UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE INGENIERÍA DE SISTEMAS

"CONSIDERACIONES DE SEGURIDAD PARA SISTEMAS DE VOZ SOBRE IP (VoIP)"

Monografía previa a la obtención del título de:

INGENIERO DE SISTEMAS

Autores:

JUAN CARLOS AZUERO PARRA
XAVIER ANIBAL CASTILLO ORDOÑEZ

Director:

ING. BOLIVAR MENDEZ RENGEL

CUENCA, ECUADOR

2006

DEDICATORIA

Dedico el presente trabajo de graduación a mis padres Julio y Narcisa por todo el apoyo brindado a lo largo de mis estudios. De igual forma a mis hermanos Diego Fernando y Lorena por ser un gran aporte en los tiempos más difíciles. A Lorena Tamayo por estar siempre dispuesta a escucharme y apoyarme con sus consejos. A mis sobrinos Mateo y Camila por ser mi inspiración para culminar mis estudios universitarios. A mis abuelitas, tíos y primos por confiar en mí y brindarme sus consejos y apoyo. Una dedicatoria especial a mi abuelito Miguel que estoy seguro que desde el cielo me cuida, a El que hubiese querido verme cumplir con esta meta. Dedico este trabajo también a mis compañeros que nos apoyamos durante nuestro viaje a Argentina; de manera especial dedico este trabajo a Mishell Zamora por estar a mi lado, por su comprensión y por darme fuerzas en mis horas de estudio.

Juan Carlos Azuero P.

DEDICATORIA

Dedico el presente documento a mi padre Mario Castillo, a mi abuelita Dolores Jaramillo, a mis primos Amaro y Mariana Castillo quienes hubieran querido estar aquí y compartir conmigo este logro, y que estoy seguro que desde donde se encuentren me están apoyando y esperando que sea un gran hombre de bien.

Xavier A. Castillo Ordóñez

AGRADECIMIENTOS

Con mucha satisfacción deseo hacer público mi agradecimiento a Dios a mis padres, hermanos y demás familiares por confiar en mi persona y por brindarme su apoyo siempre. A mis profesores un agradecimiento especial por dedicarnos su tiempo en pos de nuestra superación. Agradezco de igual forma a nuestro Director del presente trabajo de graduación Ingeniero Bolívar Méndez por su tiempo y dedicación para que el siguiente haya sido desarrollado de muy buena manera. Agradezco a Xavier Castillo, por su dedicación en el desarrollo de nuestra monografía, le deseo éxitos en su vida profesional. Deseo hacer extensivo este agradecimiento a mis compañeros Maria Fernanda Marín y Fernando Zea con quienes compartimos muchas experiencias en la capital Argentina, gracias por su paciencia al frente de el reto que nos tocó vivir. Un agradecimiento especial a Mishell Zamora por ser una gran persona y estar allí cuando la necesito, gracias por estar a mi lado. A los amigos de la Universidad del Azuay, autoridades y administrativos por su eficiente labor en el transcurso del tiempo de mi vida universitaria. A todas las personas que siempre me brindaron su apoyo muchas gracias.

Juan Carlos Azuero P.

AGRADECIMIENTOS

Agradezco especialmente a mi madre Cecilia por creer siempre en mi y apoyarme en todo lo que hacia, a los padres de Juan Carlos por haberme soportado tantas noches en su casa, a mi querida amiga y psicóloga Karla Arias por apoyarme cuando más lo necesitaba, a Jessica Cambi quien me ayudó a estudiar muchas veces para que pudiera estar haciendo hoy esta monografía, a Vinicio Bermeo quien nos facilitó unos equipos para realizar esta monografía, a mi mejor amigo y compañero en este trabajo Juan Carlos Azuero que fue el gran pilar de este trabajo y espero que no sea el ultimo proyecto en el que trabajemos juntos le deseo muchos éxitos en toda su carrera, a mis amigos de siempre Esteban Morales, Fernando Zea, y María Marín, en quienes siempre me apoyé, a los consejos desinteresados de Patricio Murillo, a mi tío el "gordo" quien siempre me quiso ayudar, aunque muchas veces yo no lo dejaba, a todos mis amigos y profesores que de una u otra forma aportaron en mi formación, y por último a Dios quien estuvo detrás de todos ellos y espero que los acompañe siempre a lo largo de sus vidas.

Xavier A Castillo Ordóñez

"Si algún mérito tiene esta obra a ellos se debe; en cuanto a los errores yo soy el único responsable"

S. K.

Índice de Contenidos

Índice de Ilustraciones y Cuadros

ANEXOS

RESUMEN GENERAL
"CONSIDERACIONES DE SEGURIDAD EN SISTEMAS DE VOZ SOBRE IP (VoIP)"

El presente trabajo de graduación, trata sobre los riesgos, ataques y vulnerabilidades que presenta el sistema de Voz sobre IP (VoIP), dentro de sus protocolos mas importantes como son H.323 y SIP en lo a que su implementación se refiere, además de brindar un sin numero de precauciones para evitar ataques a nuestra red VoIP, manteniendo la calidad de servicio (QoS) semejante a la red de telefonía convencional.

A más de las seguridades propias de una red normal, este trabajo se dan las consideraciones de seguridad y protección para el uso de equipos como Gateway, servidores Proxy, Firewall, etc., así como su configuración básica para VoIP.

De igual forma, en esta monografía se da a conocer de manera breve, las nuevas formas de protección en cuanto a protocolos se refiere como es el caso del Media Gateway Control Protocol, MEGACO e Ipsec.

En resumen el trabajo realiza una investigación de los ataques mas comunes a una red VoIP, sus debilidades y como contrarrestarlas para hacer de VoIP un sistema confiable y seguro.

ABSTRACT

GENERAL RESUME

“SECURITY CONSIDERATIONS IN VOICE OVER IP SYSTEMS (VoIP)”

The present graduation thesis is over the attacks, risks and vulnerabilities that the voice over IP system presents (VoIP), within the most important protocols, like H.323 and SIP, in to what its implementation refers, and gives a great amount of precautions to avoid attacks to our VoIP network, maintaining the quality of service, alike those of the conventional telephonic network.

Besides, the normal network security, this resume gives the security considerations and protections for the usage of the equipment: As Gateways, PROXY servers, firewalls etc.., as its basic configuration for VoIP.

Therefore, this monograph gives, in a brief manner, the new methods of protection, in to what protocols refer, as in the case of Media Gateway Control Protocol, MEGACO and IPsec.

In conclusion, this thesis makes an investigation of the most common attacks to a VoIP network, its weaknesses and how to counter attack them, to make VoIP a reliable and secure system.

INTRODUCCIÓN

La tecnología de voz sobre el Internet o VoIP por el acrónimo de *Voice over Internet Protocol,* es una forma nueva de hacer y recibir llamadas telefónicas utilizando una conexión de Internet de banda ancha en lugar de una línea telefónica corriente. VoIP convierte la llamada en una señal digital que viaja a través del Internet hasta llegar al teléfono de la persona que se está llamando.

La tecnología de redes de paquetes representa una revolución en las telecomunicaciones. Utilizando un protocolo como IP, se pueden unir servicios de comunicaciones de voz, datos y video a través de una sola red. La promesa de reducción en los gastos de operación y un aumento en los ingresos debido a servicios nuevos e integrados ha provocado que todos los proveedores de telecomunicaciones consideren a VoIP como una nueva alternativa.

Desafortunadamente, las nuevas tecnologías traen también consigo detalles a tener en cuenta respecto a la seguridad. De pronto, se presenta la necesidad de tener que proteger dos infraestructuras diferentes: voz y datos. Como cualquier nueva tecnología que se desarrolla el riesgo y la amenaza para empresas que despliegan telefonía IP son muy reales, y aunque pocos incidentes han sido informados en público, éstos son esperados para aumentar en número como el aumento del desarrollo de esta tecnología. A menos que medidas de seguridad protectoras sean tomadas, la empresa será dejada abierta a la invasión de privacidad, a fraude, y a ataques maliciosos.

Para mitigar estas amenazas apropiadamente, los riesgos verdaderos deben ser identificados y trazar un mapa de una estructura de seguridad, incluyendo recomendaciones que se han venido usando en las redes de datos normales, así como la implementación de equipos como *gatekeepers*, servidores *proxy* SIP, *firewalls*, etc. Así como el uso de autentificación de señales encriptación de datos e *Ipsec* para asegurar que la persona autorizada esta llamando.

Todo esto con motivo de mejorar la seguridad en las conversaciones. Este marco puede ser usado para establecer requisitos de seguridad para que entonces los productos usados obtengan un apropiado nivel de seguridad para la solución de este problema.

CAPÍTULO 1: VISIÓN GENERAL DE VoIP

La Voz sobre IP (VoIP) no es algo nuevo en el mundo de las telecomunicaciones, pero su uso todavía no está muy extendido. Por varios años, VoIP era una posibilidad tecnológica. Ahora, sin embargo, las compañías de telecomunicaciones y otras organizaciones tienen ya, o están el proceso de, cambiar su infraestructura de telefonía a sus redes de datos. La solución que VoIP provee es una alternativa más barata y más clara que las líneas de teléfono tradicional. Aunque su implementación está muy difundida, a menudo carece de compatibilidad y continuidad con sistemas existentes. Sin embargo, los beneficios que los actuales usuarios de VoIP citan regularmente en las encuestas son: llamadas más baratas o incluso gratuitas, teléfonos más fáciles de usar, menos conexiones telefónicas, administración más fácil del sistema telefónico, etc. VoIP es un servicio basado en red y, por tanto, tiene los mismos puntos fuertes y vulnerables que cualquier otro servicio de red. VoIP tiene que protegerse con las mismas medidas de seguridad que se utilizan en las redes informáticas.

Características principales

Por su estructura VoIP proporciona las siguientes ventajas:

- Permite el control del tráfico de la red.
- Proporciona el enlace a la red telefónica tradicional.
- Al tratarse de una tecnología soportada en IP presenta las siguientes ventajas adicionales:
    - Es independiente del tipo de red física que lo soporta.
    - Permite ser implementado tanto en software como en hardware.

Arquitectura de red

El propio Estándar define tres elementos fundamentales en su estructura:

- ***Terminales*:** Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware.
- ***Gatekeepers*:** Son el centro de toda la organización VoIP, y serían el sustituto para las actuales centralitas. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

- ***Gateways*:** Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

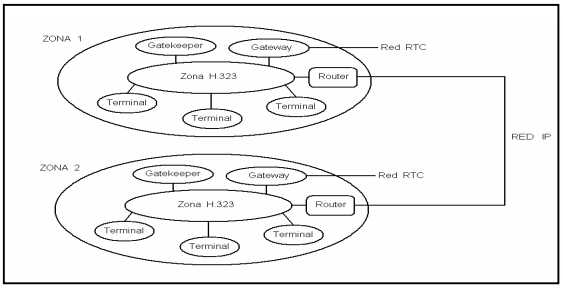


Figura 1: Esquema de ejemplo de VoIP.

- ***Protocolos*:** Es el lenguaje que utilizan los distintos dispositivos VoIP para su conexión. Esta parte es muy importante ya que de ella dependerá la eficacia y la complejidad de la comunicación.
    - Por orden de antigüedad (de más antiguo a más nuevo y los mas usados):
        - H.323 - Protocolo definido por la ITU-T
        - SIP - Protocolo definido por la IETF
        - Megaco (También conocido como H.248) y MGCP - Protocolos de control

Parámetros de VoIP

Garantizar la calidad de servicio sobre una red IP, en base a retardos y ancho de banda, actualmente no es posible, es por eso que se presentan diversos problemas en cuanto a garantizar la calidad del servicio.

- ***Codecs*:**

La voz ha de codificarse para poder ser transmitida por la red IP. Para ello se hace uso de *Codecs* que garanticen la codificación y compresión del audio y/o del video para su posterior decodificación y descompresión antes de poder generar un sonido o imagen utilizable. Según el Codec utilizado en la transmisión, se utilizará más o menos ancho de banda. La cantidad de ancho de banda suele ser directamente proporcional a la calidad de los datos transmitidos. Entre los codecs utilizados en VoIP encontramos los G.711, G.723.1 y el G.729 (especificados por la ITU-T)

- ***Retardo* o *latencia*:**

Una vez establecidos los retardos en el procesamiento, retardos de tránsito y el retardo de procesado la conversación se considera aceptable por debajo de los 150 ms.

- ***Calidad del servicio*:**

La calidad de servicio se está logrando en base a los siguientes criterios:

- La supresión de silencios, otorga más eficiencia a la hora de realizar una transmisión de voz, ya que se aprovecha mejor el ancho de banda.
- Compresión de cabeceras aplicando los estándares RTP/RTCP.
- Priorización de los paquetes que requieran menor latencia.

1.1 Visión general del manejo de datos de VoIP

Antes de que cualquier paquete de voz pueda ser enviado, se debe realizar una llamada. En VoIP, el usuario debe introducir el número al que desea llamar, este podría ser ingresado mediante el teclado o con la selección de un indicador de recurso universal (URI), después de esto se dará la transmisión basado en un protocolo de señalización de VoIP. El problema es que los sistemas de computación están direccionados con el uso de la Dirección IP. El número de teléfono debe ser conectado con una dirección IP para poder realizar la llamada, esta podría ser una dirección de Web alfabética como "www.uazuay.edu.ec" que debería ser vinculada con la dirección IP del servidor Web de la Universidad. Varios protocolos están involucrados en determinar la dirección IP al que corresponde el número telefónico llamado.

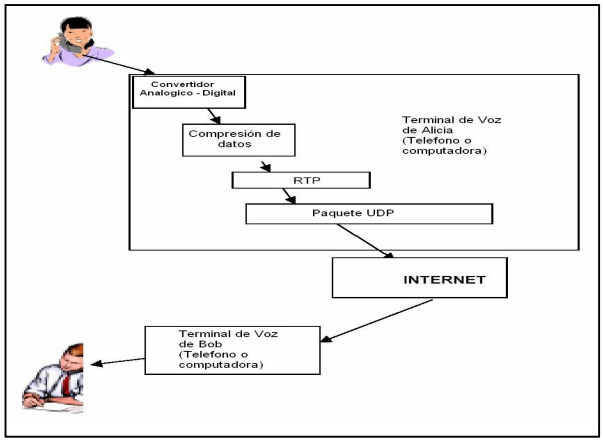


Figura 2. Procesamiento de la voz en sistemas de VoIP

La figura 2 ilustra la circulación básica de los datos de voz en un sistema de VoIP. Una vez que la persona llamada contesta, la voz debe ser convertida de su forma analógica a la forma digital, luego segmentar la señal de la voz en un grupo de paquetes. Debido a que la voz requiere un número largo de bits, podría ser usado un algoritmo de

compresión para reducir el volumen de los datos a ser transmitidos. Después, las muestras de voz son insertadas en paquetes de datos para ser llevados por la Internet. El protocolo para el envió de paquetes de voz es típicamente el protocolo de transporte de tiempo real, RTP. Los paquetes RTP tienen campos de encabezamiento especial que son necesarios para un correcto reensamblaje de los paquetes de voz en el punto final de la red. Los paquetes de voz serán llevados como carga útil dentro del protocolo UDP. En otras palabras, los paquetes de RTP son llevados como datos por las datagramas de UDP. En el punto final de la red, el proceso es invertido: los paquetes son desarmados y puestos en el orden correcto, digitalizados y descomprimidos los datos de voz extraídos de los paquetes, luego la voz digitalizada es procesada por un transformador digital - análogo para entregarlo en señales analógicas para el entendimiento de la persona llamada.

1.2 Velocidad y Calidad

VoIP puede proveer el uso reducido de ancho de banda y calidad superior a su predecesor, el PSTN convencional. Es decir el uso de medios de comunicación de ancho de banda común para comunicación de datos, combinado con la alta calidad de la voz digitalizada, hacen de VoIP una alternativa flexible para la transmisión de la voz. En la práctica, sin embargo, la situación es más complicada. El ruteo de todo el tráfico de una organización sobre una simple red causa congestión, además, enviar este tráfico sobre la Internet puede causar un retraso importante en la entrega de los datos. Muchas organizaciones que han cambiado a un esquema de VoIP recientemente no han notado ninguna degradación importante en la velocidad o la calidad.

1.3 Privacidad y temas legales de VoIP

La telefonía IP no cuenta con una regulación legal definida a nivel mundial centrándose la discusión en aspectos como:

- Se trata de Telecomunicaciones o transmisión de datos. (Aquí esta determinación implica si paga impuestos como en Ecuador del 27% o no y qué tipo de licencias se requieren para prestar el servicio).

En el Ecuador de acuerdo con lo expresado por el CONATEL en septiembre de 2003, lo siguiente fue adoptado en el pleno de la entidad regulatoria:

1. Que las normas principales que regulan el acceso de usuarios a la red de Internet y a las aplicaciones de ésta, mediante el uso de equipos de computación y relacionados, son:

a) La Ley Reformatoria a la Ley Especial de Telecomunicaciones;
b) El Reglamento General a la Ley Especial de Telecomunicaciones Reformada;
c) El Reglamento para la Prestación de Servicios de Valor Agregado; y,
d) La Resolución 399-18-CONATEL-2002.

2. Que la legislación ecuatoriana no define en ninguna parte lo que es la transmisión de voz sobre el protocolo de Internet "VoIP", ni tampoco la regula, la limita o la prohíbe.

3. Que en el Ecuador la ley define servicios y no regula tecnología, entre otras.

De acuerdo con la legislación vigente en el Ecuador, la forma en la que se está brindando acceso al Internet y a sus distintas aplicaciones entre las que se encuentra la transmisión de datos mediante el protocolo de voz sobre Internet VoIP, es absolutamente apegada a derecho, y de ninguna manera la Superintendencia de Telecomunicaciones puede prohibir la prestación o publicidad de estos servicios, máxime si consideramos el principio legal y Constitucional de que "Nadie podrá ser obligado a hacer algo prohibido o a dejar de hacer algo no prohibido por la ley".

Las normas legales de formas diversas tratan específicamente de proteger monopolios establecidos por operadoras a menudo ineficientes que encarecen los servicios sin beneficio para el usuario. Si existe una alternativa práctica, cómoda y accesible para los usuarios, entonces lo que cabe es impulsarla, incentivarla y dotarla de normas que le permitan crecer. El tipo de regulación que se necesita tiene que estar acorde con el mercado, con las necesidades de los usuarios y con el desarrollo tecnológico.

1.4 Temas de seguridad con VoIP

Con la introducción de VoIP, la necesidad de seguridad se ve agraviada porque ahora debemos proteger dos posesiones inestimables, nuestros datos y nuestra voz. Por ejemplo cuando se pide una mercancía por teléfono, la mayoría de personas leerá su

número de tarjeta de crédito a la persona que se encuentra del otro lado de la línea, Los números son transmitidos sin la encriptación necesaria al vendedor. Los paquetes enviados de la computadora de un usuario a un minorista en línea podrían pasar a través de 15-20 sistemas que no están bajo el control del usuario. Alguien con acceso a estos sistemas podía instalar un software que eche un vistazo a los paquetes que llevan la información de la tarjeta de crédito. Por esta razón, los minoristas en línea directa usan software de encriptación para proteger la información de un usuario. Así que es lógico que si nosotros transmitimos la voz sobre Internet, deberían ser aplicadas medidas de seguridad similares.

La arquitectura de Internet no provee la misma seguridad en el cable físico como las líneas de teléfonos normales. La clave para asegurar VoIP es usar los mecanismos de seguridad desplegados en redes de datos (*Firewalls*, encriptación, etcétera) y emular el nivel de seguridad actualmente disfrutado por usuarios de la red de PSTN.

Riesgos de una arquitectura VoIP

Los problemas de seguridad de esta tecnología no son nuevos y se vienen discutiendo desde hace algún tiempo. Por resumir, los problemas típicos en un despliegue VoIP están asociados a:

– La confidencialidad: la capacidad de obtener información de las conversaciones realizadas a través de la red VoIP.

– La integridad: la manipulación de conversaciones en curso a través de la inyección de tráfico, o la manipulación de los elementos de la red VoIP.

– La disponibilidad: la capacidad de interrumpir las comunicaciones VoIP e impedir el uso del servicio.

La capacidad de violar la confidencialidad de las llamadas se evidencia porque los protocolos sugieren la utilización de mecanismos de cifrado de transporte (*IPsec)* en lugar de incorporar el cifrado en el propio protocolo (salvo en el caso de SRTP). Existen múltiples formas de comprometer la confidencialidad de una comunicación, bien manipulando los dispositivos que forman la red, o bien directamente manipulando el

puerto físico al que están conectados éstos. Los propios dispositivos finales también son susceptibles a ataques. Para identificar a otro dispositivo VoIP final, basta con analizar el tráfico cuando se llama a la extensión o número final e identificar la dirección IP destino. Una vez obtenida la dirección IP se puede:

– Reconfigurar el equipo mediante alguno de los múltiples mecanismos de administración disponibles (HTTP, TFTP, SNMP o telnet) para que envíe el tráfico al atacante o, simplemente, para que envíe sus registros de actividad para determinar quién llama o a quién llama el dispositivo.

– Dejarlo sin servicio, para lo que existen múltiples ataques posibles: enviar respuestas DHCP falseadas, inundarle de paquetes, utilizar problemas de implementación de los protocolos, etc.

La mayoría de los fabricantes de teléfonos IP diseñan sus mecanismos de gestión facilitando estos ataques. Así, los siguientes mecanismos de gestión son vulnerables:

– Servicio de administración vía Web habilitado con contraseñas por defecto ('123', 'admin', etc.). Aunque disponga de una contraseña, al no estar cifrado y utilizar autenticación básica en muchos casos podría interceptarse ésta al utilizarse desde otro equipo.

– Mecanismos de descarga de nuevas versiones software que utilizan protocolos (TFTP o HTTP) o de acceso a red (DHCP o DNS) no cifrados y sin autenticación mutua, lo que permite ataques de suplantación e intercepción.

Más graves aún son los errores de implementación de los estándares publicados que se observan en los dispositivos y con consecuencias en su seguridad. Un usuario malicioso, haciéndose pasar por un teléfono, puede obtener a través del servidor DHCP información de la infraestructura de la red: servidor de TFTP utilizado para las descargas de configuraciones y software, localización del *Gatekeeper*, comunidad SNMP de acceso a los equipos y servidores SNMP autorizados, servidor de DNS y zona de DNS, etc.

CAPÍTULO 2: CALIDAD DE SERVICIO (QoS)

La calidad de servicio (*QoS*) es fundamental para las operaciones de una red VoIP. A pesar de todo el ahorro de dinero que VoIP puede proveer a los usuarios, si este no puede entregar la misma calidad de conexión de llamada y de funcionalidad de transmisión de voz y de calidad de voz como la red de telefonía tradicional, entonces este proporcionara poco valor agregado. La implementación de diferentes medidas de seguridad puede degradar *QoS*. Estas complicaciones van desde una demora o bloqueo de las conexiones de llamadas por *Firewalls* a la latencia producida por encriptación y una variación en la demora (*Jitter*). Los problemas de *QoS* son centrales para la seguridad de VoIP. Debido a la naturaleza de VoIP muchas medidas de seguridad implementadas en redes de datos tradicionales no son aplicables a VoIP. Los principales aspectos que afectan la seguridad son:

2.1 Latencia

La latencia se refiere al tiempo que toma una transmisión de voz para ir de su fuente a su destino. Preferentemente, mantener la latencia tan baja como sea posible seria lo ideal, pero hay límites muy bajos prácticos en el retardo de VoIP. El límite superior es 150 ms para tráfico de una vía. Esto corresponde al límite de latencia actual experimentado en llamadas locales por las líneas de PSTN en los Estados Unidos. Para las llamadas internacionales, un retraso mayor a 400 ms se juzgó tolerable. Esta restricción de tiempo deja un margen muy pequeño de error en entrega de paquetes. Además, coloca restricciones en la cantidad de seguridades que puede agregarse a una red de VoIP.

2.2 Jitter

El *Jitter* se refiere a retrasos de paquetes. Es causado a menudo por situaciones de bajo ancho de banda en VoIP y puede ser excepcionalmente perjudicial para una *QoS* global. Las variaciones en retrasos pueden ser más perjudiciales a *QoS* que los propios retrasos reales. El Jitter puede ser causado en paquetes al arribo y pueden procesarse fuera de secuencia. En RTP los paquetes fuera de orden no se vuelven a reensamblar a nivel protocolar. Sin embargo, permite aplicaciones para realizar el reordenamiento usando el

número de secuencia y el campo de *timestamp*. Cuando el *jitter* es alto, los paquetes llegan a su destino con gran esfuerzo. La regla general para controlar el *jitter* en puntos finales de VoIP es el uso de un *buffer*, pero este debe liberar sus paquetes de voz por lo menos cada 150 ms (normalmente mucho más pronto dado el retraso de transporte) así que deben limitarse las variaciones en el retraso. El problema de aplicación del *buffer* es compuesto por la incertidumbre de que si un paquete perdido simplemente se tarda una cantidad larga de tiempo, o está realmente perdido. Si el *jitter* es particularmente errático, entonces el sistema no puede usar tiempos anteriores de retraso como un indicador para el estado de un paquete perdido. El *jitter* también puede controlarse a lo largo de la red de VoIP usando *routers*, *firewalls*, y otros elementos de la red que soporta QoS. La ventana de entrega para un paquete de VoIP es muy pequeña, así que resulta que la variación aceptable en el retraso del paquete es aun más pequeña. Así, aunque nosotros nos preocupamos por la seguridad, debe darse sumo cuidado a asegurar que la demora en la entrega del paquete causada por dispositivos de seguridad se mantenga uniforme a lo largo del flujo del tráfico. Implementando dispositivos que soportan QoS y mejorando la eficacia del ancho de banda con la compresión del encabezado permite un retraso de los paquetes más uniforme en una red de VoIP.

2.3 Pérdida de paquetes

VoIP es intolerante a la pérdida de paquetes. La pérdida de paquetes puede ser el resultado del exceso de latencia, o puede ser el resultado del *jitter*.

La perdida de paquetes se presenta porque RTP utiliza el transporte de UDP. Sin embargo, las restricciones de tiempo no permiten el uso de un protocolo fiable como TCP para entregar la media. Cuando un paquete pudiera reportarse perdido, retransmitido, y recibido, las restricciones de QoS se excederían. Por ventaja los paquetes de VoIP son muy pequeños, conteniendo una carga útil de sólo 10-50 *bytes* que es aproximadamente 12.5 - 62.5 ms. La pérdida de tal minúscula cantidad de conversación no es palpable o por lo menos no digno de queja para un usuario humano. La congestión del Ancho de Banda y otras causas tales como la pérdida de paquetes tienden a afectar todos los paquetes que se entregan alrededor del mismo tiempo. Así aunque la pérdida de un paquete es bastante insignificante, probablemente la pérdida de un paquete significa la pérdida de varios paquetes que severamente degradan la calidad de servicio en una red VoIP.

A pesar de no poder usar un protocolo de entrega garantizado como TCP, hay algunos remedios para el problema de pérdida de paquetes. No se puede garantizar la entrega de todos los paquetes, pero si el ancho de banda disponible, enviando información redundante pueden probabilísticamente anular la oportunidad de pérdida.

2.4 Ancho de banda y Ancho de banda efectivo

Como en las redes de datos, la congestión del ancho de banda puede causar a la pérdida del paquete y otros problemas de *QoS*. Así, la reserva de ancho de banda apropiada y la asignación es esencial a la calidad de VoIP. La congestión de la red causa encolamientos de paquetes, qué contribuye a la latencia. El ancho de banda bajo también pueden contribuir al *jitter*. Los métodos para reducir el uso del ancho de banda de VoIP incluyen la compresión de la cabecera de RTP y la Detección de Actividad de Voz (VAD). La compresión de RTP condensa el tráfico del flujo de la media así que es usado un menor ancho de banda. Sin embargo, un esquema de compresión ineficaz puede causar latencia o degradación de la voz, causando una depresión global en QoS. VAD previene la transmisión de paquetes vacíos de voz (es decir cuando un usuario no está hablando, su dispositivo simplemente no manda ruido blanco). Sin embargo, por definición VAD contribuirá al jitter en el sistema.

Dado que la voz y los flujos de datos son compartidos en el mismo ancho de banda, y los flujos de datos tienden a contener paquetes mucho más grandes que VoIP, cantidades significantes de datos pueden congestionar la red y puede impedir el tráfico de voz. Por esta razón, los nuevos dispositivos de hardware despliegan en las redes un apoyo de QoS para VoIP. Estos dispositivos, hacen uso del protocolo de IP *Type of services* (ToS) para enviar antes el tráfico de datos urgentes. No sólo es el ancho de banda disponible del sistema afectado por la introducción de medidas de seguridad, además el ancho de banda eficaz del sistema de VoIP se deprecia significativamente. El ancho de banda eficaz es definido por *Barbieri et al.* como *"el porcentaje de ancho de banda que encamina datos reales con respecto al total del ancho de banda usado"*.

2.5 QoS: implicaciones de seguridad

Los requisitos de funcionamiento estrictos de VoIP tienen implicaciones significantes de seguridad, especialmente los problemas de Rechazo de Servicios (DoS). Los ataques específicos de VoIP puede producir un DoS para muchos dispositivos. Por ejemplo, los puntos finales como teléfonos SIP pueden paralizarse y colapsar cuando se intenta procesar una tasa alta de tráfico de paquetes en servidores proxy SIP. Es decir, una tasa alta del paquete puede producir un rechazo del servicio aun cuando el ancho de banda consumido sea bajo.

CAPÍTULO 3: PROTOCOLO H.323

El protocolo H.323 es la especificación de la ITU para la transmisión de audio y video en redes de paquetes. H.323 es un estándar que, abarca algunos otros protocolos, incluyendo H.225, H.245, y otros. Cada uno de estos protocolos tiene un papel específico en el proceso de configuración de llamada (*call setup*), y cada uno de estos son realizados en puertos dinámicos.

3.1 Arquitectura de H.323

Una red de H.323 podría estar formada por algunos puntos finales (terminales o host), gateways, gatekeeper, *Multipoint Control Unit* (MCU), y *Back End Service* (BES).

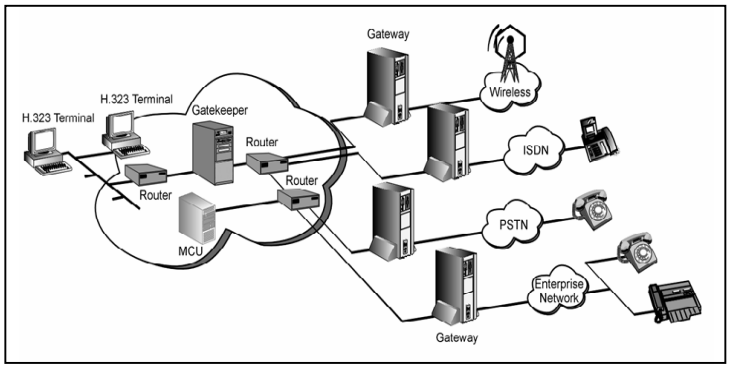


Figura 3: Arquitectura de una red H.323

Una unidad de Control de Multipunto (MCU) es un elemento opcional que facilita la conferencia de multipuntos y otras comunicaciones entre más de dos puntos finales. Consiste de:

- *Multipoint Contoller* (MC): negocia con todos los terminales para asegurar un denominador común
- *Multipoint Processor* (MP); es capaz de mezclar o conmutar tráfico de voz, datos o video

Un gatekeeper es a menudo uno de los componentes principales en los sistemas H.323.

- Provee traducción de direcciones y servicio de control de llamadas a los terminales H.323
- Es responsable de manejar la distribución de ancho de banda sobre la LAN de los terminales
- Un Gatekeeper maneja una colección de terminales, Gateway y MCU´s llamada zona.

El gateway sirve de puente entre la red de H.323 y el mundo exterior de dispositivos (posiblemente) no H.323, esto incluye redes SIP y redes PSTN tradicionales. Estos corredores pueden añadir demoras en VoIP. Si un gatekeeper está presente, un servicio de extremo posterior (BES) podría existir para mantener los datos sobre puntos finales, incluyendo sus permisos, servicios, y configuración.

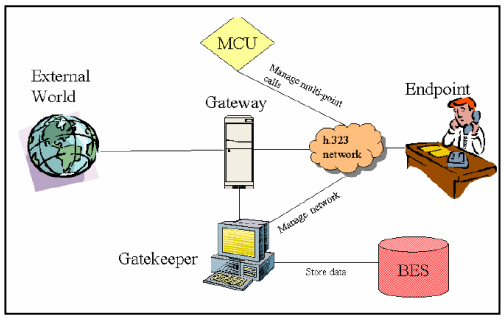


Figura 4: Arquitectura de H. 323 con MCU y BES

Protocolos de H.323

Codecs de audio:

Codifica y decodifica las señales de audio para transmitirlo desde y hacia un terminal H.323. Todos los terminales de H323 deben tener un codificador de voz. El requerimiento mínimo es el soporte de G.711. Durante el *handshake* inicial se usa H.245 para determinar el algoritmo de codificación de audio a usar.

H.225:

Registro, admisión y estado (RAS), protocolo entre gateway o equipo terminal y gatekeeper. Sus Funciones son: Registro, Control de admisión, cambios del ancho de banda, estado, y resuelve procedimientos entre estos dispositivos.

H.225 (Q.931) Call Signaling:

Usado para establecer una comunicación entre dos puntos H.323.

H.245

Control de señalización. Sus funciones son: encargase del intercambio de capacidades, abrir y cerrar canales lógicos y del control de flujo de mensajes.

RTP

El protocolo en tiempo real de transporte (RTP) provee la entrega en tiempo real de audio y video. Es usado para transmisión de datos usando UDP. RTP no garantiza QoS para los servicios en tiempo real (Anexo 1).

RTCP

RTP control protocolo (RTCP) realiza el control del RTP se basa en la periódica transmisión de los paquetes de control a todos los participantes en sesión. Sus funciones son: Identificación de la carga útil, secuencia y entrega supervisada.

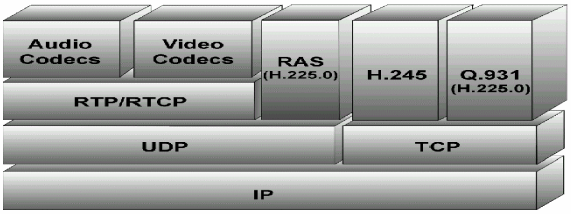


Figura 5: Arquitectura Protocolos de H.323

Establecimiento de la llamada H.323

El establecimiento de la llamada en H.323 se lleva a cabo en tres fases:

- Fase RAS: intercambio de mensajes entre el gatekeeper y el *endpoint*, para la traducción de direcciones, autorización de llamadas y gestión del ancho de banda (Anexo 1).
- Fase Q.931: intercambio de mensajes entre *endpoints* para el establecimiento de conexiones lógicas.
- Fase H.245: intercambio de mensajes entre *endpoints* para acordar en intercambio de información de usuario.

A continuación de estas tres fases, se lleva a cabo la transferencia de información de usuario por medio de los protocolos RTP/RTCP, previa apertura de los canales lógicos en los *endpoints*. Estos canales lógicos son unidireccionales, por lo que para una comunicación bidireccional se requiere abrir uno en cada dirección de transmisión.

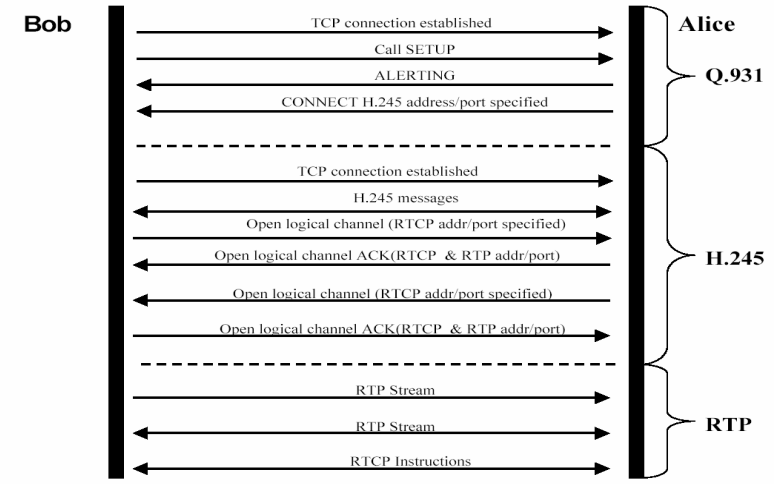


Figura 6: Modelo de establecimiento de llamada H.323

Modelo de la llamada H.323

Generalmente, hay diferentes clases de llamadas definidas en el estándar de H.323:

- Llamada con ruteo de un Gatekeeper a otro con señalización H.245
- Llamada con ruteo directo con señalización H.245 mediante un Gatekeeper
- Ruteo directo de una llamada con Gatekeeper
- Ruteo directo de una llamada sin Gatekeeper

Una sesión VoIP de H.323 es iniciada (dependiendo del modelo de llamada usado) por un protocolo TCP o un UDP (si RAS es el punto de partida) la conexión con una señal H.225. En el caso de UDP este aviso contiene el *Registration Admisión Status* (RAS), que negocia con el Gatekeeper y obtiene la dirección del punto final con el que está intentando hacer contacto. Luego el protocolo Q.931 (dentro de H.225) es usado para establecer la llamada y negociar el direccionamiento de la señal de H.245. Este procedimiento es común durante el proceso de H.323 donde un protocolo negocia la configuración del próximo protocolo a usar. H.225 sólo negocia el establecimiento de un enlace, H.245 establece las vías que serán usadas para la transferencia de media.

Los mensajes de SETUP y CONNECT concatenan los elementos de la señal H.245 necesarios. H.245 debe establecer algunas propiedades de la llamada de VoIP. Éstos incluyen los codecs de audio que serán usados y los canales lógicos para el transporte de la media. El aviso "OpenLogicalChannel" también actúa como intermediario del RTP y los puertos de RTCP. En general, 4 conexiones deben ser establecidas porque los canales lógicos (RTP y RTCP) son solamente una dirección. Después de que H.245 ha establecido todas las propiedades de la llamada de VoIP y los canales lógicos, la llamada podrá comenzar. (Descripción gráfica del Modelo de llamada: Anexo 2).

3.2 Perfiles de seguridad de H.235

Con el establecimiento de H.235 versión 2 se suministra diferente niveles de seguridad y se describe un subconjunto de los mecanismos de seguridad posibles ofrecido por H.235. Comprenden las diferentes alternativas para la protección de las comunicaciones.

3.2.1 H.235v2

Además del realce en el soporte de criptografía y el soporte para el estándar de sistema de encriptación avanzado (AES), algunos perfiles de seguridad fueron definidos para soportar la interoperabilidad del producto. Estos perfiles son definidos en anexos a H.235v2 de la siguiente manera:

- Anexo D – Punto de referencia de los perfiles de seguridad
- Anexo E - Firmas digitales sobre cada mensaje
- Anexo F - Firmas digitales y el establecimiento de secretos compartidos sobre el primer protocolo en enlace.

3.2.1.1 Anexo D de H.235v2 – Punto de referencia de los perfiles de seguridad.

Los secretos compartidos son usados para proveer la autentificación y/o la integridad del mensaje. Usar un secreto compartido para el modelo de llamada directa es en general posible pero limitado debido a que un secreto compartido tiene que ser establecido entre las partes que quieren comunicarse antes de que la comunicación verdadera tenga lugar. Esto podría ser posible en los ambientes más pequeños pero podría resultar un esfuerzo administrativo enorme en ambientes más grandes.

3.2.1.2 Anexo E de H.235v2 – Perfiles de seguridad de firma digital

Los certificados y las firmas digitales son usados para demostrar la autentificación y la integridad de mensaje. Desde este perfil se depende para obtener una infraestructura de clave pública en vez de tener secretos compartidos pre-establecidos. Este perfil sostiene una conexión rápida segura y tunneling H.245 y puede ser combinado con la encriptación de voz. Este protocolo podría tener un impacto crítico sobre el rendimiento en conjunto, esto debido a que se usa la firma digital por cada mensaje, requiriendo la generación de firmas y la comprobación sobre el equipo de remitentes y destinatarios.

3.2.1.3 Opción de encriptación de voz

La opción de encriptación de voz brinda la confidencialidad para el flujo de datos en medios de comunicación de voz y puede ser combinado con la referencia o el perfil de

seguridad de la firma. La opción de encriptación de voz describe el intercambio de llaves maestras durante la señal de llamada de H.225 y la generación y distribución de claves de secuencia de media durante la llamada de control de H.245. Los siguientes mecanismos de seguridad son descritos dentro del perfil de seguridad de encriptación de voz:

- La encriptación de paquetes de RTP con un grupo de algoritmos;
- Manejo de llaves con clave e intercambio de capacidad de seguridad;
- Mecanismo de actualización de claves y su sincronización.

Al ser descubierto ataques sobre puertos RTP / UDP, el estándar H.235 define el procedimiento de media *anti-spamming*, que provee una ligera autentificación de paquetes de RTP y la integridad de campos selectos a través de un mensaje de código de autentificación computado (*computed message authentication code* (MAC)).

3.2.1.4 Anexo F de H.235v2 – Perfiles de seguridad híbrida.

Este puede ser visto como una combinación de punto de referencia y perfil de seguridad de firma. Los certificados y las firmas digitales son usados para suministrar la autentificación y la integridad de mensaje como primer protocolo de enlace entre dos entidades. Durante el protocolo de enlace un secreto compartido es establecido, mismo que luego será usado. Este perfil sostiene una conexión rápida segura y tunneling de H.245 y puede ser combinado con la encriptación de voz. Este perfil suministra alta seguridad sin depender de los secretos compartidos pre- establecidos.

3.2.2 H.235v3

La versión 3 de H.235 tiene como protagonista un procedimiento para encriptado de señales DTMF, los objetos identificados por el algoritmo de encriptación AES para la encriptación de carga útil (payload) de la media y el modo de encriptación *Enhanced Outer FeedBack* (EOFB) para la encriptación de flujos de la media. Además, una opción de autentificación para NAT / firewall. El reporte de errores también es mejorado. H.235v3 describe un perfil para soportar SRTP.

3.2.2.1 Anexo D de H.235.v3 Realce de Puntos de referencia de los perfiles de seguridad.

Usando este perfil, los mensajes de autentificación e integridad son conseguidos calculando un valor de chequeo íntegro sobre el mensaje completo, o una autentificación solo computando un chequeo íntegro sobre una parte especial del mensaje. La opción última es útil en los ambientes donde NAT y Firewalls están presentes.

3.2.2.2 Anexo G de H.235v3. SRTP & el uso de MIKEY

El anexo G habla de la incorporación del manejo de claves que soporta el protocolo de seguridad de transporte en tiempo real (SRTP). SRTP provee confidenciabilidad, autentificación de mensajes y protección de repetición de tráfico RTP / RTCP. SRTP es definido como el perfil del protocolo de RTP[1]. SRTP puede ser usado dentro de las sesiones de multimedia para asegurar un intercambio seguro de datos de la media. Puede ser usado con algunos protocolos de control de sesión, por ejemplo con H.323 o SIP. SRTP no define el manejo de claves por si solo. Este usa un set de parámetros de configuración de las claves de sesión para la encriptación y así obtener la autentificación y protección de la integridad.

Para la solución del manejo de claves SRTP se usa *Multimedia Internet Keying* (MIKEY). MIKEY describe un esquema de manejo de claves que aborda los escenarios de multimedia en tiempo real. MIKEY también soporta la negociación simple y múltiple de las sesiones de criptografía. Esto es especialmente útil para el caso donde el manejo de llaves es aplicado a SRTP, debido a que aquí RTP y RTCP pueden ser asegurados independientemente. MIKEY soporta la negociación de teclas criptográficas y parámetros de seguridad (SP) para uno o más protocolos de seguridad. Este define tres alternativas para la autentificación de usuario y la negociación de las llaves maestras todas como 2 vías de interconexión. Estas son:

[1] Estándar RFC 3711 de la ITU-T

- Distribución de clave simétrica (llaves pre - compartidas, MAC para la protección de la integridad)
- distribución de llaves asimétricas
- Convenio de clave *Diffie Hellman* protegida por las firmas digitales.

3.2.2.3 H.235v3 Anexo H – Manejo de llaves RAS

La idea básica formulada en el anexo H de H.235 es la negociación del manejo de llaves durante la fase de descubrimiento del gatekeeper RAS. Durante esta fase un secreto compartido es establecido entre el punto final de la red y el gatekeeper. La negociación de la clave compartida puede ser protegida usando números de identificaciones personales PINs o passwords durante la fase inicial del protocolo. El bosquejo menciona dos protocolos para el intercambio de llaves encriptadas usando una llave compartida que "oculte" un intercambio de llaves Diffie-Hellman.

- El primero es el intercambio de teclas de encriptación (EKE), donde la llave compartida es usada para encriptar las llaves públicas Diffie - Hellman bajo un algoritmo simétrico.
- El segundo es el método de Simple *Password-authenticated Exponential Key Exchange* (SPEKE) donde la llave compartida desarrolla un generador para el grupo Diffie - Hellman.

3.2.3 H.323 Temas de Seguridad.

Los firewalls plantean problemas particularmente difíciles para redes de VoIP usando H.323. Con la excepción de Q.931 todo tráfico H.323 es encaminado a través de puertos dinámicos. Para el inicio rápido de H.323 y H.245 tunneling sólo un canal es usado. Generalmente la señal de llamada es llevada a cabo por el puerto 1720. Adicionalmente la comunicación H.225 RAS es hecho con gatekeeper (UDP), esto es hecho vía el puerto 1719. Es decir cada canal sucesivo en el protocolo es encaminado a través de un puerto asignado dinámicamente por su predecesor. Este método de asegurar canales no se presta bien por si mismo para una configuración estática de firewalls. Esto es particularmente verdadero en caso de *firewalls stateless* que pueden comprender el tráfico H.323. Estos filtros de paquete simples no pueden aglutinar las transmisiones de UDP. Esto hace necesario realizar agujeros en el firewall para permitir el tráfico H.323

para atravesar el puente de seguridad. Esta práctica introduciría defectos serios en la seguridad porque esta implementación necesitaría dejar abiertos de par en par 10,000 puertos de UDP y algunos puertos H.323 de protocolo TCP específicos. Allí es por lo tanto, una necesidad de un *firewall stateful* que comprenda VoIP, específicamente H.323. El firewall puede leer los mensajes de H.323 y abrir dinámicamente los puertos correctos para cada canal cuando el protocolo se mueve a través de su proceso de configuración de llamada.

NAT es también particularmente problemático para los sistemas de VoIP usando protocolo de configuración de llamada de H.323. NAT complica las comunicaciones de H.323 porque la dirección IP interna y el puerto especificó en las cabeceras de H.323 y los mensajes mismos no son la dirección / números de puerto verdadera usadas externamente por una Terminal remota. Por lo tanto, si H.323 tiene que atravesar un NAT, el dispositivo de NAT debe ser capaz de reconfigurar las direcciones en el flujo de control. Así que con NAT, no sólo el tráfico H.323 necesita ser leído, también debe ser modificado con el propósito de que las direcciones / números puerto correctos sean enviados a cada uno de los puntos finales.

3.3 Temas de encriptación y su rendimiento.

El retraso en un sistema de VoIP puede ser añadido por los codecs y por procesamientos adicionales como la encriptación. Los codecs añaden el retraso al codificar y comprimir los datos a transmitir. La encriptación tiene dos propósitos para VoIP: la protección de privacidad, cifrando los datos de voz, y la autentificación de mensaje, que protege el origen y la integridad de los paquetes de voz.

CAPITULO 4: PROTOCOLO SIP

Session Initiation Protocol (SIP) es un protocolo de señalización basado en texto usado para crear y controlar sesiones multimedia con dos o más participantes. Es un protocolo cliente – servidor transportado sobre UDP o TCP, pero las implementaciones mas comunes usa SIP sobre UDP por simplicidad y velocidad. SIP es un protocolo mucho más simple que H.323 pero tan funcional como él. SIP tiene mayor performance, flexibilidad y escalabilidad. Tiene sus raíces en protocolos de texto anteriores como HTTP.

4.1 Arquitectura SIP

Una red SIP se compone de puntos finales, un Proxy y/o servidor de redireccionamiento, servidor de localización, y registradores. En el modelo SIP, un usuario no se liga a un host específico (en H.323, el gatekeeper proporciona resolución de dirección). El usuario inicialmente informa su posición a un registrador que puede integrarse en un Proxy o un servidor de redireccionamiento. Esta información se guarda a su vez en el servidor de localización externo. Los mensajes de los puntos finales deben encaminarse a través de un proxy o un servidor de redireccionamiento. El servidor proxy intercepta mensajes de los puntos finales, inspeccionando su campo "*to*:", contacta al servidor de localización para resolver el nombre de usuario en una dirección y proporciona el mensaje al punto final apropiado u otro servidor. Los servidores de redireccionamiento realizan la misma funcionalidad de resolución, pero la carga se pone en los puntos finales para realizar la transmisión real. Es decir, los servidores de redireccionamiento obtienen la dirección real del destino del servidor de localización y devuelven esta información al remitente original que entonces debe enviar su mensaje directamente a la dirección que se resolvió.

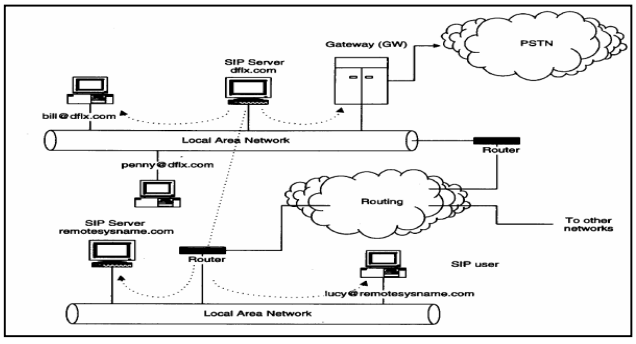


Figura 7: Estructura de SIP

Elementos de SIP

- ***User Agent* (UA)**

  Un sistema SIP consiste de Agentes de Usuario (UA) y uno o más servidores. El agente de usuario es una aplicación que inicia, recibe y termina llamadas. El agente de usuario que inicia una llamada se llama *User Agent Client* (UAC), y el agente que recibe la llamada se llama *User Agent Server* (UAS). Tanto UAC como UAS pueden finalizar las llamadas.

- **Servidores Proxy**

  Los servidores Proxy ejecutan señalización de llamadas en nombre de las partes a quienes sirven. Actúan tanto como un servidor y como un cliente para hacer requerimientos en nombre de otros clientes, además interpretan, reescriben o traducen un mensaje de requerimiento antes de reenviarlo.

- **Servidores *Redirect***

  Determinan la ubicación actual de la parte llamada e instruyen a la parte llamante a iniciar señalización con la parte llamada directamente. Los servidores *redirect* aceptan un requerimiento de SIP y mapean la dirección en otras que retorna al cliente. A diferencia de un servidor Proxy no inicia su propio requerimiento SIP. A diferencia de un UAS no acepta o termina llamadas.

Aspectos claves de SIP

- Establecimiento de llamada: SIP es auto contenido para establecer conferencias punto a punto y multipunto.
- Servicios de localización de Usuarios: Los usuarios tienen la posibilidad de moverse a otras ubicaciones y acceder a sus servicios de telefonía desde localizaciones remotas. Este servicio es equivalente al provisto por RAS en H.323.
- Capacidades de Usuario: Determinación de la media y parámetros de media a ser usados. SIP usa el formato del protocolo SDP para negociar parámetros de media así como H.323 usa la señalización H.245.
- Disponibilidad de Usuario: Determinación del deseo de la parte llamada para entrar en comunicación. SIP define códigos de respuesta muy explícitos con información sobre la disponibilidad actual del usuario.
- Manejo de llamadas: Incluye transferencia de una llamada establecida, etc. Esto es importante para servicios de telefonía en una red publica

SIP usa URIs (*Uniform resource identifiers*) para identificar direcciones de fuente, destino y redireccionamiento. Se puede incluir en el URI el número de puerto que para SIP se usa el puerto UDP número 5060. Como los otros protocolos de señalización, SIP también especifica el uso de RTP para el transporte de la media y RTCP para control de media.

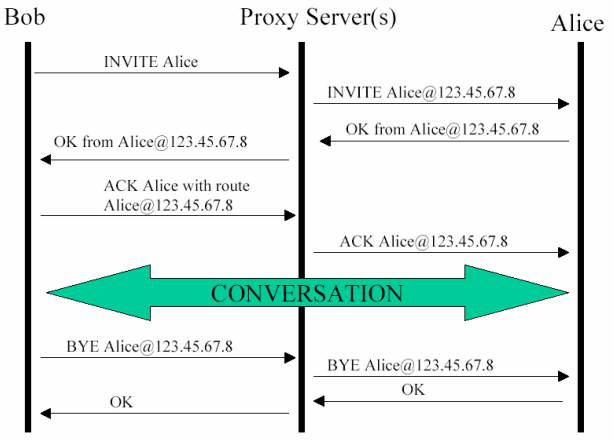


Figura 8: Modelo de establecimiento de llamada SIP

Métodos de señalización SIP

SIP usa 6 métodos de señalización: *INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER.*

INVITE

Este es el primer mensaje enviado por la parte llamante, contiene información en el header SIP que identifica a la parte llamante, *call – ID, called party, call sequence number,* entre otras. Básicamente indica que una llamada esta siendo iniciada o puede ser enviado durante una llamada para modificar el estado de operación de una llamada. El mensaje INVITE contiene usualmente una descripción SDP de parámetro de llamada, tal como tipo de media y direcciones de transporte.

ACK

El agente de llamada responde con ACK solo a requerimientos INVITE que han sido satisfactoriamente aceptados. El cuerpo del mensaje ACK puede contener la descripción SDP de la capacidad de tipo de media de la parte llamada. Si la respuesta ACK no contiene descripción SDP, significa que acepta los parámetros enviados en INVITE para la negociación de la media.

OPTIONS

Este mensaje se envía para consultar las capacidades de un agente de llamada. Es una herramienta adecuada para determinar que tipos de media soporta un usuario remoto antes de realizar una llamada.

BYE

El cliente envía este mensaje al agente de llamada para terminar la llamada, no es necesaria una contestación al mensaje BYE por parte del otro usuario.

CANCEL

Este método cancela un requerimiento en proceso, pero no tiene efecto sobre una llamada establecida cuando ningún requerimiento esta en proceso.

REGISTER

Permite a un cliente registrar la dirección listada en el campo de header "*to*" con el servidor SIP.

Modelo de llamada SIP

Usualmente ocurren 6 pasos:

1. Registrar, iniciar y localizar el usuario.
2. Determinar la media a usar.
3. Determinar el deseo de una parte llamada para comunicarse.
4. Establecimiento de una llamada.
5. Modificación de la llamada.
6. Terminación de la llamada.

Nota: Modelos de llamadas SIP en el Anexo 3.

4.2 Conceptos de seguridad existentes dentro del protocolo SIP

4.2.1 Autentificación de señales de datos usando autentificación de recopilaciones de HTTP

El esquema de autenticación de recopilaciones de HTTP esta basado en un modelo simple de desafío - contestación. Aquí, una respuesta válida contiene un *checksum* del *nombre de usuario*, la *contraseña*, los valores *eventuales* dados, el *método* HTTP y el URI solicitado. De esta manera, la contraseña nunca se envía en claro debido a su

seguridad débil, y para evitar ataques degradando el nivel de seguridad requerido de la autenticación.

4.2.2 Uso de S/MIME dentro del SIP

Los mensajes de SIP llevan cuerpos de MIME (*Multipurpose Internet Mail Extensión*: estándar para describir contenido en Internet). El propio MIME define mecanismos para la protección de integridad y la encriptación de los contenidos. SIP puede usar S/MIME para habilitar mecanismos como la distribución de la clave pública, la autenticación y protección de integridad, o confidencialidad de señalización de datos SIP. Para poder proteger también campos de la cabecera de SIP, es especificado el tunneling de los mensajes SIP en el cuerpo del MIME. Generalmente los tunneling de SIP propuestos para la protección de la cabecera de SIP crearan *overhead* adicional. S/MIME requiere los certificados y las claves privadas para ser usado, considerando que los certificados pueden emitirse por un tercero o pueden generarse a si mismos. El último caso no puede proporcionar autenticación del usuario real pero puede usarse para proporcionar una forma limitada de protección de integridad del mensaje. Si S/MIME se usa para los mensajes *tunnel* es recomendable usar una conexión TCP debido a que los mensajes son más grandes. Esto es para evitar problemas que pueden surgir por la fragmentación de paquetes UDP.

4.2.3 TLS usado en SIP

Se recomienda el uso de *Transport Level Security* (Nivel de seguridad de transporte) TLS para UAs[2]. TLS puede proteger mensajes de señalización de SIP contra la pérdida de integridad, confidencialidad y contra la repetición. Proporciona integridad de manejo de claves con autentificación mutua y asegura la distribución de la clave. TLS es apropiado para *peer to peer* entre UAs/proxys o entre proxys. El inconveniente de TLS en escenarios SIP es que requiere de una pila de transporte fiable (TCP). TLS no puede aplicarse a UDP.

4.2.4 IPsec usado en SIP

IPsec también puede usarse para proporcionar seguridad para la señalización de SIP en la capa de red. Este tipo de seguridad protege los hosts SIP en un escenario SIP *Virtual*

[2] Según RFC 3261 de la ITU-T

Private Network (VPN) o entre los dominios de SIP administrativos. IPsec trabaja para UDP y TCP basados en señalización SIP. IPsec puede usarse para proporcionar autenticación, integridad y confidencialidad para los datos transmitidos y de apoyo extremo-a-extremo así como también en los escenarios de *peer to peer*. Un protocolo aceptado para el manejo de la clave es el Intercambio de Clave de Internet (IKE), que provee un intercambio automatizado de claves criptográficas y mecanismos de manejo para IPsec. IKE se usa particularmente en el establecimiento de VPNs.

4.2.5 Realce de la seguridad en SIP

Actualmente están discutiéndose varios proyectos de seguridad, con vista a proporcionar una solución de seguridad general para los escenarios SIP. Se han producido varios proyectos acerca de la autenticación, integridad, y confidencialidad para SIP. Las subdivisiones siguientes proporcionan una apreciación global de proyectos que pueden ser de interés para una discusión de perfeccionamientos de seguridad para los escenarios comunes de SIP.

4.2.5.1.- Cuerpo de Identidad Autenticado de SIP

El Cuerpo de Identidad Autenticado de SIP (AIB) define una ficha de autenticación genérica de SIP. La ficha es proporcionada por un cuerpo de S/MIME adicional a una demanda de SIP o contestación para proporcionar integridad de la referencia en sus cabeceras. El documento define un formato para este cuerpo del mensaje llamado un cuerpo de identidad autenticado (AIB). Éste puede ser un mensaje de SIP firmado digitalmente (sip/message) o un mensaje fragmentado (sip/frag).

4.2.5.2 Manejo de Identidad Autenticado de SIP

Los mecanismos existentes para expresar frecuentemente identidad en SIP no permiten a un dominio administrativo verificar firmemente la identidad del creador de una demanda. Este documento recomienda prácticas y convenciones para autenticar a los usuarios finales, y propone una manera de distribuir criptográficamente identidades seguras autenticadas dentro de los mensajes de SIP.

4.2.5.3 S/MIME AES Requisito para SIP

El RFC 3261 especifica al 3DES como el algoritmo de encriptación mínimo requerido para las aplicaciones de S/MIME en SIP. Aunque 3DES todavía es un algoritmo viable, NIST ha seleccionado un algoritmo mejorado, AES, como un reemplazo para DES y 3DES. AES proporciona throughput más alto y la complejidad computacional más baja que 3DES, y puede llevarse a cabo con requisitos de memoria bajos, haciéndolo más conveniente para los dispositivos móviles o fijos, incluyendo los teléfonos VoIP.

4.2.5.4 Acuerdo de Mecanismo de Seguridad para SIP

SIP tiene un cierto número de mecanismos de seguridad. Algunos de ellos se han incorporado directamente en el protocolo SIP, como la autenticación de HTTP. Estos mecanismos tienen algoritmos alternativos y parámetros. Se definen tres campos de la cabecera para negociar los mecanismos de seguridad dentro de SIP entre una entidad SIP Usuario Agente y su próximo salto al servidor SIP. Esta es una norma propuesta (RFC 3329) de la IETF. Cinco mecanismos están soportados actualmente:

- TLS
- Autenticación de HTTP
- IPsec con IKE
- IPsec manualmente codificado sin IKE
- S/MIME

4.2.6 Problemas de seguridad en SIP

La codificación del texto de SIP logra hacer más fácil su análisis usando herramientas estándares de análisis gramatical. Todavía, algunos nuevos requisitos son puestos en el firewall en una red VoIP basado en SIP. Primero, los firewalls deben ser stateful y monitor del tráfico de SIP para determinar qué puertos de RTP serán abiertos y que estarán disponibles con cada dirección. Esta responsabilidad es similar a la tarea de los firewalls en una red funcional basada en H.323, excepto la configuración de la llamada y el análisis de la cabecera es mucho más simple. Al igual que con H.323, el gran problema para SIP es NAT. Los problemas existen porque en una red basada en SIP, el

proxy SIP está normalmente fuera del dispositivo NAT. Hay tres situaciones principales para usar un proxy SIP:

- El proxy está dentro del LAN corporativo y el *Teleworker* conecta desde fuera.
- El proxy está en el lado del telecom y del lado del cliente, por ejemplo, compañías más pequeñas que conectan a este proxy para el servicio de VoIP.
- Se conectan dos dominios administrativos, los dos tienen su propio proxy.

Así que el problema está intercambiando comunicación entre un servidor proxy que trata con las direcciones IP globales y una máquina que había sido asignada a una dirección privada de red. *Rosenberg & Schulzrinne* clasifica tres *sets* diferentes de problemas que el tráfico SIP tiene en tal arquitectura: originando demandas, recibiendo demandas, y manejando RTP. Para inicializar una sesión desde detrás del NAT un llamador puede simplemente enviar un mensaje de INVITE como siempre. El número del puerto saliente (5060) será conservado por el NAT, pero la comunicación de la respuesta podría perturbarse. Si SIP es implementado encima de UDP el servidor proxy debe enviar la respuesta de UDP a la dirección y al puerto de donde llegó la demanda. Una solución más simple es usar la práctica estándar de ruteo SIP en la comunicación en TCP. Con TCP, la respuesta desde el llamador se unirá al mismo canal del INVITE original y de tal modo que NAT no presentará un problema.

Cuando un usuario contacta al registrador, ellos proporcionan su dirección IP como su dirección asequible y esto se guarda en el servidor de localización. Sin embargo, ésta es su dirección IP privada. El servidor Proxy trata solo con direcciones IP globales, así cuando un mensaje entra para username@dominio.com, intentará dirigir esta llamada a la dirección registrada, pero en el dominio público. Por ejemplo, si username@domain.com esta registrado a una dirección IP interior de 10.0.0.2, entonces el servidor Proxy intentará remitir el tráfico a esta dirección, pero en el dominio público. Esta dirección es inalcanzable para el servidor de Proxy y la conexión se negará. La solución a esto es una manipulación delicada de direcciones IP y una expansión de las responsabilidades del Servidor SIP Proxy.

CAPÍTULO 5: GATEWAYS

Los protocolos de control de media gateway abordan los requisitos de redes de telefonía IP que son desarrollados usando gateways VoIP "pacíficos". Los gateways pacíficos consisten en gateways de media (MGs) y controladores de Gateway de media (MGC), y aparecen al exterior como simples gateways de VoIP. MGC maneja la señalización de datos entre los MGs y otros componentes de la red como gatekeepers de H.323 o servidores SIP. MG se concentra en la función de traducción de señal de audio, llevando a cabo la conversión entre la señal de audio llevada sobre circuitos de teléfono y paquetes de datos llevados sobre la Internet o las otras redes de paquetes. Un solo MGC puede controlar a múltiples MGs, que da como resultado las reducciones de costo cuando se despliegan sistemas más grandes. Ejemplos comunes son el Media Gateway Control Protocol (MGCP) y Megaco/H.248, que se describen el las secciones siguientes.

5.1 Media Gateway Control Protocol (MGCP)

5.1.1 Vista general de MGCP

MGCP[3] es usado para comunicarse entre los distintos componentes de un gateway de VoIP pacífico. Es un protocolo complementario de SIP y H.323. En este momento, MGCP es el estándar de la industria y todavía no ha sido reemplazado por MEGACO/H.248.

5.1.2 Arquitectura del Sistema

Dentro de MGCP el servidor de MGC o "Agente de llamada" es obligatorio y este dirige las llamadas y las conferencias, y apoya los servicios suministrados. El MG endpoint es inconsciente de las llamadas y las conferencias y no mantiene estados de llamada. MGs son esperados para ejecutar los mandatos enviados por los agentes de llamada de MGC. MGCP asume que los agentes de llamada sincronizaran con otros enviando comandos coherentes para que MGs lo tenga bajo su control. MGCP no define

[3] Especificación establecida en el RFC 2705 de la ITU-T.

un mecanismo para sincronizar agentes de llamada. MGCP es un protocolo amo / esclavo con un acoplamiento entre el MG (punto final) y el MGC (servidor).

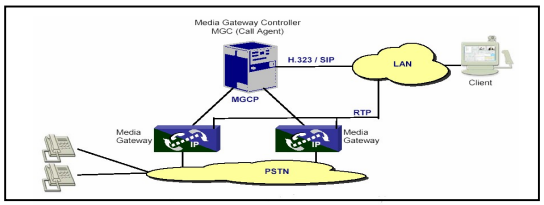


Figura 9: Escenario de MGCP

Los datos RTP son cambiados directamente entre los gateways de media involucrados. El agente de llamada usa MGCP para proveer los gateways con la descripción de los parámetros de enlace como direcciones IP, el puerto UDP y los perfiles de RTP. Estas descripciones siguen los acuerdos delineados en el protocolo de descripción de sesión (SDP). SDP[4] es un protocolo de descripción de sesión para sesiones multimedia, que también corre sobre conexiones de UDP.

5.1.3 Consideraciones de seguridad

No hay mecanismos de seguridad diseñados en el mismo protocolo MGCP. El informativo RFC 2705 hace referencia al uso de IPsec para proteger los mensajes de MGCP. Sin esta protección un atacante potencial podría permitir las llamadas no autorizadas o bloquear las llamadas en curso autorizadas. En comparación con el uso de IPsec, MGCP permite que el agente de llamada suministre gateways con claves de sesión que pueden ser usadas para encriptar los mensajes de audio, protegiéndose contra el problema de escuchar las llamadas. Las claves de sesión pueden ser usadas luego sobre la encriptación en RTP. Las claves de sesión pueden ser transferidas entre el Agente de llamada y el gateway usando el SDP.

5.2 Megaco/H.248

5.2.1 Visión General

En junio de 1999 la IETF MEGACO[5] WG y la ITU-T expusieron un documento que describía un protocolo estándar para conectarse entre el Media Gateway *Controllers* (MGCs) y el Media Gateways (MGs) MEGACO/H.248. Debido a que

[4] Descrito en el RFC 2327 de la ITU-T
[5] Descrito en el RFC 3525 de la ITU-T

MEGACO/H.248 es obtenido de MGCP, pueden ser encontradas muchas semejanzas, por ejemplo:

- Semejanza entre la semántica de los comandos en las dos especificaciones.
- El uso de gramática ABNF para la especificación de la sintaxis y el protocolo de descripción de sesión (SDP) para especificar las propiedades de flujo de media es el mismo de MGCP.
- El procesamiento de señales y eventos en el flujo de media es el mismo en MEGACO como en MGCP.
- La especificación de MEGACO para el transporte de mensajes sobre UDP es el mismo como se lo especifica en MGCP. El *three-way-handshake* y el cálculo de tiempos de retransmisión descritos en MGCP también son descritos dentro de la definición de MEGACO.

MEGACO/H.248 presenta algunos realces comparado con MGCP, incluyendo lo siguiente:

- El soporte de la multimedia y la conferencia multipunto aumentó sus servicios
- Opciones de transporte de TCP y UDP
- Admite texto o codificación binaria
- La definición ampliada de paquetes MEGACO se describió como la primera versión del protocolo de Control de Gateway dentro del RFC 3525.

5.2.2 Arquitectura de sistema

MEGACO/H.248 tiene la misma arquitectura básica de MGCP. Los comandos de MEGACO/H.248 son similares a los comandos de MGCP. Sin embargo, los modelos de protocolo son muy diferentes. MEGACO especifica un modelo de conexión de gateway de media que tiene dos entidades: Terminadores (origen o meta para (uno o más) flujos media), y contextos (grupo de terminadores conectados en una llamada). Por contraste, MGCP usa las siguientes dos entidades: puntos finales (origen o meta de los datos), y el enlace (asociación entre dos puntos finales).

Tomando una conferencia multipunto como un ejemplo, MEGACO simplifica la configuración de la conexión por terminadores adicionales para un contexto, mientras

que MGCP tiene que establecer algunas conexiones al servidor de conferencia. El contexto en este escenario puede abarcar múltiples flujos de media para mejorar los servicios de multimedia. Con MEGACO/H.248, el mecanismo principal para la extensión es por medio de los paquetes. En general, los paquetes de MEGACO/H.248 incluyen más detalle que los paquetes de MGCP. Estos definen propiedades adicionales y estadísticas junto con eventos y señales de información que podrían ocurrir en los terminadores

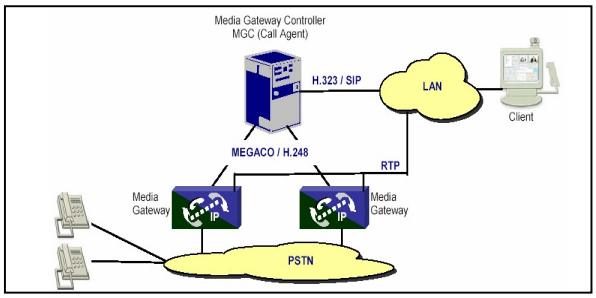


Figura 10: Escenario de MEGACO /H.248

5.2.3 Consideraciones de seguridad

MEGACO recomienda mecanismos de seguridad que pueden estar en mecanismos de transporte fundamentales, como IPsec. H.248 va un paso más lejos requiriendo que para la implementación del protocolo se implemente IPsec si el sistema operativo y la red de transporte lo permiten. H.248 expresa que la implementación empleará el encabezamiento de AH suministrando un conjunto mínimo de algoritmos para la integridad verificando el manual de uso de claves. El esquema interino de AH no provee protección contra la “escucha” y los ataques repetidos.

CAPÍTULO 6: FIREWALL, Traducción de direcciones, y el establecimiento de la llamada.

Los Firewalls y NAT representan un desafío temible en la implementación de VoIP. Es importante notar que los tres protocolos de VoIP más importantes, SIP, H.323, y H.248/MEGACO tienen problemas similares con firewalls y NATs. Aunque el uso de NATs podría ser reducido cuando IPv6 es asumido, pero este no aliviará la necesidad para firewalls así que los sistemas de VoIP deberán arreglárselas con la complejidad de firewalls y NATs.

6.1 Firewalls

Los firewalls son una constante de seguridad en las redes IP de hoy. Protegiendo una red de área local LAN, la red de área extensa WAN o simplemente protegiendo una sola computadora, un firewall es generalmente la primera línea de defensa en contra de una serie de ataques. Los firewalls trabajan impidiendo el tráfico considerado invasor, intruso, o simplemente malicioso que circula a través de ellos. El tráfico que no cubre los requisitos del firewall es retirado. El procesamiento del tráfico es determinado por un set de reglas programadas en el firewall por el administrador de la red. Estos podrían incluir tales comandos como el "Bloqueo de todo el tráfico de FTP (puerto 21)" o "Admitir todo tráfico de HTTP (puerto 80)".

Una propiedad útil de un firewall es que provee una ubicación central para desplegar las políticas de seguridad. Este es el obstáculo final para el tráfico de la red porque cuando se diseña apropiadamente, ningún tráfico puede entrar o salir de la LAN sin pasar por el firewall. Esta situación se presta a si misma para la red de VoIP donde los firewalls simplifican la administración de seguridad consolidando las medidas de seguridad en el firewall, en lugar de requerir que todos los puntos finales de la red mantengan políticas de seguridad actualizadas. Esto quita una carga enorme a la infraestructura de red de VoIP. La introducción de un firewall en la red de VoIP complica diversos aspectos de esta red, más notablemente el tráfico del puerto dinámico y el procedimiento de configuración de llamada.

Firewall Stateful y Stateless

La mayoría de tráfico de VoIP viaja por los puertos de UDP. Los firewalls típicamente procesan este tráfico usando una técnica llamada filtrado de paquetes, este investiga los encabezamientos de cada paquete que intenta cruzar el firewall y usa la dirección IP, el número de puerto y el tipo de protocolo contenidos allí para determinar la legitimidad del paquete. En VoIP y otros protocolos de transmisión de media esta información también puede ser usada para distinguir entre el inicio de una conexión y una conexión establecida.

Existen dos tipos de filtrado de paquetes de los firewalls, stateless y stateful.
Los Firewall stateless no conservan memoria del tráfico que ha ocurrido antes en la sesión. Los Firewalls stateful recuerdan el tráfico previo y también pueden investigar los datos de aplicación en un paquete. Por lo tanto los firewalls stateful pueden manejar el tráfico de aplicación que no podría estar asignado a un puerto estático.

6.1.1 Firewall específico necesitado para VoIP

Además de las prácticas estándar de un firewall, estos son a menudo desplegados en una red VoIP con la responsabilidad adicional de actuar como intermediario del flujo de datos entre la voz y los segmentos de datos de la red. Esto es una funcionalidad crucial para una red que contiene teléfonos IP basados en una PC que están en la red de datos, pero necesitan enviar mensajes de voz. Todo el tráfico de voz que emanaría o viajaría por tales dispositivos tendría que ser explícitamente aceptado si ningún firewall estuviera presente porque RTP utiliza puertos dinámicos de UDP. Dejar muchos puertos UDP abiertos es un incumplimiento atroz de la seguridad. Por lo tanto, es recomendable que todos teléfonos basados en PC sean colocados detrás de un firewall stateful para que este actúe como intermediario del tráfico de media de VoIP. Sin tal mecanismo, un ataque a UDP podía comprometer la red explotando la abundancia de puertos abiertos. *Halpern* identifica algunos de los puntos claves de colisión entre la voz y el tráfico de datos donde los firewalls son necesarios, incluyendo:

- Teléfonos IP basados en PC (datos) requiriendo acceso para el segmento (voz) para un rango de llamadas, permiso de mensajes, etcétera.
- Teléfonos IP y call manager (voz) accediendo al correo de voz (datos),

- El servidor Proxy (voz) accediendo a los recursos de la red (datos)
- El tráfico de los teléfonos IP (voz) para el director de procesamiento de llamada (voz) o servidor proxy (voz) debe pasar a través de un firewall.

6.2 *Network Address Translation* (NAT)

Network Address Translation (NAT) es una herramienta que puede ser usada para esconder direcciones de red internas y permitir algunos puntos finales dentro de una red de área local compartiendo la misma dirección IP (externa). NAT tiene las siguientes características:

- Asignación transparente de direcciones.
- Encaminamiento transparente mediante la traducción de direcciones.
- Traducción de la carga útil de los paquetes de error.

En NAT los encabezamientos de IP salientes son cambiados de direcciones de red de área local privadas a direcciones IP globales. Los encabezamientos de protocolo TCP / UDP también son cambiados mediante NAPT (traducción de dirección y puerto). Esto permite que algunas computadoras compartan simultáneamente la dirección IP global. También, computadoras que no necesitan acceder a la Internet puedan tener asignadas direcciones locales en la intranet sin producir conflictos o innecesariamente adoptar una dirección de IP. NAT también colabora indirectamente con la seguridad de una red de área local, haciendo que las direcciones IP internas sean menos accesibles desde la Internet pública.

Por lo tanto, todos los ataques en contra de la red deberían ser enfocados al router NAT. De la misma manera que un firewall, este provee seguridad porque solamente un punto de acceso debe ser protegido. La abstracción de la LAN de la Internet a través de un NAT también simplifica el manejo de la red. Por ejemplo, si uno decidiera cambiar su ISP, solamente la configuración del router externo necesitaría ser cambiada. La red interna y el plan de direccionamiento podrían ser dejados intactos.

Cono lleno de NAT (*Full Cone* NAT)

Un *Full Cone* NAT es donde todas solicitudes de la misma dirección IP interna y puerto son asignadas a la misma dirección IP externa y puerto. Además, cualquier host externo

puede enviar un paquete a un host interno, enviando un paquete a la dirección externa asignada.

Cono restringido de NAT (*Restricted Cone* NAT)

Cono restringido NAT es donde todas solicitudes de la misma dirección IP interna y puerto son asignadas a la misma dirección IP externa y puerto. A diferencia de un cono lleno de NAT, un host externo (con dirección IP: X) puede enviar un paquete al host interno sólo si el host interno habría enviado antes un paquete a la dirección IP: X.

Cono de puerto restringido (*Port Restricted Cone*)

Un *port restricted cone* NAT es como un *restricted cone* NAT, pero la restricción incluye los números de puerto. Específicamente, un host externo puede enviar un paquete, con dirección IP X y puerto de origen P, al host interno sólo si este habría enviado antes un paquete a la dirección IP X y al puerto P. Esto es usado para permitir el compartimiento de direcciones IP externas.

NAT simétrico (*Symmetric* NAT)

NAT simétrico es donde todas solicitudes de la misma dirección IP interna y puerto, a una dirección IP específica y puerto, son asignadas a la misma dirección IP externa y puerto. Si el mismo host envía un paquete con la misma dirección de origen y puerto, pero a un destino diferente, una asignación diferente es usada. Además, solamente el host externo que recibe un paquete puede enviar un paquete de UDP al host interno. Este diseño tiene implicaciones importantes para VoIP. En primer lugar, un intento de hacer una llamada en la red es muy complicado cuando un NAT esta presente. La situación es parecida a una red telefónica donde algunos teléfonos tienen el mismo número de teléfono.

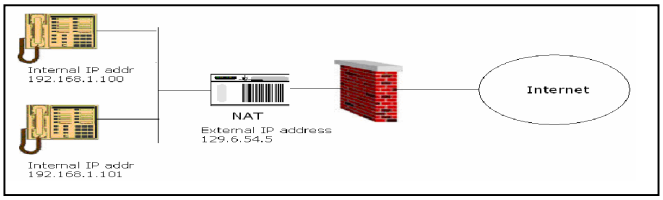


Figura 11: Teléfonos IP detrás de un NAT y un Firewall

6.3 Firewalls, NATs, y Temas de VoIP

Algunos asuntos de VoIP con firewall y NATs están desvinculados del protocolo de configuración de llamadas usado. Ambos dispositivos de la red hacen difícil para las llamadas entrantes ser recibidas por una Terminal detrás del firewall / NAT. Las siguientes secciones describen estos asuntos específicos.

6.3.1 Llamadas entrantes

Sin considerar el protocolo usado para la configuración de llamada, los firewalls y NATs ponen en apuros considerables a las llamadas entrantes. Admitir el tráfico de la señal a través de un Firewall de una llamada entrante implica dejar varios puertos abiertos que pueden ser explotados por atacantes. Una cuidadosa administración y definiciones de reglas deberían ser usadas si existen hoyos cuando un firewall admite conexiones entrantes.

NAT crea aún más dificultades para las llamadas entrantes. Cualquier aplicación de IP, incluyendo VoIP, que tenga que hacer un enlace desde el ambiente externo a una posición detrás de un NAT, necesitaría saber el IP externo de esta posición y el número de puerto asignado por el router. Esta situación esta lejos de un modelo de perfección porque impide a un llamador de fuera del NAT llegar a una dirección interna excepto en circunstancias extremas. A decir verdad, estar con puertos dinámicos asignados por NAT, es casi una situación imposible porque el puerto en que el llamador requiere podría ser cambiado por el NAT. Para puntos finales detrás de firewalls y NATs, podría ser necesario divulgar la dirección de contacto para permitir que a otros clientes los llamen.

6.3.2 Efectos sobre la Calidad de Servicio QoS

Tantos Firewalls como NATs pueden degradar la calidad de servicio (QoS) en un sistema de VoIP introduciendo latencia y jitter. NATs también puede actuar como un embotellamiento en la red porque todo tráfico es encaminado a través de un solo nodo.

VoIP es muy susceptible a la latencia. Así que un Firewall tiene que poder actuar como intermediario de tráfico de los datos, pero puede incurrir en penas de tiempo de cualquier longitud importante.

Dos aspectos de VoIP pueden causar el comportamiento degradado en el Firewall. Primero, el proceso de *call setup* tiene que ser echo usando H.323 o SIP. Sin considerar el protocolo usado, los firewalls tienen que "Excavar profundamente" en estos paquetes para determinar su validez. Un torrente de paquetes de petición de llamadas, como el resultado de un aumento en el volumen de llamadas o un ataque malicioso, puede intensificar este efecto. La presencia de un NAT agrava este asunto porque el *payload* del paquete debe luego ser cambiado en el nivel de aplicación para corresponder la traducción de origen NAT o la dirección de destino y puertos, requiriendo no sólo "Cavar" sino también llenar el hoyo con nueva "basura". Todo este trabajo pone una carga tremenda sobre el procesador del Firewall, que debe hacer todas estas tareas mientras introduce un mínimo indispensable de latencia, especialmente si las medidas de protocolo de seguridad son usadas, como la integridad de mensaje.

El otro aspecto de VoIP que puede poner una resistencia sobre la CPU de un Firewall es que es pequeña para el número abundante de paquetes RTP que levantan una conversación de VoIP. Los firewall son raramente preocupados por el tamaño de un paquete, pero debido a que cada paquete debe ser inspeccionado, muchos paquetes pueden ser sometidos al firewall. Firewalls de QoS para VoIP son diseñados para evitar problemas de rendimiento como éstos. Como sea la rapidez de la conexión de la red, el CPU del firewall es un obstáculo para todos paquetes de la red no encriptados. Por lo tanto, una solución para este asunto es usar una *Virtual Private Network* (VPN) para todo tráfico de VoIP.

6.3.3 Firewalls y NATs

Los firewalls tienen problemas para revisar completamente el tráfico de señal de VoIP. Hay soluciones para esto pero hay un problema adicional, y aun más irritante relacionado con firewalls y la media de VoIP. En el tráfico RTP es asignado un par de números de puerto del rango de puertos de UDP (1024-65534). Además, el puerto de RTCP que controlará esta secuencia circulará a través de un puerto asociado asignado al

azar. Admitir tal tráfico a lo largo de tal número inmenso de puertos por *default* podría dejar el sistema muy expuesto. Así que los firewalls deben estar dinámicamente conscientes de que puertos de media están circulando a través y entre cuales terminales. Por esta razón, solamente firewalls stateful que pueden procesar H.323 y SIP deben ser incluidos en la red para abrir y cerrar puertos. Muchos firewalls nuevos vienen equipados con tal funcionalidad, aunque a veces soportan solamente un protocolo (H.323 o SIP). Si tales firewalls no están disponibles o viables, existen soluciones disponibles de hardware adicionales, o VPNs pueden ser usadas para hacer un túnel a través del firewall.

Antes que nada, la práctica del estándar NAT debe asignar nuevos números de puerto al azar destruyendo la relación de pareja de RTP y los números de puerto de RTCP. La traducción de direcciones IP y puertos por NAT es también problemática para la recepción de paquetes de VoIP. Si el router NAT no procesa el tráfico apropiadamente, las nuevas direcciones / puertos no corresponderán a aquellas negociadas en el proceso de instalación de llamada (*CALL SETUP*). En este ambiente, el gateway de VoIP no podría repartir apropiadamente los paquetes de RTP. El problema es agravado si ambos participantes de la llamada están detrás de NATs.

El uso de NATs añade otra complicación posible a señal de llamada de VoIP debido a la naturaleza finita de enlaces NAT. En un NAT, una dirección IP publica esta unida a una privada por un cierto periodo de tiempo (t). Esta notación se podría eliminar si ningún tráfico fuera observado en NAT en un periodo de tiempo "t" o si el enlace fuera roto explícitamente. Además, podría existir un periodo de silencio durante una conversación que llegara a ser más largo que un periodo de tiempo t, pero el no recibir tráfico en un tiempo t no es suficiente indicador para demostrar la finalización de una sesión. Por consiguiente, es posible que algo de información de estado sea destruido antes de que la negociación y/o la llamada terminen en realidad.

6.4 CALL SETUP: Consideraciones importantes en Firewalls y servidores NAT

Los usuarios de VoIP podrían no tolerar excesiva latencia en el proceso de instalación de llamada (CALL SETUP), que corresponde a levantar el auricular y discar el numero en un sistema tradicional. Los usuarios podrían estar molestos con un proceso de

instalación que requiera más que unos pocos segundos. Muchos factores influyen en el tiempo de instalación de una llamada de VoIP: En el nivel de red incluye la topología y la ubicación de ambos puntos finales tanto como la presencia de un firewall o NAT. En el nivel de aplicación, el grado o la falta de la autentificación y otras medidas de seguridad de datos, también como la opción del protocolo usado para la configuración de la llamada, pueden modificar dramáticamente el tiempo necesario para preparar una conexión de VoIP.

6.4.1 Niveles de Aplicación de Gateways

Los niveles de aplicación de Gateway (ALGs) son la típica solución comercial para el problema de firewalls / NAT. Un ALG es un software empotrado sobre un firewall o NAT, que permite una configuración dinámica basado en aplicaciones de información específica. Un Firewall con un ALG puede analizar y comprender H.323 o SIP, y abrir o cerrar los puertos necesarios dinámicamente. Cuando NAT está siendo empleado, el ALG tiene que abrir los paquetes de VoIP y reconfigurar la información de la cabecera para allí corresponder la correcta dirección IP interna en la red privada, o en la red pública para el tráfico saliente. Esto incluye modificar los encabezamientos y los cuerpos de mensaje en H.323 y SIP. El problema de NAT es aliviado cuando el ALG reemplaza las direcciones de la red privada con la misma dirección del ALG. Este trabaja no sólo cambiando la dirección IP sino también mapeando el tráfico de RTP en puertos de los que el ALG puede leer y enviar a la maquina interna correcta. La necesidad de puertos consecutivos para RTP y RTCP puede causar un problema aquí porque todo tráfico de VoIP en la red (y tráfico de datos también) estarían siendo encaminado a través del ALG así que con los aumentos de volumen de llamadas, encontrar suficientes puertos consecutivos podría ser un problema. Así que aunque ambos puntos finales podrían tener puertos adecuados para realizar una conversación, las deficiencias de los firewalls podrían causar que la llamada sea rechazada como "Ocupado" por el mismo ALG. Aun así con todos estos inconvenientes, un ALG es el más simple y seguro modo indirecto para permitir la coexistencia de VoIP, firewalls, y NAT.

6.4.2 Soluciones Middlebox

Una desventaja para ALGs es que son adaptados en el mismo firewall, y por lo tanto, la latencia y el retraso de throughput de todo tráfico que atraviesa el firewall es adicionado y luego empeorado por el volumen de llamadas de VoIP. Las soluciones del estilo *Middlebox* intentan aliviar este mal poniendo un dispositivo adicional fuera del firewall que efectúa muchas de las funciones relacionadas con un ALG. El dispositivo de la que la aplicación inteligente es extraída puede ser un sistema de "En la ruta" (*In Path*) como un gatekeeper de H.323 o SIP proxy que se encuentra en la ruta de control de la sesión y es considerado ser un "Sistema de confianza" que analiza el tráfico de VoIP y ordena al firewall que abra o cierre puertos basado en las necesidad de señalización de VoIP vía un protocolo *midcom*. Resumir la inspección de *stateful* y la manipulación de la señalización de paquetes de los NATs y firewalls (*middleboxes*) mejorará la escalabilidad y a la larga, reducirá el costo de actualizar la red para no tener que reemplazar el firewall cada vez que los protocolos cambien. También hay una mejora de rendimiento que viene de resumir dos tareas muy intensivas del procesador (análisis de VoIP y filtrado de paquetes).

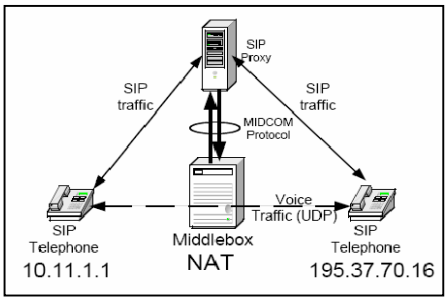


Figura 12: Escenario de comunicaciones Middlebox

6.4.3 Session Border Controllers

Mientras los ALGs pueden tener las funciones de escalabilidad, las soluciones de *middlebox* no han encontrado su manera fuera de los estándares y en productos comerciales tan rápido como pudo haber sido esperado. En ausencia de una solución universalmente aceptada para los asuntos relacionada con el firewall / NAT, los desarrolladores de productos han traído al mercado una solución que ha llegado a ser conocida como un controlador de sesión, o un controlador de borde de sesión (SBC).

SBCs son aparatos dedicados que brindan uno o más de los siguientes servicios para un perímetro de VoIP: Firewall / NAT, el control de admisión de llamada (*Call Admisión Control*), monitoreo de contrato de nivel del servicio (*Service Level Agreement Monitoring*), y protocolo interworking (*protocol interworking*).

6.5 Mecanismos para solucionar el problema de NAT

Especialmente para protocolos de comunicación en tiempo real como H.323 y SIP, NAT causa problemas porque estos protocolos incluyen la dirección IP en sus mensajes. Para la protección de integridad el dispositivo de NAT tendría que ser un host intermedio de confianza para recalcular la verificación de la integridad. Desde un punto de vista de seguridad de end–to–end esto no es recomendable. Por lo tanto la siguiente sección describe mecanismos para manejar el problema de NAT de manera diferente.

6.5.1 Simple Traversal de UDP a través de NATs (STUN)

Simple Traversal de UDP a través de NATs (STUN) es un protocolo ligero que permite que las aplicaciones descubran la presencia y los tipos de NATs y firewall presentes entre ellos y la Internet pública. También provee la capacidad a las aplicaciones de determinar las direcciones IP públicas asignadas a ellos por el NAT. STUN trabaja con muchos NATs existentes, y no requiere ningunos cambios para NATs. STUN no trabaja con NAT simétricos, porque la asignación del puerto de la dirección IP está en función del destino.

6.5.2 Traversal Usado en Relay NAT (TURN)

Traversal usado en Relay NAT (TURN) es un protocolo que permite a un elemento detrás de un NAT o Firewall recibir los datos entrantes de conexiones TCP o UDP para complementar las limitaciones de STUN. El servidor TURN actuaría como una carrera de relevos de datos, recibiendo los datos sobre la dirección que provee a los clientes, y enviándolos a los clientes. TURN es idéntica en la sintaxis y la operación general a STUN, pero asigna direcciones de transporte enlazadas. A diferencia de un servidor STUN, un servidor TURN provee recursos (ancho de banda y puertos) a clientes que se

conectan hacia él. Por lo tanto, solamente clientes autorizados pueden acceder al servidor TURN. El cliente usa un secreto compartido para autentificarse a si mismo en una solicitud enviada sobre TLS. La respuesta confidencial compartida que suministra el cliente contiene un nombre de usuario único y su contraseña. Esta contraseña luego es usada para autentificar el mensaje de asignación enviado por el cliente al servidor TURN para preguntar por una dirección IP pública y el puerto. Para los datos entrantes, el servidor TURN guarda la dirección remota y el puerto desde dónde vinieron los datos y envía los datos al cliente. El servidor TURN es responsable de garantizar que los paquetes enviados a la dirección IP pública se encaminen por el servidor TURN.

6.6 *Virtual Private Networks* y Firewalls

Las VPNs alivian muchos de los asuntos de los problemas tratados haciendo tunneling a través de firewalls. Sin embargo, este método "Ordinario" tiene algunas desventajas. Primero, hacer tunneling de todo el tráfico de VoIP sobre VPNs prohíbe el uso de firewall de investigación de tráfico malicioso entrante y saliente. También, la centralización de seguridad en el firewall es prácticamente perdida. También, VPN tunneling con IPsec puede ser incompatible con NAT.

CAPÍTULO 7: ENCRIPTACION E IPsec

Firewalls, gateways, y otros dispositivos pueden ayudar a impedir a los intrusos comprometer una red, pero los firewalls no son ninguna defensa contra un hacker interno. En VoIP, como en las redes de datos, esto puede ser logrado encriptando los paquetes a nivel IP usando IPsec. De esta manera si cualquiera en la red, autorizado o no, intercepta tráfico de VoIP no prometido a ellos (por ejemplo con un Sniffer), estos paquetes serán ilegibles. La colección IPsec de protocolos de seguridad y algoritmos del encriptación es el método estándar para asegurar paquetes contra los espectadores desautorizados encima de las redes de datos y será soportada por la pila protocolar en IPv6.

Varios factores, incluso la expansión de tamaño del paquete, que cifran latencia, y una falta de urgencia de QoS en el propio motor de criptografía puede causar una cantidad excesiva de latencia en la entrega de paquetes VoIP. Esto lleva a degradar la calidad de voz, así una vez más hay un trueque entre seguridad y calidad de voz, y una necesidad de velocidad. Afortunadamente, las dificultades no son insuperables. Pruebas muestran que IPsec puede incorporarse en una red SIP con aproximadamente unos tres segundos de retardo adicional en tiempo de configuración de llamada, un retardo aceptable para muchas aplicaciones. Esta sección explica los problemas abarcados con éxito incorporando encriptación de IPsec en los servicios de VoIP.

7.1 IPsec

IPsec[6] es la forma preferida de tunneling VPN a través del Internet. Los componentes fundamentales de la arquitectura de seguridad IPSec son los siguientes:

- Protocolos de Seguridad: Autenticación de cabecera (AH) y seguridad de Encapsulamiento de Carga Útil (ESP).
- Asociaciones de Seguridad.
- Manejo de Clave: manual y automática (Internet Key Exchange, IKE).
- Algoritmos para la autenticación y encriptación.

Los protocolos de seguridad de Encapsulamiento de Carga Útil (ESP) y la Autenticación de la Cabecera proporcionan integridad sin conexión, autentificación del

[6] El RFC 2705de la ITU-T hace referencia al uso de IPsec

origen y un servicio de anti-repetición. IPsec también soporta dos modos de entrega: Transporte y Túnel. El modo de transporte encripta la carga útil (datos) y cabeceras de la capa superior en el paquete IP. La cabecera de IP y la nueva cabecera de IPsec se quedan fuera del plano. Así si un atacante interceptó un paquete en modo de transporte, ellos no podrían determinar lo que contuvo; pero ellos podrían decir qué partes se conectaron, cuando, y por cuánto tiempo. El modelo Túnel encripta todo el datagrama IP y lo coloca en un nuevo paquete IP. La carga útil y la cabecera de IP son encriptadas. La cabecera de IPsec y la nueva cabecera de IP para este paquete encapsulando son la única información de salida sin sospecha.

7.2 El rol de IPsec en VoIP

La facilidad de capturar un paquete en una red basada en IP ocasiona la necesidad de encriptar VoIP. La seguridad en VoIP preocupa tanto a la persona que escucha como a la persona que esta hablando. La incorporación de IPsec en IPv6 aumentará la disponibilidad de encriptación. VoIPsec (VoIP usando IPsec) ayuda a reducir la amenaza de ataques en puntos medios, captura de paquetes, y muchos tipos de análisis de tráfico de voz. Combinado con las implementaciones de un firewall, IPsec hace de VoIP más seguro que una línea telefónica normal. Es importante anotar, sin embargo, que IPsec no siempre es apropiado para algunas aplicaciones así que algunos protocolos continúan confiando en sus propias características de seguridad.

7.3 Dificultades que surgen en VoIP

IPsec ha sido incluido en IPv6. Es un fiable, robusto, y ampliamente implementado método de protección de datos y de autentificación del remitente. Sin embargo, hay varios problemas asociados con VoIP que no es aplicable al tráfico normal de datos. De interés particular son los problemas en Calidad de Servicio (QoS). Entre éstos esta la latencia, jitter, y pérdida de paquetes. En una transferencia normal de datos sobre TCP, si un paquete se pierde, este puede ser reenviado a petición. En VoIP no hay tiempo para esto. Los paquetes deben llegar a su destino y deben llegar rápido. Por supuesto los paquetes también deben estar seguros durante sus viajes, de aquí la introducción de VoIPsec. Sin embargo, el precio de esta seguridad es una baja decisiva en QoS causado por varios factores.

7.4 Encriptación / Desencriptación: Latencia

Estudios realizados revelaron a la máquina de criptografía como un cuello de botella para tráfico de la voz transmitido sobre IPsec. Se estableció un experimento controlado para medir el efecto de encriptación y desencriptación en el *throughput*. Se probaron cuatro algoritmos de criptografía en una red totalmente dedicada para VoIP usando el mismo tráfico como una referencia. Los resultados mostraron que computacionalmente los algoritmos más ligeros lograron mejor *throughput* que los más pesados. La latencia de encriptación/desencriptación es un problema para cualquier protocolo de criptografía, porque mucho de él es el resultado del tiempo de cómputo requerido por el encriptamiento.

7.5 Tamaño del Paquete extendido

IPsec también aumenta el tamaño de paquetes en VoIP que lleva a más problemas de QoS. Se ha mostrado que aumentando el tamaño del paquete aumenta el *throughput*. La diferencia es que el aumento en tamaño del paquete debido a IPsec no produce una capacidad de la carga útil aumentada. El aumento es realmente es en el tamaño de la cabecera debido al encriptamiento y encapsulación de la vieja cabecera de IP y la introducción de la nueva cabecera de IP y la información de encriptación. Esto lleva a varias complicaciones cuando IPsec se aplica a VoIP. Primero, el ancho de banda eficaz se disminuye tanto como un 63%. Así las conexiones los usuarios en áreas de bajo ancho de banda (es decir vía módem) puede volverse impracticable. La diferencia del tamaño también puede causar problemas de latencia y jitter.

7.6 Incompatibilidad de IPsec y NAT

NAT invalida el propósito de AH completamente porque la dirección origen de la máquina detrás del NAT se enmascara del mundo externo. Así, no hay ninguna manera de autenticar al verdadero remitente de los datos. Hay varios otros problemas que se levantan cuando el tráfico de ESP intenta cruzar un NAT. Si solo uno de los puntos finales está detrás de un NAT, la situación es más fácil. Si ambos están detrás de un NAT, la negociación de IKE puede usarse, con encapsulamiento UDP de los paquetes de IPsec.

CAPITULO 8: SOLUCIONES PARA LOS ASUNTOS DE VoIPsec

Hasta ahora, se ha planteado varios asuntos importantes con el rol de IPsec en VoIP. Sin embargo, muchos de estos problemas técnicos son resolubles. A pesar de la dificultad relacionada con estas soluciones es digno del establecimiento de una implementación de VoIPsec.

Nota: El Anexo 4 contiene un resumen de riesgos, ataques y vulnerabilidades de VoIP así como su forma de prevenirlos.

8.1 Encriptación en los puntos finales de la red

Una solución propuesta atribuible a los asuntos de encriptación fuera el manejar la encriptación / desencriptación únicamente en los puntos finales en la red de VoIP. Una consideración con este método es que los puntos finales deben ser computacionalmente fuertes lo suficiente para tratar con el mecanismo de encriptación. Pero típicamente los puntos finales son menos fuertes que los gateway. Aunque idealmente la encriptación debe ser mantenida en cada salto del tiempo de vida de un paquete en VoIP, esto no podría ser viable con los teléfonos IP simples con poco poder computacional. En tal caso, podría ser preferible para los datos sean cifrados entre el punto final y el router, pero el tráfico no encriptado sobre la LAN es ligeramente menos perjudicial que el tráfico no encriptado a través de la Internet. Afortunadamente, el incremento de poder de procesamiento de teléfonos más nuevos está haciendo menos encriptación en los puntos finales.

8.2 Secure Real Time Protocol (SRTP)

Sin protección RTP es considerado inseguro. Adicionalmente, la manipulación y repetición de los datos de RTP podrían resultar en una mala calidad de voz debido a que colma la secuencia de audio / video. El protocolo de tiempo real seguro (SRTP) es un perfil del protocolo de transporte de tiempo real (RTP) que brinda no sólo la confidencialidad sino también la autentificación de mensaje, y la protección de repetición para el tráfico de RTP como para RTCP. SRTP provee un marco para la encriptación y la autentificación de mensaje de RTP y flujos de RTCP. SRTP puede

conseguir un *throughput* alto y una baja expansión de paquetes. Las ventajas sobre el estándar de seguridad de RTP y también sobre la seguridad de H.235 para la secuencia de datos de media se encuentran a continuación.

SRTP provee un incremento en la seguridad, conseguido por:

- Confidencialidad tanto para RTP como para RTCP para la encriptación de las respectivas cargas útiles;
- La integridad para RTP y paquetes de RTCP, junto con la protección de repetición;
- La posibilidad de regenerar la sesión de claves periódicamente, que limita la cantidad del texto cifrado causada por una clave fija;
- Un marco extensible que permite actualizarse con los nuevos algoritmos criptográficos;
- Seguridad para aplicaciones RTP *unicast y multicast*.

SRTP ha mejorado el rendimiento conseguido por:

- Bajo costo computacional echo por algoritmos pre definidos;
- Bajo costo de ancho de banda y un *throughput* alto por la expansión de paquete y por un marco que mantiene la compresión del encabezado de RTP;

8.3 Dirección de claves para SRTP – MIKEY

SRTP usa un conjunto de parámetros de negociación de los que las claves de sesión para la encriptación, la autentificación y la protección de integridad son obtenidas. MIKEY describe un esquema de manejo de claves que aborda los guiones de multimedia de tiempo real. También soporta la negociación de sesiones simples y múltiples de criptografía. MIKEY soporta la negociación de claves criptográficas y parámetros de seguridad (SP) para uno o más protocolos de seguridad.

MIKEY tiene algunas propiedades importantes:

- Puede ser implementado en una biblioteca de software independiente para ser integrado fácilmente en un protocolo de comunicación multimedia.
- Existen cuatro alternativas para la distribución de claves:
    - Claves pre compartidas.

- Encriptación de claves públicas.
- El intercambio de claves Diffie - Hellman protegidas por la encriptación de claves públicas.
- El intercambio de claves Diffie - Hellman protegidas con claves pre establecidas y funciones *keyed hash* (usando una extensión de MIKEY).

8.4 Una mejor planificación

La incorporación de AES o algún otro rápido algoritmo de encriptación podrían ayudar temporalmente a alivianar el obstáculo, pero esto no es una solución escalable porque no aborda el grado de causa más alto del retardo. Sin una manera para el proceso de criptografía para priorizar paquetes, esta todavía será propensa a los ataques de DoS y debilidades de tráfico de datos que impedirá el tráfico de VoIP en tiempo - urgente. Algunos paquetes grandes pueden obstruir la larga cola de espera haciendo que los paquetes de VoIP se tarden mas de lo debido. Una de las soluciones que se implementó en los más recientes routers es programar los paquetes con QoS en mente antes de la fase de encriptación.

Priorizar QoS también puede ser hecho después del proceso de encriptación siempre que sus procedimientos mantengan los bits de ToS de la cabecera original de IP en la nueva cabecera de IPsec. Esta funcionalidad no está garantizada y está en función de varios equipos físicos de la red y software, pero si es implementado admite que la planificación de QoS sea usada en cada salto de paquetes cifrados encontrados.

8.5 Compresión del tamaño de paquete

Otra solución para los asuntos de QoS relacionados con VoIPsec es propuesto por *Barbieri et al.*, esta se centra en el aumento del tamaño del paquete que proviene del uso de IPsec. Aquí se implementó cIPsec: una versión de IPsec que comprime el encabezamiento interno de un paquete bajando a aproximadamente cuatro bytes. Esto es posible porque gran parte de los datos en la cabecera interna de un paquete se quedaba constante o se duplicaban en la cabecera exterior.

Los resultados de pruebas iniciales publicados en la universidad de Milán indican que la compresión de las cabeceras de IPsec resulta en el uso de ancho de banda comparable con IP simple. Esto da como resultado considerablemente menos fluctuación (jitter) y latencia. El rendimiento del procesador de criptografía también mejora. Por supuesto, hay un precio para estos incrementos de producción. El esquema de compresión pone más esfuerzo en las capacidades de CPU y memoria de los puntos finales pertinentes para conseguir la compresión, y, por supuesto, ambos finales de un enlace deben usar el mismo algoritmo de compresión. Sin embargo, el estudio encontró que el tiempo perdido en la compresión fue ganado en la fase de encriptación, cuando el procesador de criptografía es más eficiente con los paquetes comprimidos. Una cosa que no consideraron es el tremendo esfuerzo puesto en el CPU del punto final a diferencia del procesador de criptografía. El CPU del punto final podría ser computacionalmente lento o puede estar llevando a cabo muchas más operaciones que sólo VoIP. En cualquiera de los dos casos, el tiempo verdadero requerido para llevar a cabo la compresión podría tomar mucho más de lo asignado en el procesador de criptografía. Es importante notar que el esquema de compresión usado en cIPsec solamente comprime la información de la cabecera de paquete.

8.6 Resolución de incompatibilidades de NAT / Ipsec

Hay soluciones para los problemas incompatibilidad de IPsec / NAT. Aquí se habla de varios de estas, incluyendo *Realm-Specific* IP (RSIP), IPv6 *Tunnel Broker*, IP *Next Layer* (IPNL), y encapsulación de UDP.

RSIP es diseñado como un reemplazo para NAT y provee un túnel despejado entre hosts y el Gateway de RSIP. RSIP soporta tanto AH como ESP, pero implementar RSIP podría requerir una revisión importante de la arquitectura de red de área local en curso así que mientras sea totalmente una solución elegante, es actualmente impracticable.

El método IPv6 tunnel broker usa un túnel de IPv6 como un túnel IPsec, y encapsula un paquete IPv6 en un paquete IPv4. Pero esta solución también requiere versiones actualizadas de LAN y no trabaja en las situaciones donde múltiples NATs son usados.

IPNL introduce una nueva capa en los protocolos de la red entre IP y el protocolo TCP / UDP para solucionar el problema, pero IPNL está en competencia con IPv6 e IPv6 es un estándar mucho más usado.

La solución generalizada más probable para el problema de NAT traversal es la encapsulación de UDP de IPsec. Esta puesta en práctica admite todo tráfico de ESP para atravesar el NAT. En modo de túnel, este modelo envuelve el paquete encriptado de IPsec en un paquete de UDP con una nueva cabecera IP y una nueva cabecera UDP. El campo de SPI dentro del paquete encapsulado de UDP es puesto en cero para diferenciarlo de una comunicación de IKE. Esta solución admite paquetes de IPsec para atravesar estándares NATs en ambas direcciones. La aprobación de este método estándar debe admitir el tráfico VoIPsec para atravesar NATs, aunque un poco de sobrecarga adicional es añadido en el proceso de encapsulación / desencapsulación. El problema todavía persiste en IP basado en la autentificación de paquetes que puede ser segura al otro lado de NAT, pero el uso de un secreto compartido negociado a través de IKE podría proveer la autentificación.

8.7 Seguridad en las Comunicaciones IP

Las Comunicaciones IP permiten a las empresas implementar redes convergentes, donde los servicios de voz, video y datos son provistos sobre la red IP de una manera segura, generando beneficios tales como la reducción de costos y aumento de la productividad de los empleados.

Cuando nos protegemos contra los tipos de vulnerabilidades comunes de voz y sistemas relacionados a la voz, es importante considerar tres componentes críticos:

- Privacidad: Provista vía comunicaciones seguras. Tecnologías como IP *Security* (IPSec) nos permiten implementar *Virtual Private Networks* (VPNs) seguras que nos ayudan a robustecer las comunicaciones tanto en la LAN como en la WAN.
- Protección: Provista por sistemas de defensa contra amenazas. Tecnologías como los firewalls, gatekeepers combaten las amenazas originadas interna y externamente.

- Control: Provisto vía sistemas de identidad y confiabilidad. Servidores de control de acceso permitiendo que solo la gente correcta pueda tener acceso a la información en el momento correcto.

Con la solución apropiada desplegada, cuando un usuario hace una llamada telefónica, el *CallManager* es capaz de encriptar y autenticar la señalización. Opcionalmente, la voz puede ser encriptada para lograr un nivel más alto de privacidad. Todo esto es posible gracias a las capacidades de confiabilidad basadas en certificados digitales y tecnologías relacionadas de autorización y autenticación.

8.7.1 Amenazas

Desafortunadamente existen numerosas amenazas que conciernen a las redes VoIP; muchas de las cuales no resultan obvias para la mayoría de los usuarios. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables. La conversación es en sí misma un riesgo y el objetivo más obvio de una red VoIP. Las llamadas son también vulnerables al "secuestro". En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada.

8.7.1.1 Spoofing

Por *spoofing* se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada. Desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

Para evitar ataques de spoofing contra nuestros sistemas podemos tomar diferentes medidas preventivas; en primer lugar, parece evidente que una gran ayuda es reforzar la secuencia de predicción de números de secuencia TCP. Otra medida sencilla es eliminar las relaciones de confianza basadas en la dirección IP o el nombre de las máquinas, sustituyéndolas por relaciones basadas en claves criptográficas; el cifrado y el filtrado de las conexiones que pueden aceptar nuestras máquinas también son unas medidas de seguridad importantes de cara a evitar el spoofing.

8.7.2 Defenderse

Lo primero que deberíamos tener en mente a la hora de leer sobre VoIP es la encriptación. Aunque lógicamente no es sencillo capturar y decodificar los paquetes de voz, puede hacerse. Y encriptar es la única forma de prevenirse ante un ataque. Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN, el protocolo Ipsec y otros protocolos como SRTP. Esto debería aliviar cualquier riesgo de amenaza.

Lo próximo, como debería esperarse, podría ser el proceso de asegurar todos los elementos que componen la red VoIP: servidores de llamadas, routers, teléfonos, etc. Se necesita configurar cada uno de esos dispositivos para asegurarte de que están en línea con tus demandas en términos de seguridad. Los servidores pueden tener pequeñas funciones trabajando y sólo abiertos los puertos que sean realmente necesarios. Los routers y switches deberían estar configurados adecuadamente, con acceso a las listas de control y a los filtros. Todos los dispositivos deberían estar actualizados en términos de parches y actualizaciones. Por último, podemos emplear un firewall y un IDS (*Intrusion Detection System*) para ayudar a proteger la red de voz.

Una opción válida para la defensa de nuestra red VoIP es la utilización de un firewall debido a que tanto los protocolos H.323 como SIP utilizan números de puertos estándares (H.323 usa 1719 y 1720; SIP utiliza el 5060) se puede bloquear dichos puertos en las reglas de establecimiento del dispositivo con esto se logra bloquear la telefonía IP. Manipulando estos puertos se puede mejorar la seguridad ya que al existir puertos habilitados en un rango de 1024 a 65534 se puede escoger un número de puerto al azar y este utilizarlo para nuestras comunicaciones de voz sobre la red privada, así bloquearemos la posibilidad de que un intruso pueda acceder a nuestro sistema mediante los puertos bien conocidos de los protocolos de VoIP.

CONCLUSIONES Y RECOMENDACIONES

Con la aparición y evolución de la telefonía IP se presenta los beneficios de bajar los costos en cuanto a lo que comunicación se refiere, pero como toda nueva tecnología la necesidad imperiosa de aumentar las seguridades es un problema que requiere especial tratamiento.

Al desarrollar este trabajo, se puede concluir que la gran mayoría de ataques a la red de Voz sobre IP, se presentan desde el interior de nuestra propia red, motivo por el cual se presenta un estudio de las vulnerabilidades riesgos, ataques y defensas más comunes para lograr que la red VoIP pueda cumplir con normas estándares para la comunicación multimedia de forma confiable y segura.

Los riesgos comunes que presenta la comunicación VoIP, hacen referencia a la capacidad de invadir y capturar información de las conversaciones que se realizan, es decir se violenta la confidenciabilidad, de igual manera la disponibilidad del servicio y la integridad, son aspectos que el presente documento tienen muy en cuenta, a la hora de implementar un sistema de comunicación de voz sobre IP. Los ataques a este tipo de redes van relacionados especialmente al robo de identidad, mediante el cual un *hacker* tiene la posibilidad de interceptar nuestras conversaciones.

En esta monografía, se dan a conocer aspectos de seguridad para contrarrestar los ataques a una red de telefonía de VoIP, la implementación de nuevas técnicas como IPsec de IPv6, SRTP, TLS entre otras, permiten brindar soluciones a dichos problemas.

La instalación de equipos de protección como Gatekeepers, firewall, NATs o servidores proxy para SIP, posibilitan la restricción de accesos a la red de telefonía, sin embargo se debe considerar que la implementación de estos sistemas, conlleva a una perdida de Calidad de servicio (QoS), la cual determina si es factible o no, la implementación del sistema de comunicación. En tal sentido en esta monografía se presentan las soluciones a los problemas más significativos relacionados a QoS, considerando recursos de protección para priorizar el tráfico entrante y saliente.

También es importante recordar, que las recomendaciones de seguridad descritas en el Anexo 4, tales como la supervisión del tráfico de entrada y salida, el control de admisión de una llamada, poseer un registro detallado de todas las llamadas, no usar medios de comunicación compartidos, cuidar sus contraseñas y cambiarlas periódicamente, etc.

Para la demostración de las seguridades anteriormente descritas, se utilizó programas como el "*OpenPhone*" para llamadas mediante el protocolo H.323, el cual por configuración necesita registrarse a un gatekeeper (a través del software "*OpenGK*"), el cual en su tabla de "*Authentication Credentials"* define quienes pueden acceder al servicio y cuales serán sus contraseñas. A más de no permitir el acceso a teléfonos no registrados, tiene la función de resolución de nombres y de asignación de ancho de banda para las comunicaciones.

De igual forma se implementó la comunicación mediante el protocolo SIP con la utilización del software "X-lite", el cual es un teléfono SIP. De igual forma, éste tiene que registrarse y recibir autorización de un servidor proxy SIP (por medio del programa "OnDO SIP Server"). El servidor, en su tabla de "*Authentication*" describe los usuarios que tienen autorización para utilizar el servicio, además de asignar la contraseña para disponer comunicación de voz sobre IP.

Finalmente, la utilización de un Firewall para VoIP es primordial, ya que aquí se puede realizar el bloqueo de los puertos asignados para VoIP, y en forma aleatoria establecer números de puertos confiables, que sólo la red interna los maneja y conoce.

GLOSARIO

ACK *Acknowledgment* (Acuse de recibo) Notificación enviada por un dispositivo de red a otro para confirmar un evento.

AES *Advanced Encryption System* (Sistema de Encriptación Avanzado) Sistema avanzado para la encriptación de los datos.

AH Authentication Header (Autenticación de Cabecera) Provee la autentificación de origen de la transmisión y ofrece integridad en la conexión.

AIB *Authenticated Identity Body* (Cuerpo de Identidad Autenticado) define una ficha de autenticación genérica de SIP para proporcionar integridad de la referencia en sus cabeceras.

ALG *Application Level Gateways* (Niveles de Aplicación de Gateway) software empotrado sobre un firewall o NAT, que permite una configuración dinámica basado en aplicaciones de información específica.

BES *Back End Service* (servicio de programas de respaldo) dispositivo que mantiene los datos sobre puntos finales, incluyendo sus permisos, servicios, y configuración.

DES *Data Encryption Standard* (Estándar de cifrado de datos) Algoritmo estándar para la encriptación de datos.

DNS *Domain Name Service* (Servicio de Nombres de Dominio) Servicio de asignación de nombres a las computadoras con una estructura jerárquica.

EKE *Encrypted Key Exchange* (Intercambio de Teclas de Encriptación) Algoritmo simétrico que usa claves compartidas para cifrar las claves publicas *Diffie – Hellman.*

EOFB *Enhanced Outer Feedback* (Realimentación exterior mejorada), modo de encriptación de flujos de la media.

ESP *Encapsulating Security Payload* (Seguridad de Encapsulamiento de Carga Útil) Provee servicio seguro de encapsulación de datos a mas ofrece integridad en la conexión.

Firewall Servidor de acceso para proporcionar seguridad entre el Internet y una red privada mediante el uso de reglas para permitir el paso de una red a otra.

Gateway VoIP Dispositivo que tiene la función principal de interconectar una red VoIP con una red de telefonía normal.

H.323 Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real.

IDS *Intrusion Detection System* (Sistema de Detección de Intrusos) Sistema de VoIP que sirve para detectar intrusiones no autorizadas en la red.

IETF *Internet Engineering Task Force* (Grupo de Ingeniería de Internet) Grupo responsable del desarrollo de estándares de Internet.

IKE *Internet Key Exchange* (Intercambio de Clave de Internet) Protocolo para la administración de claves en Internet.

IP *Internet Protocol* (Protocolo Internet) Protocolo de la capa de red de TCP/IP que ofrece un servicio de comunicación no orientado a conexión. Ofrece funciones de direccionamiento, especificación del tipo de servicio, fragmentación, reensamblaje y seguridad.

IPSec *IP Security* (Protocolo de Seguridad IP) Conjunto de medidas de seguridad para proteger las transmisiones del protocolo IP.

ISAKMP *Internet Security Association and Key Management* (Asociación de Seguridad de Internet y el Protocolo de Manejo de Claves).

ISDN *Integrated Services Digital Network* (Red Digital de Servicios Integrados, RDSI) Protocolo de comunicación que ofrecen las compañías telefónicas y que permite que las redes telefónicas transmitan voz, datos y otros tipos de tráfico.

ISP *Internet Service Provider* (Proveedor de Servicios de Internet, PSI).

ITU-T *International Telecommunications Union – Telecommunications* Organización internacional que desarrolla estándares de comunicación.

JITTER Distorsión en una línea de comunicación análoga que puede producir perdida de datos.

LAN *Local Area Network* (Red de área local) Red de datos de alta velocidad que cubre un área geográficamente pequeña.

LATENCIA Tiempo que toma una transmisión de voz para ir de su fuente a su destino.

MAC *Message Authentication Code* (código de autentificación de mensaje) suministra la autentificación de paquete de RTP y la integridad sobre campos seleccionados.

MC *Multipoint Contoller* (controlador de multipunto) Parte del MCU, negocia con todos los terminales para asegurar un denominador común.

MCU *Multipoint Control Unit* (Unidad de Control Multipunto) Unidad de que permite y establece la conferencia de llamadas entre mas de 2 puntos finales.

MEGACO/H248 *Media Gateway Control* (Control de Gateway de Media) protocolo estándar para conectarse entre el Media Gateway Controllers (MGCs) y el Media Gateways (MGs).

MG *Media Gateway* (Gateway de media) se concentra en la función de traducción de señal de audio, llevando a cabo la conversión.

MGC *Media Gateway Controllers* (Controladores de Gateway de Media) maneja la señalización de datos entre los MGs y otros componentes de la red.

MGCP *Media Gateway Control Protocol* (Protocolo de Control de Gateway) usado para comunicarse entre los distintos componentes de un gateway de VoIP (MG y MGC).

MIKEY *Multimedia Internet Keying*, protocolo usado para la solución del manejo de claves SRTP.

MIME *Multipurpose Internet Mail Extensión*, estándar para describir contenido en Internet. Define mecanismos para la protección de integridad y la encriptación.

MP *Multipoint Processor* (procesador de multipunto) Parte del MCU, es capaz de mezclar o conmutar tráfico de voz, datos o video.

NAT *Network Address Translation* (traducción de direcciones de red) Mecanismo que reduce la necesidad de tener direcciones IP únicas. Usado para esconder direcciones de red internas y permitir algunos puntos finales dentro de una LAN compartir la misma dirección IP (externa).

PBX *Private Branch Exchange* (Centralita Telefónica Privada) Conmutador de un teléfono analógico o digital que se usa para conectar redes telefónicas.

PPP *Point to Point Protocol* (Protocolo Punto a Punto) Proporciona conexión router a router y host a red sobre circuitos síncronos y asíncronos.

PSTN *Public Switched Telephone Network* (Red de Telefonía Conmutada Pública) Termino que se refiere a las diversas redes de servicios telefónicos que hay en todo el mundo.

QoS *Quality of Service* (Calidad de Servicio) Medida de rendimiento de un sistema de transmisión que refleja su calidad de transmisión y disponibilidad de servicio.

RAS *Registration, Authentication and Status* (Registro, Autentificación y Estado) Protocolo que negocia con el *Gatekeeper* y obtiene la dirección del punto final con el que está intentando contactar en una llamada por IP.

RTP *Real Time Transport Protocol* (Protocolo de Tiempo Real) Diseñado para suministrar funciones de transporte de red de extremo a extremo para aplicaciones que transmiten en tiempo real.

RTCP *Real Time Control Protocol* (Protocolo de Control de Tiempo Real) Protocolo que controla las operaciones de RTP.

SBC *Session Border Controller* (Controlador de Borde de Sesión) Equipo que brinda servicios para VoIP como Firewall / NAT, control de admisión de llamada, protocolo interworking.

SDP *Session Description Protocol* (Protocolo de Descripción de Sesión) es un protocolo que describe el inicio de sesiones multimedia, que también corre sobre conexiones de UDP.

SIP *Session Initiation Protocol* (Protocolo de Inicio de Sesión) Protocolo de señalización basado en texto usado para crear y controlar sesiones multimedia con dos o más participantes dentro de VoIP.

SPEKE *Password-authenticated Exponential Key Exchange*, método donde la llave compartida desarrolla un generador para el grupo Diffie - Hellman.

SPOOFING Cuando un paquete alega ilegalmente provenir de una dirección de la cual no proviene.

SRTP *Security Real Time Protocol* (seguridad del protocolo de tiempo real) Perfil del protocolo de transporte de tiempo real (RTP) que brinda confidencialidad, autentificación de mensaje, y protección de repetición para tráfico RTP y RTCP.

STUN Simple Traversal de UDP a través de NAT, Característica que permite que dos dispositivos se conecten entre si a través de una topología arbitraria e lugar de a través de un enlace directo.

TCP *Transmission Control Protocol* (Protocolo de Control de Transmisión) Protocolo de la capa de transporte orientado a conexión que proporciona una transmisión *full duplex*.

TLS *Transport Level Security* (Nivel de seguridad de transporte) protege mensajes de señalización de SIP contra la pérdida de integridad, confidencialidad y contra la repetición. Proporciona integridad de manejo de claves con autentificación mutua y asegura la distribución de claves.

ToS *Type of Services* (tipos de servicios) Campo de un datagrama IP que indica el modo en el que se debe manejar el datagrama.

TURN Traversal usado en Relay NAT, protocolo que permite a un elemento detrás de un NAT o Firewall recibir los datos entrantes de conexiones TCP o UDP para complementar las limitaciones de STUN.

UA *User Agent* (Agente del Usuario) SIP, Aplicación que inicia, recibe y termina llamadas.

UAC *User Agent Client* (Usuario Agente Cliente) SIP, agente de usuario que inicia una llamada.

UAS *User Agent Server* (Usuario Agente Servidor) SIP, agente de usuario que recibe una llamada.

UDP *User Datagram Protocol* (Protocolo de Datagramas de Usuario) Protocolo no orientado a conexión de capa de transporte de TCP/IP, intercambia datagramas sin confirmación o garantía de entrega. Requiere que el procesamiento de errores y las retransmisiones sean manejados por otros protocolos.

URI *Universal Resource Indicator* (Indicador de Recurso Universal) Forma de numeración telefónica universal

VAD *Voice Activity Detection* (Detección de Actividad de Voz) Dispositivo que previene la transmisión de paquetes vacíos de voz. Cuando el usuario no esta hablando el dispositivo no manda ruido blanco.

VLAN *Virtual Local Area Network* (Red de Área Local Virtual) Grupo de dispositivos en una LAN que se configuran de modo que puedan comunicarse como si estuvieran conectados a un mismo cable.

VoIP *Voice over IP* (Voz sobre IP) Permite la transmisión de voz sobre una red IP.

VoIPsec Seguridad en VoIP, Utilización de Ipsec en VoIP. Reduce la amenaza de ataques en puntos medios, captura de paquetes, y muchos tipos de análisis de tráfico de voz.

VPN *Virtual Private Network* (Red Privada Virtual) Permite que el tráfico viaje seguro sobre una red TCP/IP publica mediante el cifrado del tráfico

WAN *Wide Area Network* (red de área amplia) Red de comunicación de datos que presta servicio a usuarios ubicados a lo largo de una área geográfica extensa y a menudo utiliza dispositivos de transmisión suministrados por operadoras de telecomunicaciones.

BIBLIOGRAFÍA

- Ares Roberto. *Telefonía IP*. **www.monografias.com**. Página visitada el 15 / 02 / 2006.
- Collier Mark. *Ediciones Básicas de la Vulnerabilidad para el SIP*. **www.securelogix.com**. Página visitada el 13 / 11 / 2005.
- Csrc. Publicaciones sobre seguridades de VoIP. **www.csrc.nist.gov**. Página visitada el 10 / 12/ 2005
- GNU Gatekeeper. *Manual de Gatekeeper*. **www.gnugk.org**. Página visitada el 13 / 02 / 2006.
- HHI Corecom. Artículos sobre seguridad en VoIP. **www.hhi.corecom.com**. Página visitada el 10 / 12/ 2005
- Kuhn Richard, Walsh Thomas, Fries Steffen. *Recommendations of the National Institute of Standards and Technology for the Security for Voice Over IP Systems.* United States of America. January 2005.
- LA FLECHA Diario de Ciencia y Tecnología. *Seguridad en el protocolo VoIP*. **www.laflecha.com**. Página visitada el 21 / 02 / 2006.
- Microsoft. *VoIP: El Teléfono por Internet*. **www.microsoft.com**. Página visitada el 30 / 01 / 2006.
- Navarro Schlegel Anna. *Diccionario de términos de comunicaciones y redes*. Núñez de Balboa. 2003.
- Net2phone. *Legislación sobre servicios agregados del Internet en Ecuador, incluyendo VoIP.* **www.net2phone.com**. Página visitada el 15 / 02 / 2006.
- Open H.323. *Software Openphone y OpenGK*. **www.openh323.org**. Pagina visitada el 15 / 01 /2006.
- Ordóñez Ojeda Xavier et al. *Arquitectura de Sistemas Computarizados. Instalación de Firewall bajo Linux.* **www.monografias.com**. Página visitada el 15 / 02 / 2006.
- SIP Software. *Software Ondo SIP Proxy*. **www.sipsoftware.com**. Pagina visitada el 21 / 02 /2006.
- Video Development Initiative. *Protocolo para Inicio de Sesión (SIP)*. **www.vide.com**. Página visitada el 15 / 02 / 2006.
- Voipsa. *Recommendations of the National Institute of Standards and Technology*. **www.voipsa.org**. Página visitada el 14 / 01 / 2006.
- YMDG. *Descripción técnica detallada sobre Voz sobre IP (VoIP).* **www.recursosvoip.com**. Página visitada el 15 / 02 /2006.

ANEXO 1

Operaciones de Registro Admisión y Status (RAS)

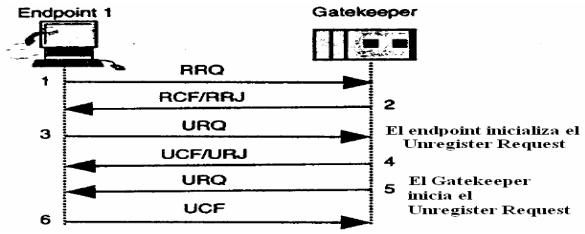
H.323 usa un canal lógico sobre la LAN para manejar las operaciones de Registración, Admisión y Status (RAS). En el canal RAS se usan mensajes H.225.

Procedimiento de descubrimiento de un Gatekeeper

- Se envía un mensaje GRQ (Gatekeeper Request) para preguntar al Gatekeeper sobre la dirección de transporte del canal RAS en el cual debe registrarse el Terminal.
- El gatekeeper devuelve un mensaje GCF (*Gatekeeper Confirmation*) si acepta la petición, este mensaje contiene la dirección del canal de transporte a la cual debe registrarse; a su vez el gatekeeper podría enviar un mensaje GRJ (Gatekeeper Reject) si rechazara la petición del Terminal.

Procedimiento de registración en un gatekeeper

- El Terminal se une a una zona y provee al Gatekeeper sus direcciones de transporte del canal RAS, control de llamadas y alias.



Proceso de registración en un Gatekeeper

Donde:

RRQ: Register Request, Requerimiento de Registración.

RCF: Register Confirmation, Registración Autorizada.

RRJ: Register Reject, Registración Rechazada.

URQ: Unregister Request, Requerimiento de Deregistración.

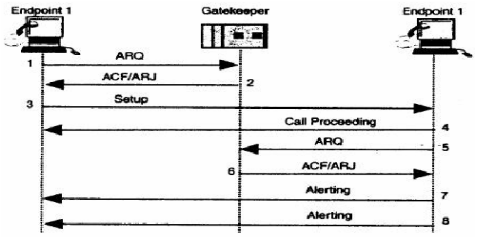
UCF: Unregister Confirmation, Deregistración Aceptada.

URJ: Unregister Reject, Deregistración Rechazada.

Procedimiento de admisión

H.323 define el uso de un protocolo de señalización Q.931, los mensajes se usan entre los terminales. Los mensajes RAS se usan entre los terminales y el Gatekeeper. El mensaje Admisión Request (ARQ) contiene el parámetro de ancho de banda: número de 100 bits/seg. requerido para la llamada bidireccional; y el parámetro "*Call Reference Value*" (CRV). En el procedimiento de admisión intervienen los siguientes mensajes:

- ARQ Admisión Request: que contiene entre otros el parámetro de ancho de banda.
- ACF Admisión Confirmation: que confirma y sincroniza entre otros parámetros el ancho de banda a usar.
- ARJ Admisión Reject: que rechaza la petición de la Terminal.
- Setup: Parámetros de configuración de llamada que se transmiten entre terminales.
- Call Proceeding: Información entre terminales que indica que la instauración de la llamada, se esta realizando.
- Alerting: Mensaje de la Terminal que recibió la petición de llamada en la cual se configura las instancias en la cual procederán con la llamada.



Proceso de admisión

Cambios de ancho de banda

- BRQ Bandwith Change Request: contiene parámetros de el ancho de banda
- BCF Bandwith Change Confirmation: Confirma el requerimiento
- BRJ Bandwith Change Reject: Rechaza el requerimiento y provee la razón.

Procedimiento para notificar sobre terminación de llamada

- DRQ Disengage Request: Contiene el identificador del endpoint, identificador de la llamada y causa de este mensaje.
- DCF Disengage Confirmation. Confirmación del pedido anterior.
- DRJ Disengage Reject. Negación del pedido anterior.

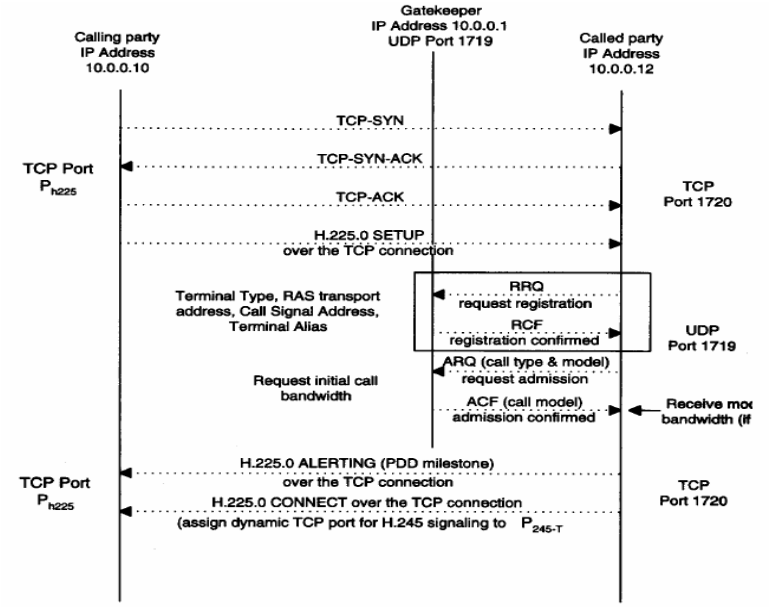
ANEXO 2

Modelos de llamada de H.323.

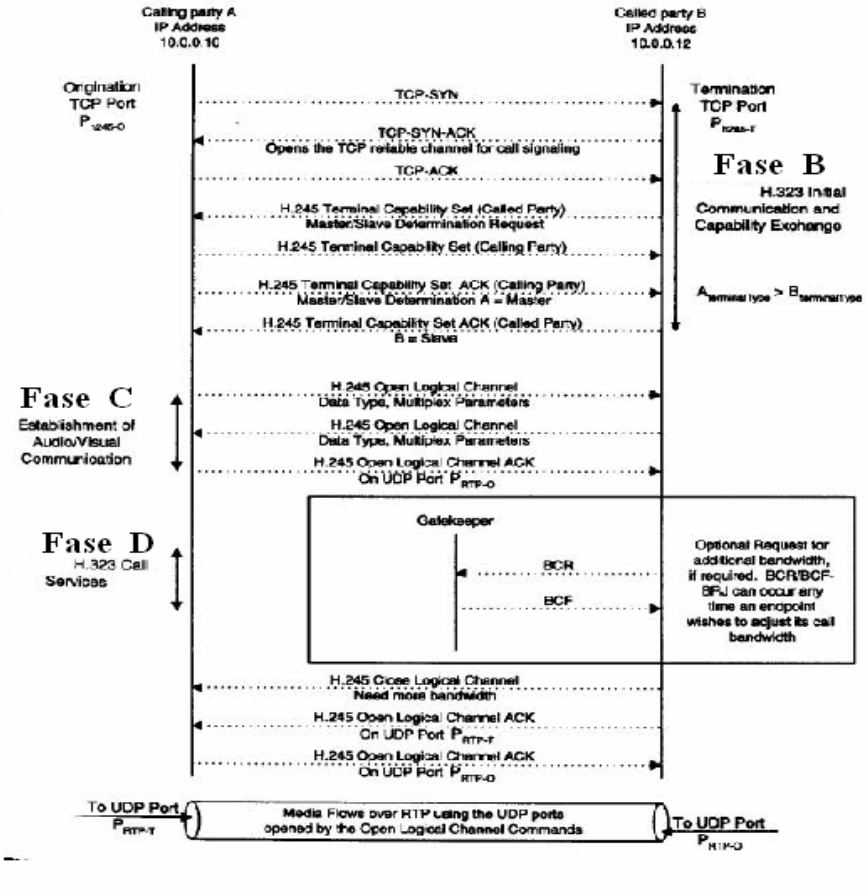
Modelo de ruteo directo: El modelo del ruteo directo en el contexto de una llamada punto a punto consta de 5 fases:

- Fase A: Establecimiento de la llamada.
- Fase B: Comunicación inicial entre endpoits e intercambio de capacidades de los terminales.
- Fase C: Establecimiento de comunicación audio/visual entre endpoints.
- Fase D: Requerimiento y negociación de servicios de llamada.
- Fase E: Terminación de la llamada.

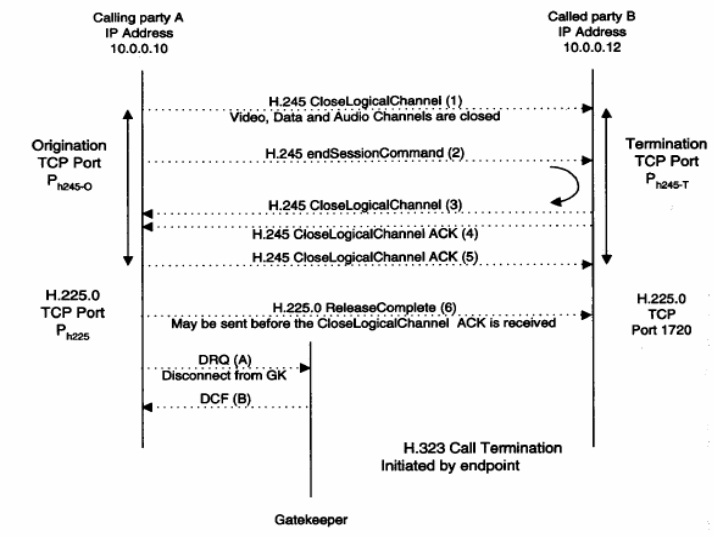
Fase A



Fases B, C y D



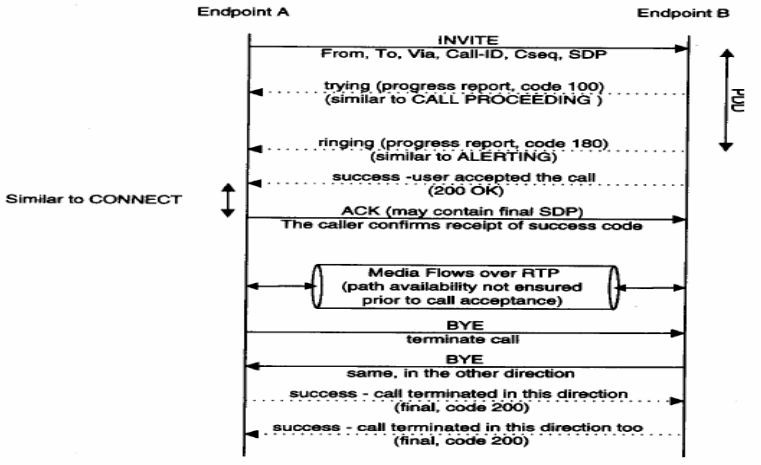
Fase E



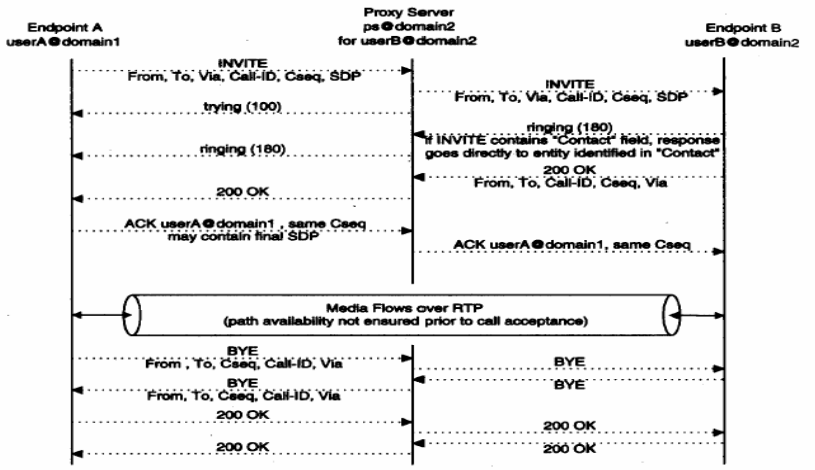
ANEXO 3

Modelos de llamadas en SIP

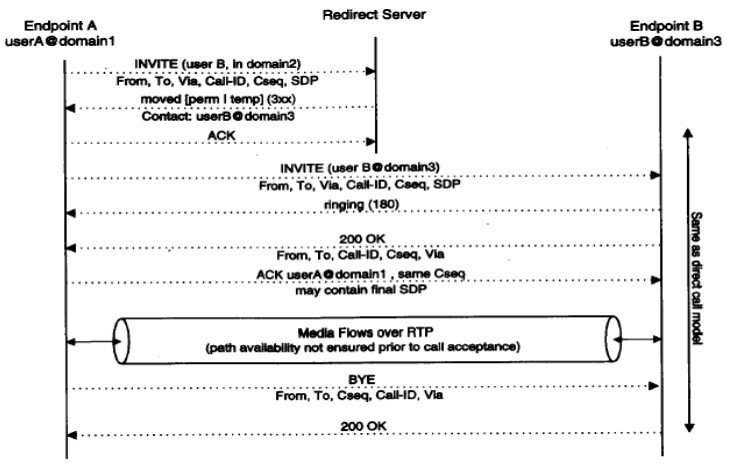
Señalización directa entre agentes de Usuario



SIP modelo de llamada Proxy



SIP Modelo de llamada redireccionada



ANEXO 4

Seguridad de VoIP: Riesgos, ataques y vulnerabilidades; formas de prevenirlos

A medida que crece su popularidad aumentan las preocupaciones por la seguridad de las comunicaciones vía VoIP. Estos problemas de seguridad no sólo comprometen el contenido de una conversación, sino también la información sobre la propia llamada. Estos datos podrían ser interceptados y registrados por terceros para conocer las llamadas entrantes y salientes de un terminal, configurar y dirigir llamadas sin consentimiento del propietario o grabar los datos de todos sus contactos para "bombardear" sus buzones de voz IP con spot (*Spam over Internet Telephony*), técnica bautizada como *bombing* o *Vbombing*. Otro riesgo es que los paquetes de datos sean interceptados para alterar los parámetros de una llamada, escuchar una conversación o retransmitirla íntegramente. Las llamadas también están expuestas al riesgo del "secuestro" por parte de *hackers*, lo que abre una serie de posibilidades maliciosas que van desde el redireccionamiento hasta el robo de identidad, también conocido como *spoofing*. Una de las formas de proteger las comunicaciones basadas en voz sobre IP es la "encriptación", tanto de la señal de la llamada como de los paquetes de datos. Además, es importante proteger periódicamente de *hackers* y *spammers* los elementos que componen la red VoIP con las actualizaciones y parches oportunos.

Riesgos de VoIP

- **Robo:** Un atacante que llegue a tener acceso a un servidor VoIP también puede obtener acceso a los datos de voz almacenados y al propio servicio telefónico para escuchar conversaciones o hacer llamadas gratuitas a cargo de otros usuarios.
- **Ataques de virus:** Si un virus infecta un equipo de un servidor VoIP, el servicio telefónico puede quedar interrumpido. También pueden verse afectados otros equipos conectados a ese sistema.
- **Tecnología no regulada:** Aunque se está legislando al respecto, los usuarios aún están expuestos a algunas vulnerabilidades y al riesgo de sufrir ciertos timos especializados. Por ejemplo, a través del *telemarketing* se puede utilizar la comunicación VoIP para enviar una cantidad ingente de mensajes de voz a

consumidores, lo que podría provocar la desconexión de un sistema. Los delincuentes también pueden utilizar un proceso consistente en la suplantación de ID de la persona que llama (en el que se muestra una firma de ID de llamada falsa a los destinatarios) para cometer fraudes haciéndose pasar por empleados de entidades en las que se confía con objeto de que los clientes divulguen información confidencial sobre sus cuentas.

Ataques

La información sobre una llamada es tan valiosa como el contenido de la voz. La conversación es en sí misma es un riesgo y el objetivo más obvio de una red VoIP. Consiguiendo una entrada en una parte clave de la infraestructura, como una puerta de enlace de VoIP, un atacante puede capturar y volver a montar paquetes con el objetivo de escuchar la conversación. O incluso peor aún, grabarlo absolutamente todo, y poder retransmitir todas las conversaciones sucedidas en la red. Las llamadas son también vulnerables al "secuestro". En este escenario, un atacante puede interceptar una conexión y modificar los parámetros de la llamada. Se trata de un ataque que puede causar bastante pavor, ya que las víctimas no notan ningún tipo de cambio. Las posibilidades incluyen la técnica de spoofing o robo de identidad, y redireccionamiento de llamada, haciendo que la integridad de los datos estén bajo un gran riesgo.
La enorme disponibilidad de las redes VoIP es otro punto sensible. En el PSTN, la disponibilidad era raramente un problema. Pero es mucho más sencillo *hackear* una red VoIP. Los efectos de los ataques de negación de servicio son demoledores. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicarte vía voz o datos.

Los teléfonos y servidores son blancos por sí mismos. Aunque sean de menor tamaño o nos sigan pareciendo simples teléfonos, son en base, ordenadores con software. Obviamente, este software es vulnerable con los mismos tipos de *bugs* o agujeros de seguridad que pueden hacer que un sistema operativo pueda estar a plena disposición del intruso. El código puede ser insertado para configurar cualquier tipo de acción maliciosa.

Vulnerabilidades de VoIP

SIP tiene las mismas vulnerabilidades de IP y del uso-nivel que otros protocolos de VoIP, pero hay varios factores que hacen el SIP potencialmente menos seguro:

Madurez: las puestas en práctica estándares y de soportes del SIP son relativamente nuevas.
Complejidad: SIP mismo es moderado complejo, pero con todas las extensiones necesarias, es un protocolo complicado.
Extensibilidad: SIP apoya las extensiones, que son nuevas y a menudo frágiles desde un punto de vista de la seguridad.
Codificando: SIP utiliza los mensajes del texto, que son más fáciles de considerar con un succionador.

Secuestro Del Registro

Este ocurre cuando un atacante personifica un UA válido y substituye el registro por su propia dirección. Este ataque hace todas las llamadas y recibe las entrantes.
Según lo mencionado, el registro se realiza normalmente usando el UDP, que hace más fácil a las peticiones del *spoof*. La mayoría de los escenarios de SIP o no desafían peticiones, o piden solamente un *username/password* simple, que se puede derrotar con ataques diccionario-estilo. Un ataque diccionario-estilo es donde el atacante tiene uno de sus *usernames* y después camina a través de una lista de contraseñas probables construida basada en su conocimiento de su empresa. Algunas empresas pueden utilizar las contraseñas compartidas, débiles, o "mecánicamente" generadas. En estos casos, un atacante que aprende una de sus contraseñas podría aprender todos.

El secuestro del registro puede dar lugar a la pérdida de llamadas del UA legítimo, que puede ser uno de los teléfonos o de un recurso crítico. También, el UA atacante puede recoger la autentificación u otra información importante. O este puede también realizar un ataque Hombre-En-Medio, donde transparente se sienta entre el llamador y el llamado y ser capaces de recoger y de modificar señales.

Personificación Del Poder

La personificación del poder ocurre cuando un atacante trampea un UAs. Si un atacante personifica con éxito un poder, él tiene acceso a todos los mensajes del SIP y está en el control completo de la llamada. El UA se comunica con UDP y no requieren normalmente autentificación fuerte al comunicarse con otro UA. Un poder del atacante puede por lo tanto insertarse en la corriente que señala con varios medios, incluyendo el servicio del **Domain Name** (DNS) *spoofing*, el *Address Resolution Protocol* (ARP) *spoofing*, o cambiando simplemente la dirección del poder para un teléfono del SIP.
Si el DNS **spoofing** se utiliza para volver a dirigir llamadas salientes a un dominio particular (ejm. "company.com"), todas las llamadas de salida a ese sitio se pueden interceptar, manipular, bloquear.

Mensaje Que trata de forzar

El mensaje que trata de forzar ocurre cuando un atacante intercepta y modifica los paquetes intercambiados entre los componentes del SIP. Este puede ocurrir con el secuestro del registro, la personificación del poder, o un ataque contra cualquier componente confiado en los mensajes de proceso del SIP, tales como la entrada de los medios, o al firewall.

Desmontaje De Sesión

El desmontaje de sesión ocurre cuando un atacante captura señales para una configuración de una llamada y después envía un ***spoofed*** mensaje "*bye*" del SIP al UAs que participa en dicha llamada. Desafortunadamente la mayoría de los UAs SIP no requiere autentificación fuerte, y permite que un atacante envíe mensajes "*bye*" correctos hechos a mano a los dos UAs, declinando la llamada.

Recomendaciones

La seguridad del SIP comienza con seguridad básica del IP y VoIP. La seguridad de SIP puede ser mejorada usando las puestas en práctica que apoyan TCP/IP. Puede también ser mejorada grandemente usando un estándar de la seguridad, tal como la

seguridad de la capa de transporte (TLS), para proporcionar la autentificación y el cifrado fuertes entre los componentes del SIP. Una vez que se elija un estándar de seguridad tal como TLS, hay evitar de usar cualquier componente que no pueda utilizarlo. Usar cualquier componente no seguro tal como un teléfono barato del SIP permitirá muchos de los tipos de ataques descritos arriba. Si este estándar (o un equivalente) no se utiliza, entonces requerirá el uso de firewalls SIP-optimizados, que protegen el sistema interno de SIP contra los ataques. Un buen cortafuego debe poder hacer, entre otros, lo siguiente:

- Supervisar los mensajes de entrada y de salida de SIP para los ataques del uso-nivel y desechar los paquetes malévolos
- Apoyar TLS y otras seguridades estándares.
- Realizar el control de la admisión de llamada (CAC). Controlar el número de llamadas simultáneas.
- Proporcionar la registración detallada de todos los mensajes de SIP. Registrar todas las llamadas no autentificadas.
- Mantener QoS en todos los paquetes de media. Dar prioridad a los paquetes de media y preservar las marcas de QoS.

- No usar dispositivos de medios de comunicación compartidos como centros en redes de VoIP corporativas. Usar esto podría permitir que un pirata informático tenga acceso para todas conversaciones que atraviesan la red. Los administradores de la red necesitarán hacer las auditorias periódicas para asegurarse de que no hay ningún dispositivo no autorizado husmeando en la red.

- Los distribuidores deben ser presionados para que asegurar que todo tráfico de VoIP que es enviado sobre una red de IP pública será cifrado. En este momento el motor para distribuidores de equipo de VoIP es la calidad de servicio. La encriptación también podía ser hecha solamente en el enlace - nivel. Los dispositivos de Gateway son diseñados manejar cargas de procesamiento más pesadas normalmente y este método debe ser transparente para los usuarios. La encriptación podía estar limitada a campos específicos dentro de los paquetes de VoIP que contienen la información confidencial.

- Verifique que su firewall sea específico para VoIP. Los piratas informáticos pueden en algún momento encontrar una manera de montar en una red a través de una firewall manipulando un paquete H.323. Cuando se usa NAT y la encriptación hay dificultades

adicionales con el protocolo SIP porque las direcciones IP aparecen en el cuerpo del protocolo.

Medidas para aumentar la seguridad de VoIP

Utilice una caja de derivación: A menudo la suministra el proveedor del servicio VoIP con el paquete. Lleva directamente la comunicación VoIP al teléfono convencional, sin necesidad de utilizar un equipo doméstico. De este modo contribuye a proteger el teléfono de posibles ataques; y el equipo, de virus que podrían transmitirse a través de Internet.

Utilice contraseñas privadas seguras: Cree contraseñas seguras para el acceso a los sitios Web en los que se almacene su correo de voz y otros datos de audio. No las comparta con nadie.

Ayude a proteger su propio equipo: Si utiliza un equipo para obtener acceso a su correo de voz y a su cuenta VoIP a través del sitio Web de un proveedor, también debe procurar que el equipo esté protegido con contraseñas seguras y software de servidor de seguridad, antivirus y actualizaciones.

ANEXO 5

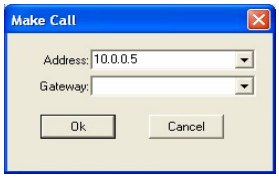
Implementación de servicios y seguridades de Voz sobre IP

Telefonía con el protocolo de VoIP H.323

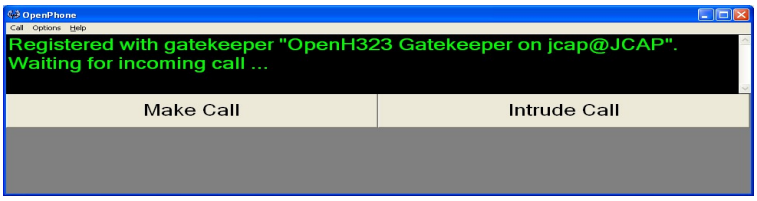
Teléfono OpenH323.

El teléfono OpenH323 es un software basado en el protocolo H323 de VoIP, este nos servirá para la comunicación y demostración de una conversación en VoIP.
A continuación se muestra la pantalla de inicio de OpenH323. Esto en el caso de que la llamada sea realizada directamente sin necesidad de registrarse en un Gatekeeper.

Luego dando un clic sobre "*Make Call*" procedemos a realizar la llamada como se muestra en el siguiente cuadro



En el caso, y el más recomendado, de que la llamada sea realizada mediante un Gatekeeper lo primero que se necesitara es registrarse en el mismo.



Una vez realizado la registración el usuario podrá realizar las llamadas. Cave destacar que la registración puede ser configurada para que se la realice de forma automática a los teléfonos autorizados.

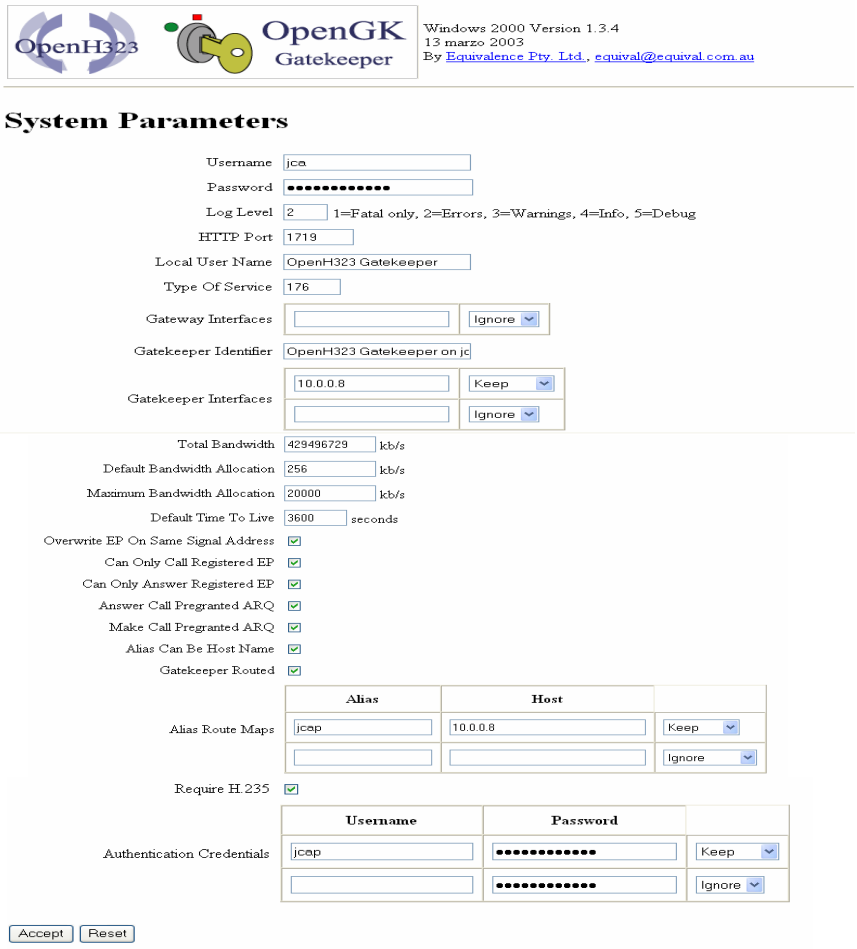
Gatekeeper OpenGK

Una de las partes importantes de la seguridad dentro de una red VoIP basada en H323 es la incorporación de un Gatekeeper que realizará funciones diversas como control de acceso así como resolución de nombres entre otras. Para la puesta en práctica de este proyecto hemos usado un software llamado OpenGK que simula los beneficios de un Gatekeeper.

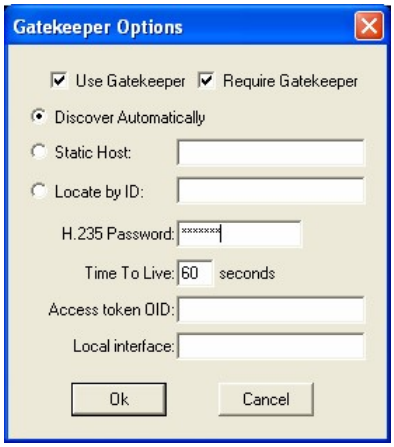
Para un inicio Seguro OpenGK pide una contraseña de administrador antes de mostrar sus funciones

Una vez ingresado procedemos a configurar el Gatekeeper.

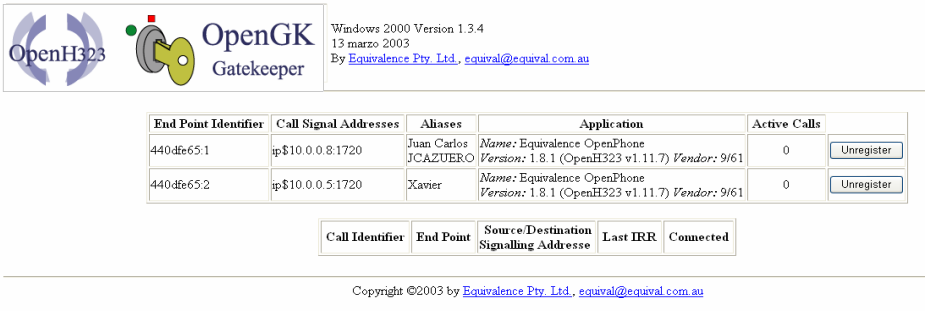
En el siguiente cuadro se puede realizar el cambio de password, así como la configuración del puerto en el cual se realizara las llamadas, de igual forma establecer Gateways en el caso de que existiera. De igual forma se puede configurar el ancho de banda que se usara para las comunicaciones. Un punto importante es el establecimiento de permisos de llamadas, es decir, quienes y que requerimientos necesitan para poder comunicarse dentro de una red interna. También podemos encontrar una tabla de ruteo con los aliases que existen dentro de la red y una lista de autentificación de credenciales que son asignadas a los usuarios de la red VoIP H323.



Cave destacar que en la parte de "*Authentication Credentials*" se puede autorizar a las personas a realizar llamadas, aquí se le asigna un password para que pueda realizar la registración. El usuario desde su teléfono H323 deberá digitar la clave para poder acceder al servicio tal como lo demuestra el siguiente cuadro



En la parte de "*Status*" podemos encontrar un listado de los equipos registrados en la red, sus direcciones IP, sus aliases así como su actividad.



Cuando se realiza una llamada este lleva un registro de quien y a quien se esta llamando

Call Identifier	End Point	Source/Destination Signalling Addresse	Last IRR	Connected	
985439d6-47f5-1810-8a72-0011437ad06a	440dfe65:2	Juan Carlos (JCAZUERO) [10.0.0.8]@ip$10.0.0.8:3426 Xavier@ip$10.0.0.5:1720	17:14:28		Clear
985439d6-47f5-1810-8a72-0011437ad06a	440dfe65:3	Juan Carlos@ip$10.0.0.8:3423 ip$10.0.0.5:1720	17:14:28	17:14:28	Clear

El administrador puede forzar a terminar una llamada con la ayuda del botón "Clear".

Telefonía con el protocolo de VoIP SIP

Teléfono SIP

El siguiente es el software llamado X-Lite que utilizamos para realizar las comunicaciones entre dos o más computadoras, este modelo de teléfono utiliza el protocolo SIP.

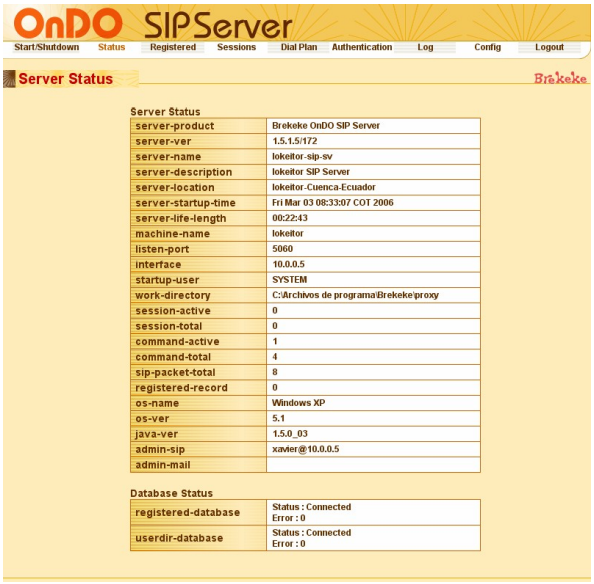
Este software permite la configuración del Proxy a utilizar permitiendo cambiar los puertos de "*Listen*" del teléfono y el del SIP Proxy, usuario autorizado, clave, etc.

SIP Proxy

El siguiente software tiene por nombre OnDO SIP, el mismo que realiza las funciones de un servidor Proxy para el protocolo SIP, a continuación detallaremos su funcionamiento.

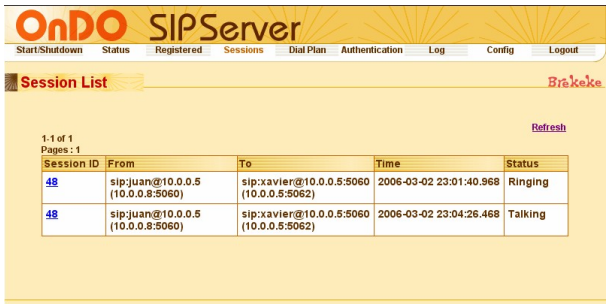
El siguiente cuadro muestra la presentación inicial del SIP Proxy donde se ingresa únicamente con la contraseña del administrador.

Esta pantalla muestra el estado de la configuración del Proxy

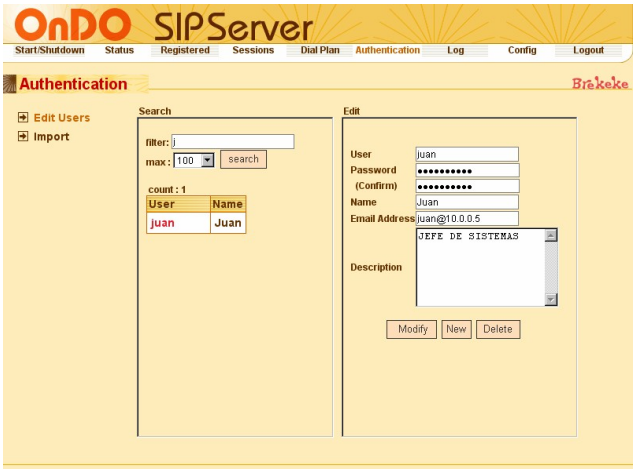


En primera instancia se realiza la registración de los usuarios permitidos dentro del sistema de VoIP, La siguiente pantalla muestra un ejemplo de usuarios que están registrados en el Proxy.

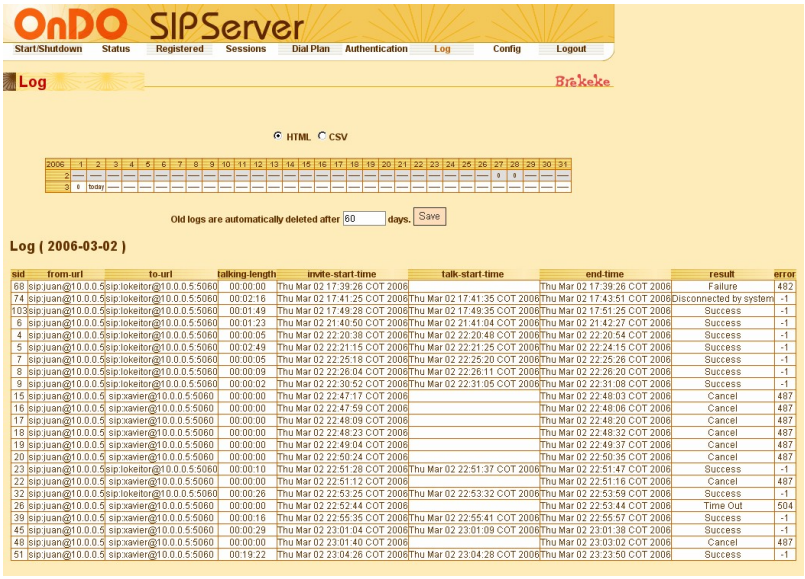
El servidor Proxy permite al administrador monitorear las llamadas que se están realizando así como también las que están esperando conexión, también se puede revisar el estado de la llamada en proceso.



El siguiente es un formulario de ABC de usuarios autorizados por el Proxy, a esta como al resto de funciones solamente tiene acceso el administrador autorizado.



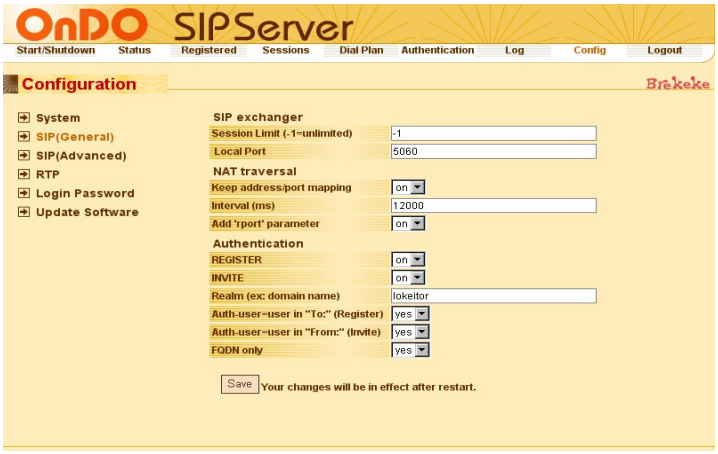
En el siguiente cuadro se demuestra como se puede revisar todas las llamadas realizadas en un día específico, quien y a quien llamo durante que tiempo estuvieron conectados así como también los errores de conexión.



sid	from-url	to-url	talking-length	invite-start-time	talk-start-time	end-time	result	error
68	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:00	Thu Mar 02 17:39:26 COT 2006		Thu Mar 02 17:39:26 COT 2006	Failure	482
74	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:02:16	Thu Mar 02 17:41:25 COT 2006	Thu Mar 02 17:41:35 COT 2006	Thu Mar 02 17:43:51 COT 2006	Disconnected by system	-1
103	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:01:49	Thu Mar 02 17:49:28 COT 2006	Thu Mar 02 17:49:35 COT 2006	Thu Mar 02 17:51:25 COT 2006	Success	-1
6	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:01:23	Thu Mar 02 21:40:50 COT 2006	Thu Mar 02 21:41:04 COT 2006	Thu Mar 02 21:42:27 COT 2006	Success	-1
4	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:05	Thu Mar 02 22:20:38 COT 2006	Thu Mar 02 22:20:48 COT 2006	Thu Mar 02 22:20:54 COT 2006	Success	-1
5	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:02:49	Thu Mar 02 22:21:15 COT 2006	Thu Mar 02 22:21:25 COT 2006	Thu Mar 02 22:24:15 COT 2006	Success	-1
7	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:05	Thu Mar 02 22:25:18 COT 2006	Thu Mar 02 22:25:20 COT 2006	Thu Mar 02 22:25:26 COT 2006	Success	-1
8	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:09	Thu Mar 02 22:26:04 COT 2006	Thu Mar 02 22:26:11 COT 2006	Thu Mar 02 22:26:20 COT 2006	Success	-1
9	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:02	Thu Mar 02 22:30:52 COT 2006	Thu Mar 02 22:31:05 COT 2006	Thu Mar 02 22:31:08 COT 2006	Success	-1
15	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:47:17 COT 2006		Thu Mar 02 22:48:03 COT 2006	Cancel	487
16	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:47:59 COT 2006		Thu Mar 02 22:48:06 COT 2006	Cancel	487
17	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:48:09 COT 2006		Thu Mar 02 22:48:20 COT 2006	Cancel	487
18	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:48:23 COT 2006		Thu Mar 02 22:48:32 COT 2006	Cancel	487
19	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:49:04 COT 2006		Thu Mar 02 22:49:37 COT 2006	Cancel	487
20	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:50:24 COT 2006		Thu Mar 02 22:50:35 COT 2006	Cancel	487
23	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:10	Thu Mar 02 22:51:28 COT 2006	Thu Mar 02 22:51:37 COT 2006	Thu Mar 02 22:51:47 COT 2006	Success	-1
22	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:51:12 COT 2006		Thu Mar 02 22:51:18 COT 2006	Cancel	487
32	sip:juan@10.0.0.5	sip:lokeitor@10.0.0.5:5060	00:00:26	Thu Mar 02 22:53:25 COT 2006	Thu Mar 02 22:53:32 COT 2006	Thu Mar 02 22:53:59 COT 2006	Success	-1
26	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 22:52:44 COT 2006		Thu Mar 02 22:53:44 COT 2006	Time Out	504
39	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:16	Thu Mar 02 22:55:35 COT 2006	Thu Mar 02 22:55:41 COT 2006	Thu Mar 02 22:55:57 COT 2006	Success	-1
45	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:29	Thu Mar 02 23:01:04 COT 2006	Thu Mar 02 23:01:09 COT 2006	Thu Mar 02 23:01:38 COT 2006	Success	-1
48	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:00:00	Thu Mar 02 23:01:40 COT 2006		Thu Mar 02 23:03:02 COT 2006	Cancel	487
51	sip:juan@10.0.0.5	sip:xavier@10.0.0.5:5060	00:19:22	Thu Mar 02 23:04:26 COT 2006	Thu Mar 02 23:04:28 COT 2006	Thu Mar 02 23:23:50 COT 2006	Success	-1

En esta pantalla se configura las opciones generales del sistema como nombre del servidor, descripción, localidad, direcciones del administrador, e interfaz de red del Proxy.

En ente siguiente cuadro se puede configurar las opciones del protocolo SIP como el número de puerto, el número de llamadas máximas que pueden atravesar el Proxy, de igual manera en el caso de utilización de un servidor NAT.



A continuación se presenta las configuraciones avanzadas de SIP como solo aceptar registro del un dominio específico, verificar registro, y tiempos de "*Ringing*", duración de llamada, y tiempo de establecimiento de registro.

En esta pantalla se configura si los paquetes RTP son manejados a través del servidor y si un UA instalado en el servidor manejara dichos paquetes, además se establece los números máximos y mínimos de puertos RTP que puede utilizarse para voz y para video, y el tiempo de sesión RTP.

Cada cambio que se realice en las configuraciones solo tendrá efecto al reiniciar el servidor.

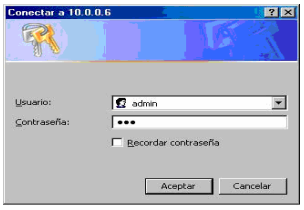
Llamadas telefónicas a través de la Internet

Gateway

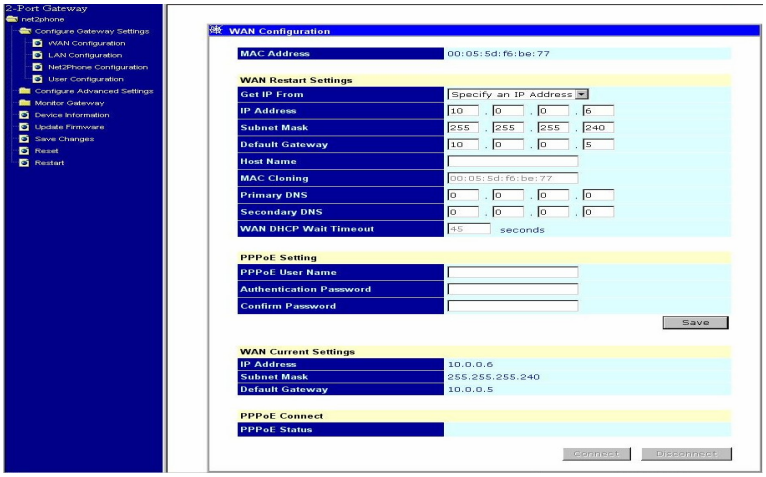
Es un equipo dentro de una red VoIP que tiene como función principal entre otras la posibilidad de comunicar una red de VoIP con una red de telefonía normal (PSTN).

Las siguientes pantallas son del equipo 2-Port Gateway.

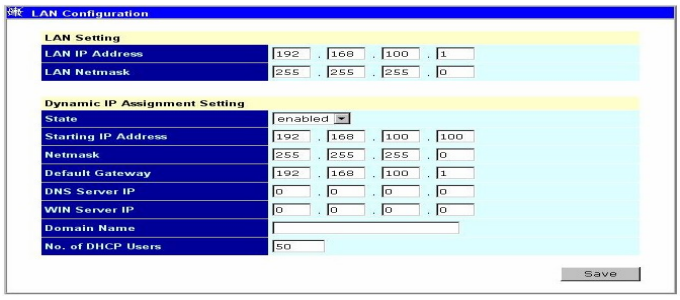
Para seguridad del administrador el software del equipo solicita el ingreso del usuario y su password.



Configuración WAN: Al utilizar la red de Internet para su comunicación con la red PSTN se necesita configurar una dirección IP pública, así como su mascara y puerta de salida entre otras



Configuración LAN: El equipo deberá ser configurado de igual manera con su dirección IP de la red privada así como su mascara y otras configuración es de red.



Configuración del servidor de telefonía por Internet: Existen varias empresas en Internet dedicadas a brindar el servicio de llamadas telefónicas a través de Internet como es el

caso de “net2phone”. En el siguiente cuadro se demostrara una configuración del equipo para que la empresa brinde el servicio requerido.

Firewall

En el Firewall sirve para denegar o autorizar el acceso desde y hacia la LAN privada estableciendo reglas de filtrado. Existen dos maneras de implementar un firewall:

1) Política por defecto ACEPTAR: en principio todo lo que entra y sale por el firewall se acepta y solo se denegará lo que se diga explícitamente.

2) Política por defecto DENEGAR: todo esta denegado, y solo se permitirá pasar por el firewall aquellos que se permita explícitamente.

Ejemplo de reglas de un Firewall

Para el ejemplo de nuestras reglas de seguridad bloquearemos los puertos 5060, 1720 y 1719 que utilizan los protocolos SIP y H.323 de VoIP y los reemplazaremos por números al azar para evitar ataques mediante esos puertos.

```
#!/bin/sh
## SCRIPT de IPTABLES – ejemplo del manual de iptables
## con política por defecto DROP
echo -n Aplicando Reglas de Firewall...
PUERTOS_UDP="5060 1720 1719"
PUERTOS_VoIP="3333 5555 5556"
## FLUSH de reglas
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
## Establecemos politica por defecto
iptables -P INPUT DROP
iptables -P OUTPUT DROP
iptables -P FORWARD DROP
.....................
# Cerramos los puertos UDP que se utilizan por defecto en VoIP#
for j in $PUERTOS_UDP
do
        iptables -A INPUT -m state --state NEW -p udp --dport $j -j DROP
        iptables -A OUTPUT -m state --state NEW -p udp --dport $j -j DROP
        iptables -A FORWARD -m state --state NEW -p udp --dport $j -j DROP
done
# Para el ejemplo abrimos puertos a lazar los cuales configuramos
# previamente en los servidores y en los telefonos #
for k in $PUERTOS_VoIP
do
        iptables -A INPUT -m state --state NEW -p udp --dport $k -j ACCEPT
        iptables -A OUTPUT -m state --state NEW -p udp --dport $k -j ACCEPT
        iptables -A FORWARD -m state --state NEW -p udp --dport $k -j ACCEPT
done
```