Configurar las políticas IKE

Habilitamos IPSEC

r1(config)# crypto isakmp enable

Crear una nueva política IKE. Cada política se identifica por su número de prioridad (de 1 a 10.000; 1 la más prioridad más alta)

r1(config)# crypto isakmp policy 10

Especificar el algoritmo de cifrado a utilizar

r1(config-isakmp)# encryption 3des

Elegir el algoritmo de hash a usar: Message Digest 5 (MD5 [md5]) o Secure Hash Algorithm (SHA [sha]).

r1(config-isakmp)# hash md5

Determinar el método de autenticación: pre-shared keys (pre-share), RSA1 encrypted nonces (rsa-encr), o RSA signatures (rsa-slg).

r1(config-isakmp)# authentication pre-share

Especificar el identificador de grupo Diffie-Hellman

r1(config-isakmp)# group 2

Crea un grupo IKE para los clientes VPN

r1(config)# crypto isakmp client configuration group Cisco

Establece cisco123 como key para el grupo Cisco

r1(config-isakmp-group)# key cisco123

Se selecciona el pool de direcciones para los clientes

r1(config-isakmp-group)# pool vpn.pool

Elegimos el máximo de usuarios

r1(config-isakmp-group)# max-users 5

IV. Configurar la política IPSec

Establece las políticas de seguridad IPSEC que se usarán en las comunicaciones

r1(config)# crypto ipsec transform-set set1 esp-3des esp-md5-hmac

Crea un crypto map dinámico que se usa cuando la IP del host remoto no se conoce, como es el caso en las VPN de acceso remoto

r1(config)# crypto dynamic-map map1 10

Asocia el transform set set1 al crypto map dinámico

r1(config-crypto-map)# set transform- set set1

Activa Reverse Route Injection (RRI)

r1(config-crypto-map)# reverse-route

Configura un crypto map estático que puede ser asociado a una interfaz

r1(config)# crypto map map1 client configuration address respond

Define el conjunto de usuarios con permisos de autenticación

r1(config)# crypto map map1 client authentication list USER

Establece el grupo de usuarios y los parámetros de acceso a la red

r1(config)# crypto map map1 isakmp authorization list AUTH-LIST

Asocia el crypto map dinámico creado para los clientes de acceso remoto

r1(config)# crypto map map1 10 ipsec-isakmp dynamic map1

Accedemos a la configuración de la interfaz por la que se conectarán los clientes VPN

r1(config)# interface f0/0

Asociamos el crypto map a la interfaz

r1(config-if)# crypto map map1

Servicio de telefonia

Habilite las funcionalidades de CME en el router R1.

R1(config)# telephony-service

Debido a que solo se tienen 2 host corriendo CIPC, configure el número máximo de teléfonos a 2. Luego configure el número máximo de números de directorio a 10.

R1(config-telephony)# max-ephones 2

R1(config-telephony)# max-dn 10

Configure un mensaje del sistema, el cual aparecerá en todos los teléfonos asociados con el CME.

R1(config-telephony)# system message CCNA Voice Luis Muñoz

Tiempo de espera para la llamada 10 segundos

R1(config-telephony)# timeouts ringing 10

Formato del dia

R1(config-telephony)# date-format dd-mm-yy

Configure la dirección origen (source address) para SCCP. Para ello utilice la dirección IP de la interface FastEthernet del router con número de puerto 2000.

R1(config-telephony)# ip source-address 192.168.10.1 port 2000

Configuración de Teléfonos

En R1 ingrese al modo de configuración del ephone 1 (Host A).

R1(config)# ephone 1

Asocie al ephone 1 su correspondiente dirección MAC.

R1(config-ephone)# mac-address 0800.2707.0420

Configure el tipo de teléfono a ser utilizado. En este caso se simulan los teléfonos Ethernet utilizando Cisco IP Communicator (CIPC).

R1(config-ephone)# type cipc

Asigne al primer botón del teléfono el número de directorio 1 utilizando el comando button line. Este comando asigna las líneas telefónicas

R1(config-ephone)# button 1:1

En R1 ingrese al modo de configuración del ephone 2(Host A).

R1(config)# ephone 1

R1(config-ephone)# mac-address 0800.27F0.B705

R1(config-ephone)# type cipc

R1(config-ephone)# button 1:2

Configuramos Pat en el Router 1

Configuramos la dirección IP para la interface de salida

Interface fastEthernet 0/1

ip addres 192.168.137.1 255.255.255.0

Habilitamos la interface

no shutdown

Declaramos la interfas de salida de NAT

ip nat outside

Configuramos la dirección IP para la interface de entrada

Interface fastEthernet 0/0

ip addres 192.168.10.1 255.255.255.0

Habilitamos la interface

no shutdown

Declaramos la interfas de entrada de NAT

ip nat inside

Creamos una ruta estática y la direccionamos a la interface de salida

Ip route 0.0.0.0 0.0.0.0 192.168.137.2

Creamos una lista de con la red a la cual vamos aplicar NAT

access-list 10 permit any

Ligamos la lista de acceso con la interface de salida

ip nat inside source list 10 interface fastEthernet 0/1 overload

Resultado de los Análisis

Despues de la implementación del proyecto terminal obtuvimos los siguientes resultados:

```
R1#show crypto ipsec sa

interface: FastEthernet0/1
    Crypto map tag: map1, local addr 192.168.137.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.10.21/255.255.255.255/0/0)
   current_peer 192.168.137.2 port 1038
     PERMIT, flags={}
    #pkts encaps: 73, #pkts encrypt: 73, #pkts digest: 73
    #pkts decaps: 106, #pkts decrypt: 106, #pkts verify: 106
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 2

     local crypto endpt.: 192.168.137.1, remote crypto endpt.: 192.168.137.2
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x64CE96AC(1691260588)

     inbound esp sas:
      spi: 0xCD65BB52(3445996370)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel UDP-Encaps, }
        conn id: 3, flow_id: SW:3, crypto map: map1
        sa timing: remaining key lifetime (k/sec): (4530890/3215)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

Figura 18: Show crypto ipsec sa Router A

Aplicando el comando Show crypto ipsec sa en el router A como se muestra en la figura 18 se muestran los paquetes que fueron encriptados y desencriptados por el router A. tenemos que tomar en cuenta que el número de paquetes en nuestro caso depende de la duración de la llamada. En la imagen podemos verificar los paquetes que son encriptados y desencriptados son diferentes debido a que el router encripta los paquetes que van de salida y desemcripta los paquetes que van entrando. Tomando en cuenta los resultados podemos decir que desencripta mas paquetes que los que reside.

Analizaremos los campos más importantes del comando Show crypto ipsec sa.

Primero se muestra la interface de salida que se encarga de encriptar y desencriptar los paquetes.

Interface: FastEthernet0/1

Podemos observar que el map crypto que fue utilizado en esta interface es el mapa map1 con la dirección IP 192.168.137.1

Crypto map tag: map1, local addr 192.168.137.1

Podemos apreciar que en el segmento de red local no tiene dirección ya que estamos utilizando acceso remoto

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)

Ahora podemos ver que la dirección que le corresponde a la computadora que entra mediante el acceso remoto

remote ident (addr/mask/prot/port): (192.168.10.21/255.255.255.0/0/0)

Aquí se identifica la dirección IP de donde viene la ip de acceso remoto y realiza la conexión por el puerto

current_peer 192.168.137.2 port 1038

PERMIT, flags={origin_is_acl,}

Se muestra el numero de paquetes que son encapsulados, encriptados y aceptados para poder viajar en la VPN.

#pkts encaps: 73, #pkts encrypt: 73, #pkts digest: 73,

Se muestra el numero de paquetes que son desencapsulados, desencriptados y verificados para que puedan accesar a nuestra VPN

#pkts decaps: 106, #pkts decrypt: 106, #pkts verify: 106,

#pkts compressed: 0, #pkts decompressed: 0

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

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

Utilizando el comando Show crypto ipsec sa podemos comprobar que hemos creado en VPN de acceso remoto que esta recibiendo y enviando paquetes en ella.

Ahora comprobaremos el tráfico de Voz para ello utilizaremos el software wireshark, esta herramienta tiene como objetivo principal el de capturar el tráfico que hay en una interfaz de red en una computadora.

De acuerdo con el proyecto analizaremos el tráfico que hay cuando realizamos una llamada con Cisco IP Communicator que se encuentra instalados en nuestras máquinas virtuales.

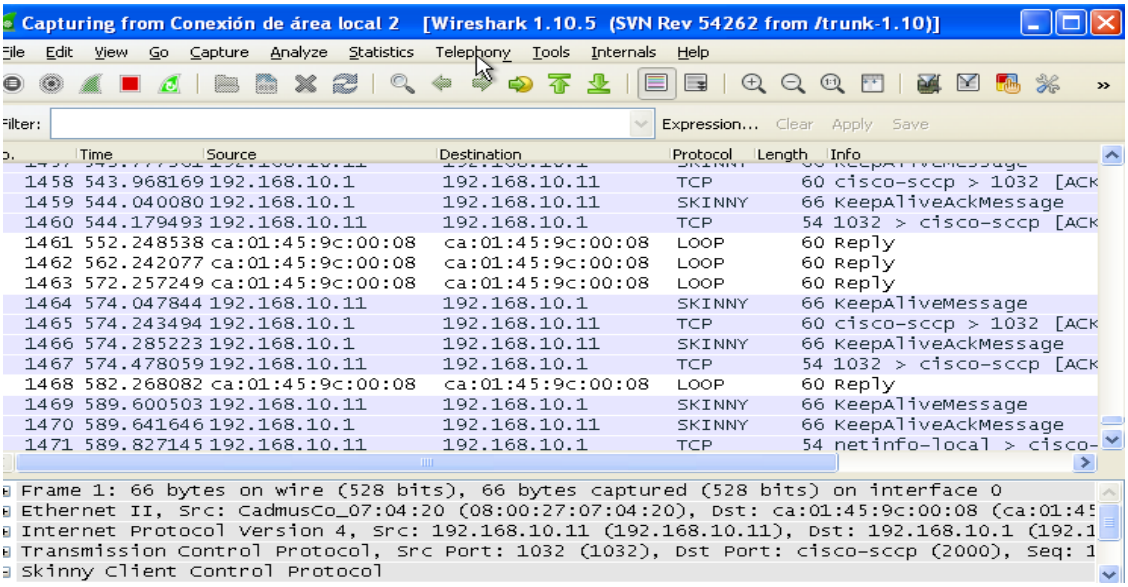

Figura 19: Trafico que de la PC1(Se encuentra en el segmento de red)

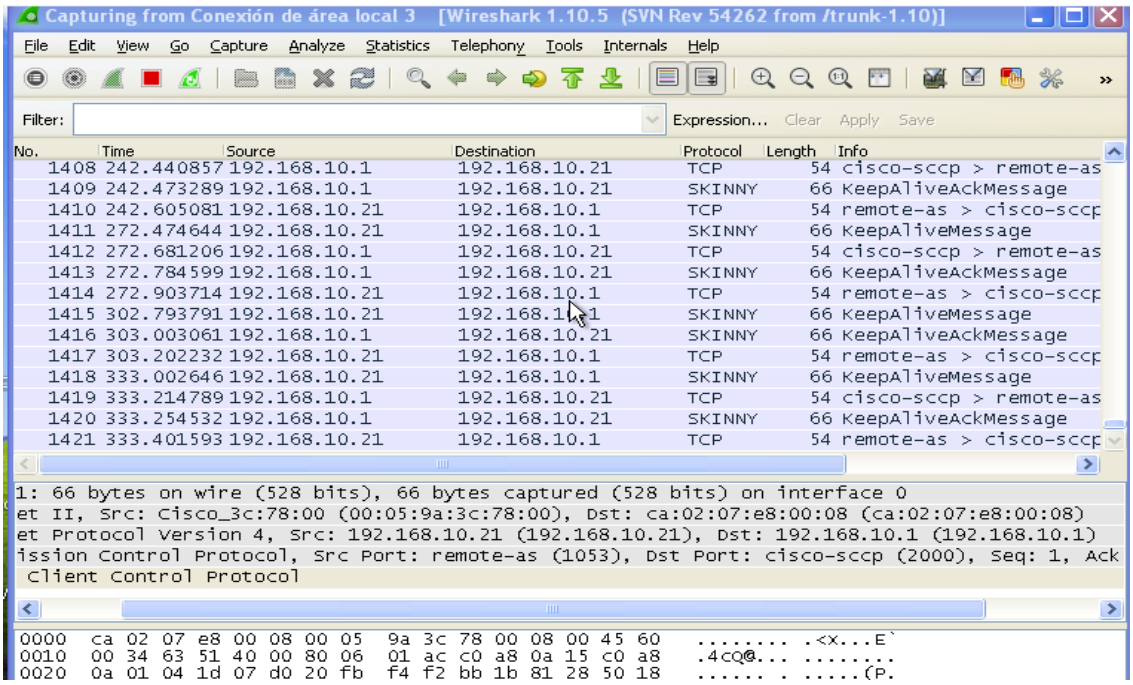

Figura 20: Trafico que de la PC2 (Conectada mediante acceso remoto)

En la figura 16 y en la figura 17, podemos observar la IP de cada computadora en el caso de la PC1 es 192.168.10.11 y el destino que es gatekeeper un nuestro caso es 192.168.10.1 que es el mismo para las dos computadoras, en el caso de la PC2 es la ip que le asigna La VPN de acceso remoto la cual es 192.168.10.21 y el destino es el mismo gatekeeper 192.168.10.1 y se comunican entre si utilizando el protocolo SKINNY, con esto se establece una conexión y forman el canal RTP que es por donde viaja las Voz.

Analisaremos a detalle cómo funciona el protocolo SKINNY.

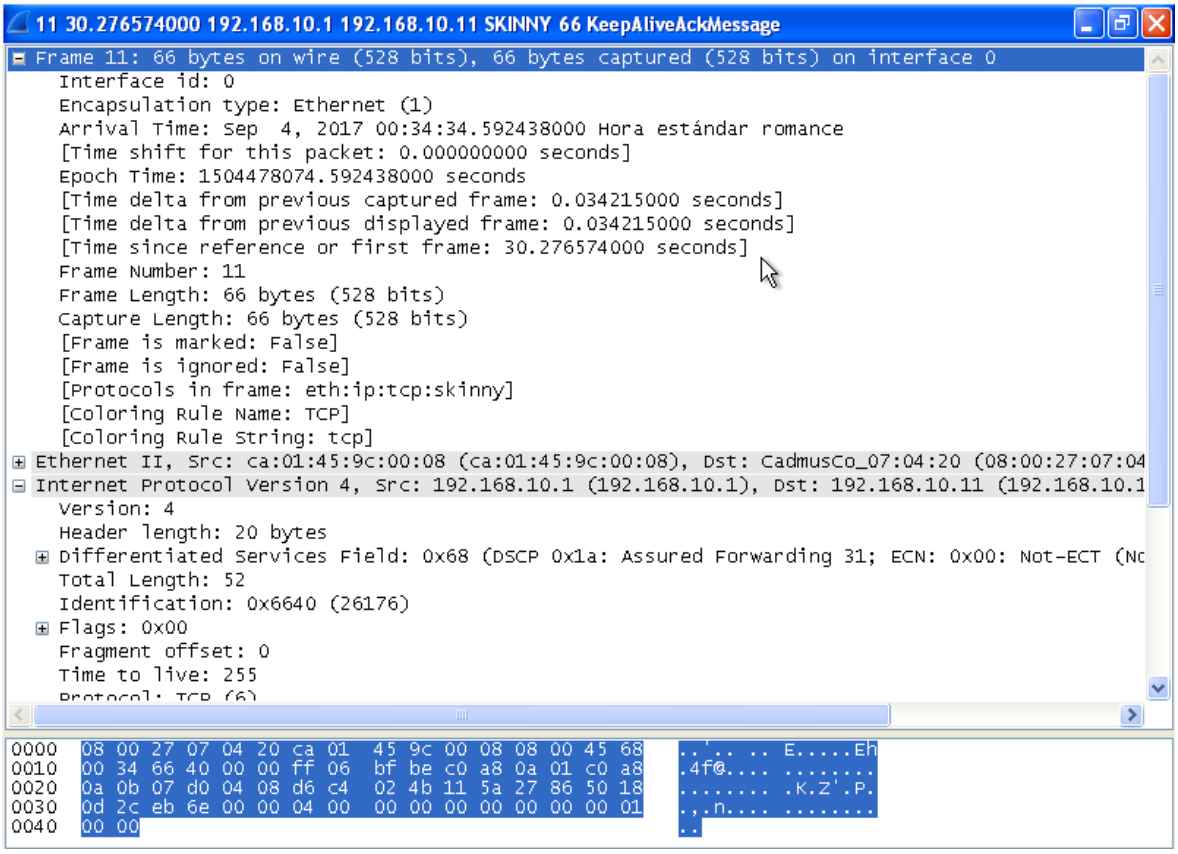

Figura 21: Paquete SKINNY detallado

Dando doble clik en cualquier renglón que contenga SKIMMY se mostraran los detallen que contiene. En la figura se puede observar los puertos que utiliza en nuestro caso es el puerto 2000, el protocolo que se utiliza, la dirección IP de destino (192.168.10.11), la dirección IP de origen (192.168.10.1), entre otras cosas como se muestra en la figura 18.

Para ver todas las señalizasiones de llamada seleccionamos en el menú Thelepony, luego damos clic en VoIP Call. Aquí se mostraran todas las llamadas que fueron realizadas durante la captura de tráfico.

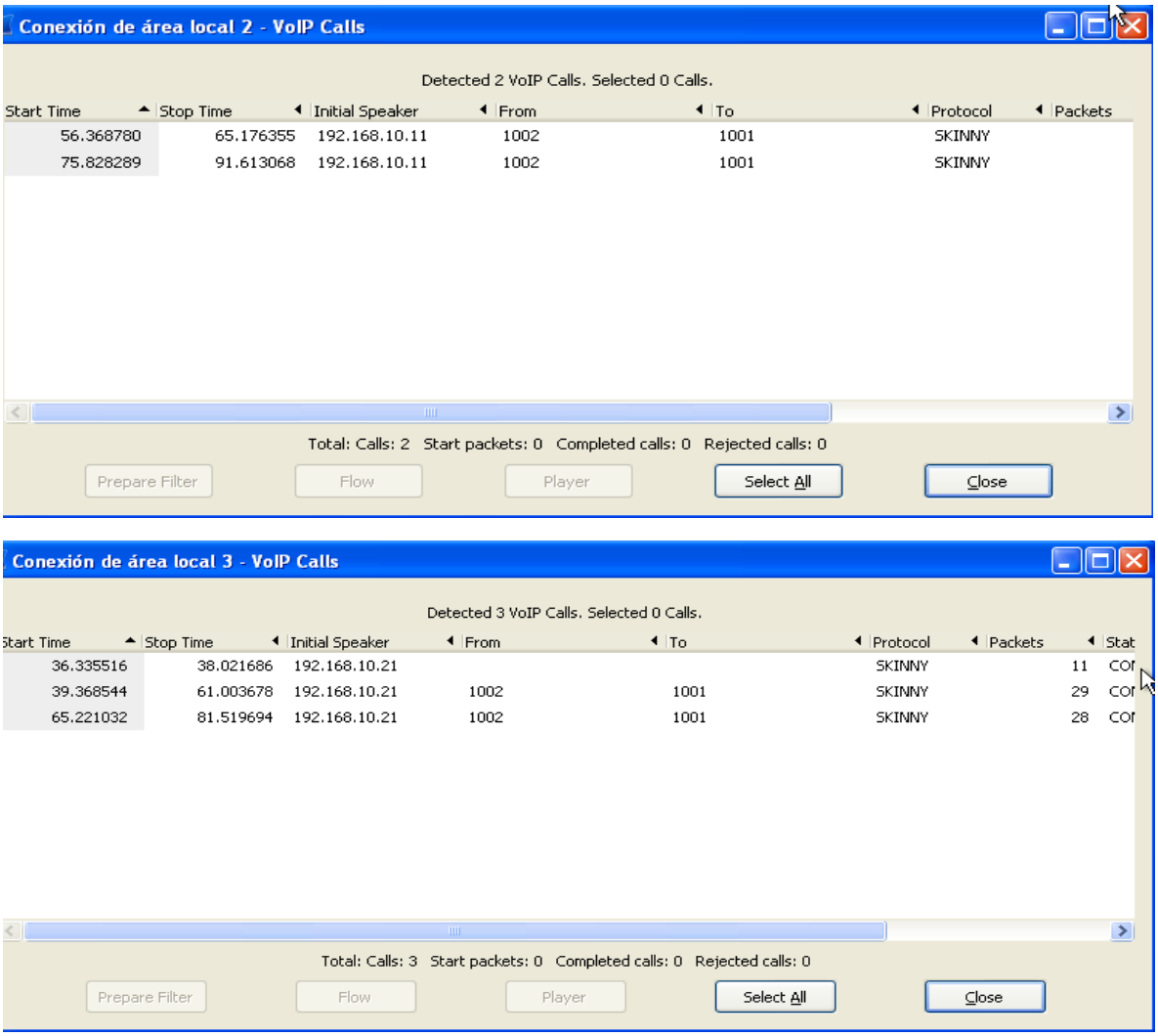

Figura 22: Detalles de las llamadas.

La figura 19 nos muestra el tiempo de inicio y fin de las llamadas, la dirección IP de la cual inician las llamadas, el identificador de quien inicia y recibe la llamada, el protocolo utilizado, el numero de paquetes de la señalización de la llamada y el estado de la llamada.

Para poder ver todas las señalizaciones de las llamadas, elegimos la llamada y damos clic en flow.

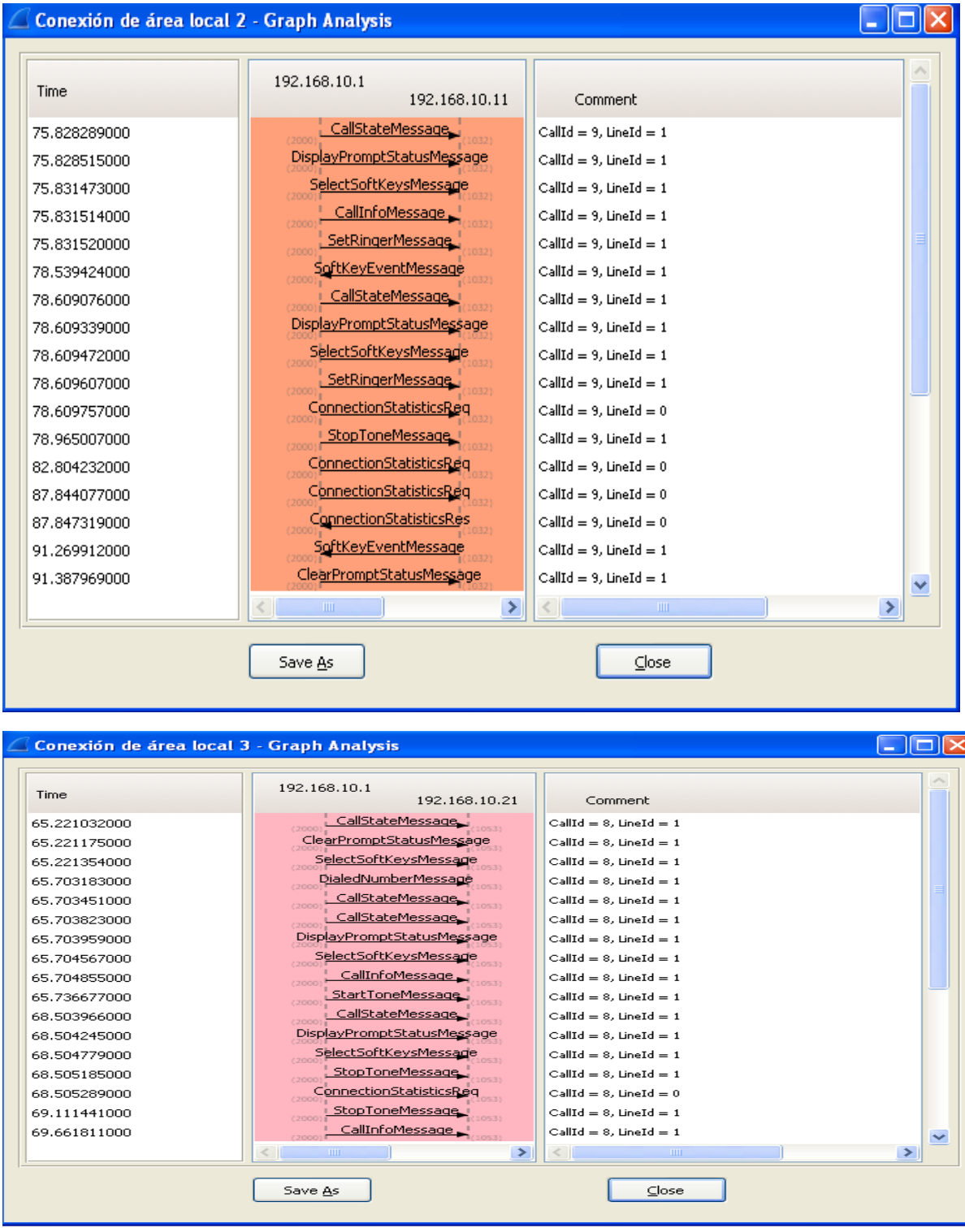

Figura 23: Señalización de las llamadas

La señalización de la llamada se da entre el Gatekeeper y ambos extremos de la llamada.

Ahora vamos analizar el flujo RTP seleccionamos un paquete RTP y vemos los detalles.

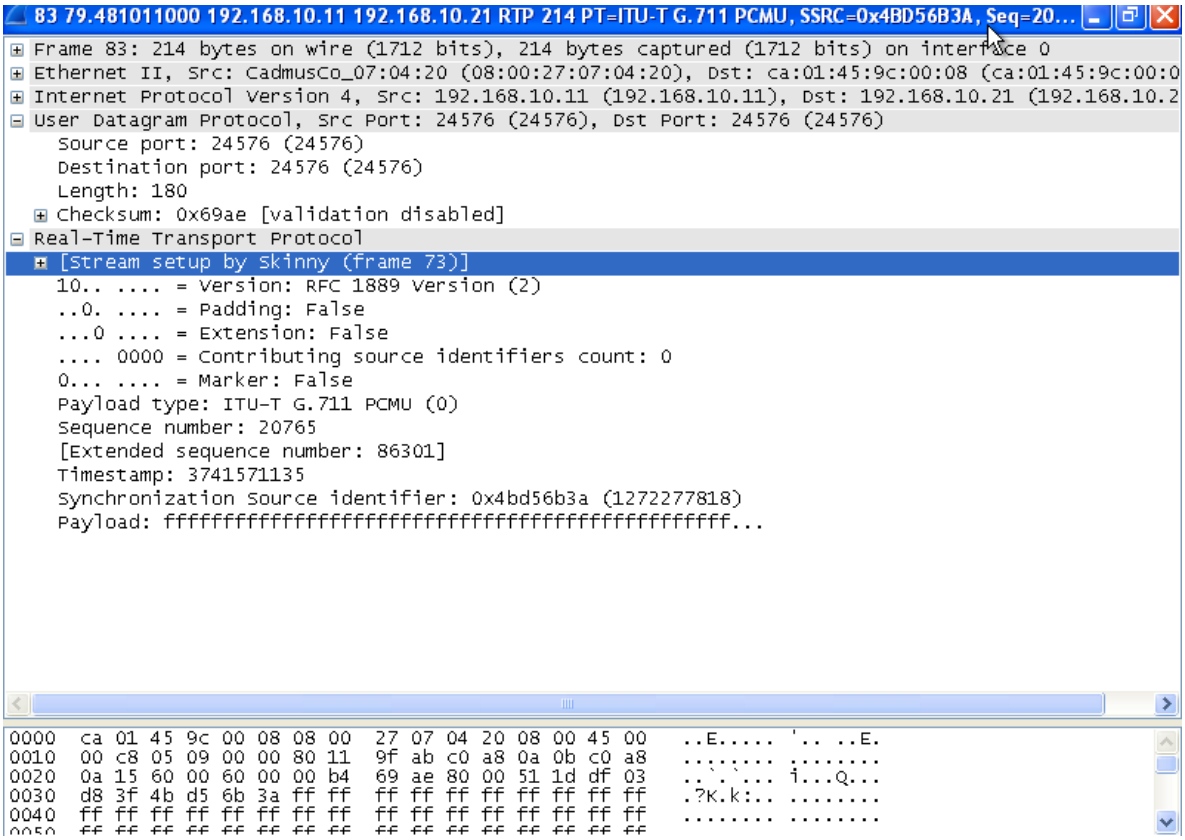

Figura 24: Detalles paquete RTP

Se puede observar que el flujo RTP fue establesido por el protocolo SKINNY, que viaja por UDP y la dirección IP del origen y destino.

Tambien podemos observar el tip que es ITU-T G.711 PCMU, podemos decir que usa el códec de audio G.711 estandarizado por ITU.

Para poder ver el flujo RTP seleccionamos en el menú Telephony, luego en RTP y en Show All Stream. Aquí nos mostrara una ventana con los flujos de RTPque se establecieron mientras se capturaba el tráfico.

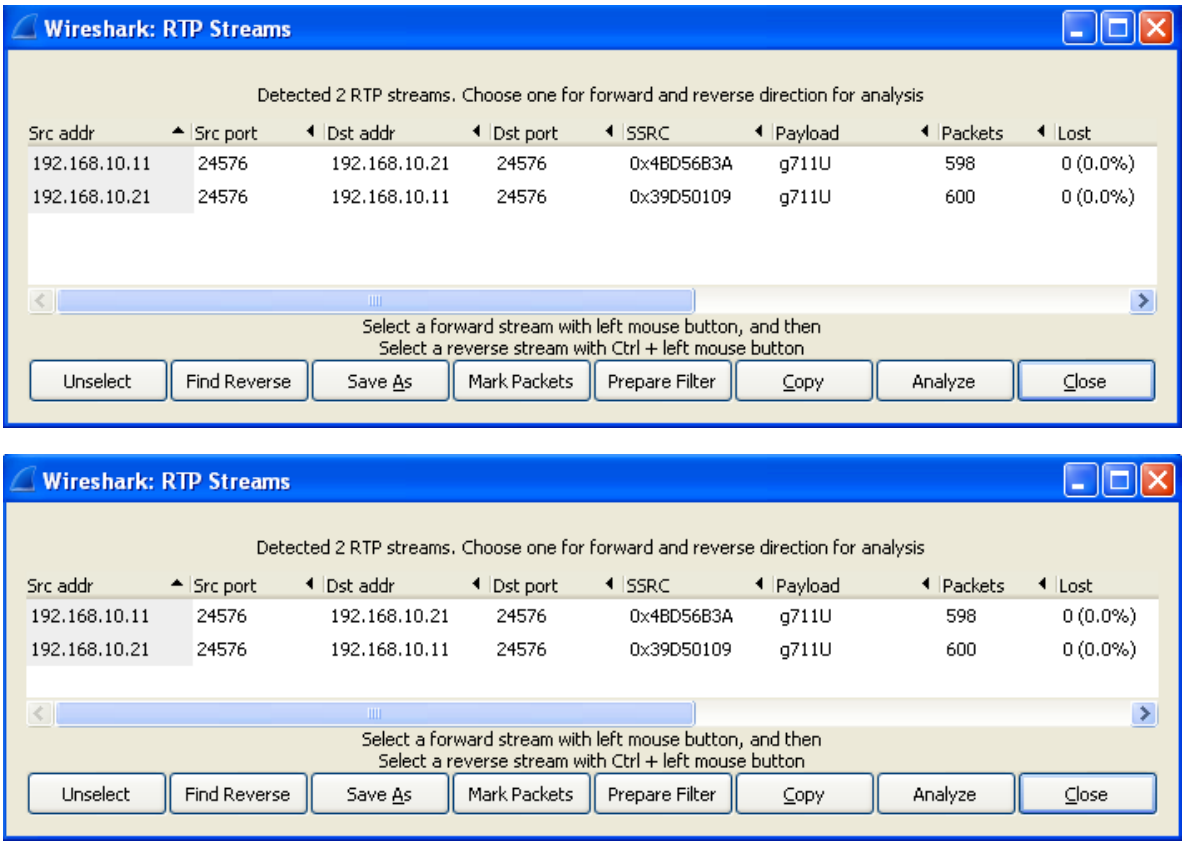

Figura 25: Flujo RTP

Ya seleccionados los flujos de entrada y salidadamos clic en el botón de Analyze, aquí se mostrara el analizis de los flujos RTP.

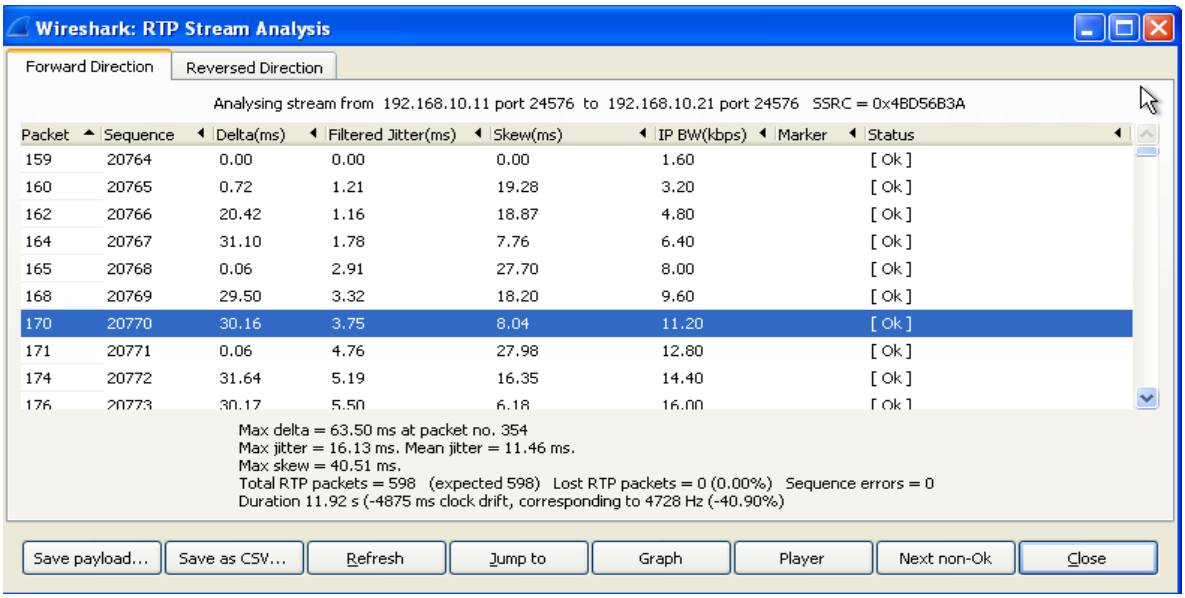

Figura 26: Análisis del flujo RTP

Para ver el audio de cada llamada se oprime el botón Player donde se mostrara la interfaz para poder reproducir la llamada.

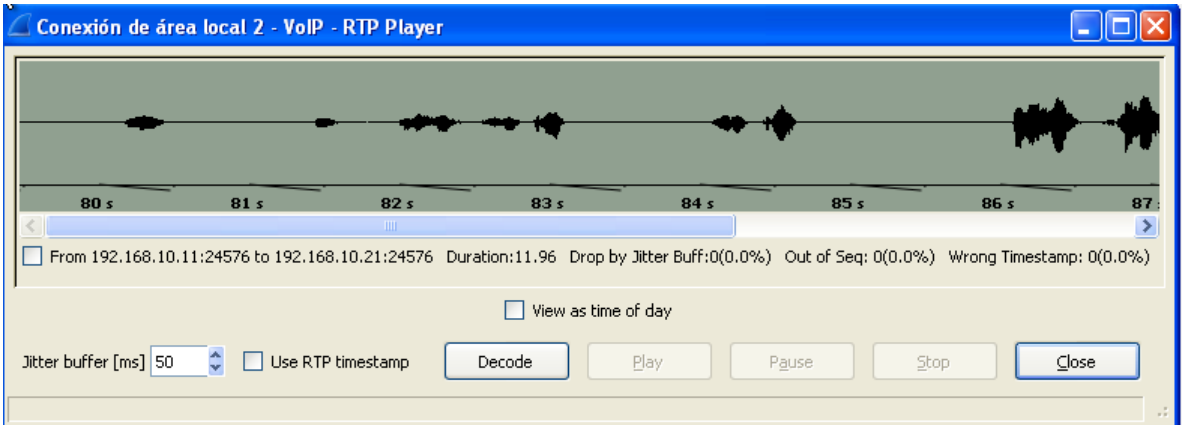

Figura 27. Reproducción del audio

Conclusiones

Tras la implementación del proyecto podemos concluir que las redes virtuales (VPN) son una excelente tecnología para el acceso remoto, ya que las VPN son un sustituto indispensable a los métodos tradicionales que son muy costosos. Tambien podemos decir que mientras mas grande sea una VPN el ahorro económico será mayor.

Con la realización de Una VPN de Acceso remoto comprobamos que es ideal para cualquier persona que viaja, que quiera conectarse desde su casa o cualquier lugar que tenga internet, esta facilidad la ocupan las empresas para que se aumente la productividad de los empleados ya que puedes accedes desde cualquier lugar.

Con respecto a la seguridad pudimos conocer como trabaja el protocolo IPSec que es el encargado de brindar la seguridad que hay en la VPN de Acceso remoto, este protocolo nos permite la confidencialidad de la llamada, debido a la encriptación que tiene, otro benéfico que tiene es que las llamadas no pueden ser interceptadas ni decodificadas.

Definitivamente las VPN seguirán siendo motivo de investigación, muchos estaremos utilizando esta tecnología sin saberlo y el aporte que demos todos los profesionales involucrados en las redes de información serán fundamentales.

Bibliografia

- Tecnologia VoIP y Telefonia IP, Jose Manuel Hudrobo Moya y David Roldan Martinez, Primera Edicion: Alfaomega Grupo Editor, Mexico, junio 2006
- Redes Privadas Vituales con Linux , Oleg Kolesnikov, Primera Edicion, Editorial Prendice Hall, Año 2003.
- Security in Computing, Pfeeger P. Charles, Second Edition: Prentice Hall PTR, año 1997
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/s1/sec-s1-cr-book/sec-cr-s3.html#wp3458936948
- https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cipc/7_0/localization/ipcugesp.pdf

- http://www.udb.edu.sv/udb/archivo/guia/electronica-ingenieria/fundamentos-de-voz-sobre-ip-y-calidad-de-servicio/2015/i/guia7.pdf
- https://www.cisco.com/c/es_mx/support/docs/wireless-mobility/wlan-security/81837-vpnclient-wlan-wlc-conf.html
- https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html

Entregable A

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa authentication login USER local
aaa authorization network AUTH-LIST local
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.10.1 192.168.10.10
!
ip dhcp pool lan
   network 192.168.10.0 255.255.255.0
   default-router 192.168.10.1
!
!
no ip domain lookup
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
username admin01 password 0 admin01
!
!
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
!
crypto isakmp client configuration group cisco
 key cisco123
 pool vpn-pool
!
!
crypto ipsec transform-set set1 esp-3des esp-md5-hmac
!
crypto dynamic-map map1 10
 set transform-set set1
 reverse-route
!
!
crypto map map1 client authentication list USER
crypto map map1 isakmp authorization list AUTH-LIST
crypto map map1 client configuration address respond
crypto map map1 10 ipsec-isakmp dynamic map1
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
```

```
interface FastEthernet0/1
 ip address 192.168.137.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
 crypto map map1
!
ip local pool vpn-pool 192.168.10.20 192.168.10.25
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.137.2
no ip http server
no ip http secure-server
!
!
ip nat inside source list 10 interface FastEthernet0/1 overload
!
logging alarm informational
access-list 10 deny   any
access-list 10 permit any
access-list 11 permit any
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
telephony-service
 max-ephones 5
 max-dn 10
 ip source-address 192.168.10.1 port 2000 strict-match
 timeouts ringing 10
 system message CCNA VOICE Luis Mu_oz
 user-locale ES
 network-locale ES
 date-format dd-mm-yy
 max-conferences 4 gain -6
!
!
ephone-dn  1  dual-line
 number 1001 secondary 22501001
 label Luis M.(1001)
```

```
 description Luis Mu_oz
 name Luis Mu_oz
!
!
ephone-dn  2  dual-line
 number 1002 secondary 22501002
 label Aurora S(1002)
 description Aurora Salgado
 name Aurora Salgado
!
!
ephone  1
 mac-address 0800.2707.0420
 type CIPC
 button  1:1
!
!
!
ephone  2
 mac-address 0800.27F0.B705
 type CIPC
 button  1:2
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
!
!
end
```

Entregable B

```
!

!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
```

```
hostname R2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
!
resource policy
!
ip subnet-zero
no ip icmp rate-limit unreachable
ip cef
ip tcp synwait-time 5
!
!
!
!
no ip domain lookup
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.11.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.137.2 255.255.255.0
 ip nat outside
 ip virtual-reassembly
```

```
 duplex auto
 speed auto
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.138.137.1
no ip http server
no ip http secure-server
!
!
ip nat inside source list 11 interface FastEthernet0/1 overload
!
logging alarm informational
access-list 11 permit any
no cdp log mismatch duplex
!
!
!
!
control-plane
!
!
!
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```