VOZ SOBRE IP

MARILYN LORENA CASTRO
GARDEL ALFREDO JURADO
PATRICIA YALILE ARTEAGA

INSTITUTO TECNOLOGICO DEL PUTUMAYO
TECNOLOGIA EN PROGRAMACION Y SISTEMAS
MOCOA
2007

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En el presente trabajo se expone el trabajo investigativo realizado acerca de la tecnología Voz Sobre IP, la cual conjuga dos mundos históricamente separados: la transmisión de voz y la de datos. Se trata de transportar la voz, previamente convertida a datos, entre dos puntos distantes. Esto posibilitaría utilizar las redes de datos para efectuar las llamadas telefónicas, y desarrollar una única red que se encargue de cursar todo tipo de comunicación, ya sea vocal o de datos. Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier operador que ofrezca ambos servicios.

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas.

Con la realización del presente trabajo esperamos brindar una documentación valiosa que contribuya a ampliar en mayor escala el estudio de la tecnología de Voz sobre IP, el cual es un tema de actualidad y que día a día esta tomando mayor auge a nivel mundial. De igual forma es un aporte de nuestro grupo investigativo a las futuras generaciones de Técnicos e Ingenieros en Sistemas Computacionales de nuestro Instituto Tecnológico del Putumayo, y en especial para la Tecnología en Programación y Sistemas.

2. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS

2. 1. OBJETIVO GENERAL

Profundizar los conocimientos sobre la transmisión de voz en redes y de Voz sobre IP; su evolución a partir de los sistemas tradicionales; las tecnologías utilizadas, criterios de implicaciones de diseño, calidad de servicio, aspectos regulatorios y estándares.

2.2. OBJETIVOS ESPECÍFICOS

- Determinar los mecanismos empleados para garantizar la seguridad de las comunicaciones sobre IP.
- Demostrar que las tecnologías de comunicación cada día convergen más hacia la red Internet.
- Mostrar las ventajas y desventajas de VoIP sobre la telefonía convencional.
- Analizar la calidad de servicio en las comunicaciones IP.
- Presentar la forma de direccionamiento en la transmisión de voz sobre IP.
- Indicar la manera en la que la señalización es utilizada en VoIP.
- Analizar el procedimiento de trasporte y los procesos asociados a la transmisión de una llamada sobre IP.

3. CONCEPTOS FUNDAMENTALES DE LA TECNOLOGIA VOZ SOBRE IP

Como tecnología, la Voz sobre IP (VoIP) lleva varios años de presencia en el mercado. Sin embargo, no ha sido hasta la emergencia de nuevos e innovadores servicios basados en esta tecnología que la integración de datos y voz se ha hecho realidad, lo que, para las empresas, ha significado un ahorro de costos y unas comunicaciones más eficientes y efectivas.

Se prevé que en el año 2010 el mercado VoIP moverá más de 10.000 millones de dólares, especialmente desde el momento en que las percepciones del mundo corporativo le son más favorables.

3.1 CONCEPTOS – VOIP

3.1.1 Definición

Los productos de telefonía por Internet se denominan: Telefonía IP (IP telephony) Voz sobre Internet -Voice over the Internet (VOI)- o Voz sobre IP -Voice over IP (VOIP).

FIGURA 1

La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos. La Telefonía IP es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un

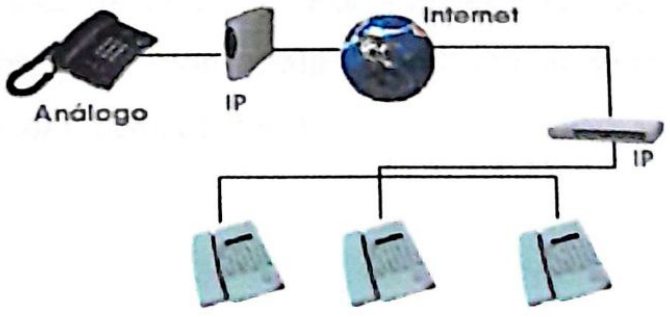
PC, Gateway y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportados vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

La VoIP (Voz sobre IP) esta sigla designa la tecnología empleada para enviar información de voz en forma digital en paquetes discretos a través de los protocolos de Internet (IP significa Protocolo de Internet), en vez de hacerlo a través de la red de telefonía habitual. Antes de seguir, tal vez sea conveniente aclarar qué es un protocolo de conexión. Un protocolo de conexión es un conjunto de normas, un "lenguaje en común" que ambas partes acuerdan utilizar para poder comunicarse, es como decir: Ahora vamos a comunicarnos en inglés, y nos ponemos de acuerdo en que "esto es inglés", o sea es una convención.

La industria de Voz sobre IP se encuentra en una etapa de crecimiento rápido. La evolución del uso de Voz sobre IP vendrá con la evolución de la infraestructura y de los protocolos de comunicación. En el año 2010, una cuarta parte de las llamadas mundiales se basarán en IP.

A lo largo del tiempo, las aplicaciones de voz y datos han requerido redes distintas que usan tecnologías diferentes. Sin embargo, últimamente se han realizado numerosos esfuerzos para encontrar una solución que proporcione un soporte satisfactorio para ambos tipos de transmisión sobre una sola red.

La Voz sobre IP es una tecnología de telefonía que puede ser habilitada a través de una red de datos de conmutación de paquetes, vía el protocolo IP (Protocolo de Internet). La ventaja real de esta tecnología es la transmisión de voz de forma gratuita, ya que viaja como datos.



La tecnología VoIP puede revolucionar las comunicaciones internas al ofrecer:

- Acceso a las redes corporativas desde pequeñas sedes a través de redes integradas de voz y datos conectadas a sucursales.
- Directorios corporativos basados en la Intranet con servicios de mensajes y números personales para quienes deben desplazarse.
- Servicios de directorio y de conferencias basadas en gráficos desde el sistema de sobremesa.
- Redes privadas y gateways virtuales gestionados para voz que sustituyen a las Redes Privadas Virtuales (VPN).

VoIP (Voz sobre IP) brinda nuevas oportunidades para quienes sean capaces de preverlas y actúen con la rapidez suficiente para superar la confusión que envuelve esta extraordinaria tecnología.

Como se usa la Voz sobre IP

Es importante conocer como se usa esta tecnología de VoIP (Voz sobre IP), básicamente hay que comprar un dispositivo que visualmente es una cajita negra que se conecta por un lado al aparato telefónico y por el otro a la PC (computadora), aunque también hay disponibles teléfonos IP. Por supuesto se necesita instalar un software para que dicho dispositivo funcione. Este dispositivo casi siempre se vende en los mismos comercios que venden computadoras.

Hay dos posibilidades de conexión:

- Una de las partes tiene VoIP (Voz sobre IP) y la otra no.
- Ambas partes tienen VoIP (Voz sobre IP)

Si ambas partes tienen VoIP (Voz sobre IP) la llamada es totalmente gratuita, pues se llama de VoIP (Voz sobre IP) a VoIP (Voz sobre IP); sólo tiene que discar el número telefónico y nada más.

Si sólo quien llama tiene VoIP (Voz sobre IP), entonces hace uso de una tarjeta que se compra online (en línea). La mencionada tarjeta no es una tarjeta de plástico o de cartón como las que se venden en los comercios, mas bien es una tarjeta virtual que se compra y carga por Internet. Uno de los proveedores de esta tarjeta prepaga es: Innosphere cuya dirección electrónica es:
http://www.innosphere.net/customer_center.html.

Es necesario aclarar que se puede instalar un VoIP (Voz sobre IP) aunque tenga una central telefónica y más de una línea de teléfono, pues se puede designar una línea para que trabaje directamente con el VoIP (Voz sobre IP), sin perjuicio de seguir utilizándola normalmente.

El VoIP (Voz sobre IP) es una buena alternativa para quien tiene oficinas en el exterior y hace llamadas de larga distancia diariamente o de mucha duración.

3.1.2.Elementos de la Voz sobre IP

El modelo de Voz sobre IP está formado por tres principales elementos:

- **El cliente.** Este elemento establece y termina las llamadas de voz. Codifica, empaqueta y transmite la información de salida generada por el micrófono del usuario. Asimismo, recibe, decodifica y reproduce la información de voz de entrada a través de los altavoces o audífonos del usuario. Cabe destacar que el elemento cliente se presenta en dos formas básicas: la primera es una suite de software corriendo en una PC que el usuario controla mediante una interfase gráfica (GUI); y la segunda puede ser un cliente "virtual" que reside en el gateway.

- **Servidores.** El segundo elemento de la Voz sobre IP está basado en servidores, los cuales manejan un amplio rango de operaciones complejas de bases de datos, tanto en tiempo real como fuera de él. Estas operaciones incluyen validación de usuarios, tasación, contabilidad, tarificación, recolección, distribución de utilidades, enrutamiento, administración general del servicio, carga de clientes, control del servicio, registro de usuarios y servicios de directorio entre otros.
- **Gateways.** El tercer elemento lo conforman los gateways de Voz sobre IP, los cuales proporcionan un puente de comunicación entre los usuarios. La función principal de un gateway es proveer las interfases con la telefonía tradicional apropiada, funcionando como una plataforma para los clientes virtuales. Estos equipos también juegan un papel importante en la seguridad de acceso, la contabilidad, el control de calidad del servicio (QoS; Quality of Service) y en el mejoramiento del mismo.

3.1.3 Características de Voz sobre IP

Por su estructura el estándar proporciona las siguientes características:

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.
- 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 la integración con las grandes redes de IP actuales.
    - Es independiente del hardware utilizado.

- Permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

3.1.4 Protocolos de Voz sobre IP

Hoy en día, existen dos protocolos para transmitir voz sobre IP, ambos definen la manera en que los dispositivos de este tipo deben establecer comunicación entre sí, además de incluir especificaciones para codecs (codificador-decodificador) de audio para convertir una señal auditiva a una digitalizada compresa y viceversa.

3.1.4.1 H.323

H.323 es el estándar creado por la Unión Internacional de Telecomunicaciones (ITU) que se compone por un protocolo sumamente complejo y extenso, el cual además de incluir la voz sobre IP, ofrece especificaciones para vídeo-conferencias y aplicaciones en tiempo real, entre otras variantes.

3.1.4.2 Session Initiation Protocol (SIP)

Sesión Initiation Protocol (SIP) fue desarrollado por la IETF (Internet Engineering Task Force) específicamente para telefonía IP, que a su vez toma ventaja de otros protocolos existentes para manejar parte del proceso de
conversión, situación que no se aplica en H.323 ya que define sus propios protocolos bases.

3.1.5 El Estándar Voz sobre IP

Desde hace tiempo, los responsables de comunicaciones de las empresas tienen en mente la posibilidad de utilizar su infraestructura de datos, para el transporte del tráfico de voz interno de la empresa. No obstante, es la aparición de nuevos estándares, así como la mejora y abaratamiento de las tecnologías de compresión de voz, lo que está provocando finalmente su implantación.

Después de haber constatado que desde un PC con elementos multimedia, es posible realizar llamadas telefónicas a través de Internet, podemos pensar que la telefonía en

IP es poco más que un juguete, pues la calidad de voz que obtenemos a través de Internet es muy pobre. No obstante, si en nuestra empresa disponemos de una red de datos que tenga un ancho de banda bastante grande, también podemos pensar en la utilización de esta red para el tráfico de voz entre las distintas delegaciones de la empresa. Las ventajas que obtendríamos al utilizar nuestra red para transmitir tanto la voz como los datos son evidentes:

- Ahorro de costes de comunicaciones pues las llamadas entre las distintas delegaciones de la empresa saldrían gratis.

Realmente la integración de la voz y los datos en una misma red es una idea antigua, pues desde hace tiempo han surgido soluciones desde distintos fabricantes que, mediante el uso de multiplexores, permiten utilizar las redes WAN de datos de las empresas (típicamente conexiones punto a punto y frame-relay) para la transmisión del tráfico de voz. La falta de estándares, así como el largo plazo de amortización de este tipo de soluciones no ha permitido una amplia implantación de las mismas.

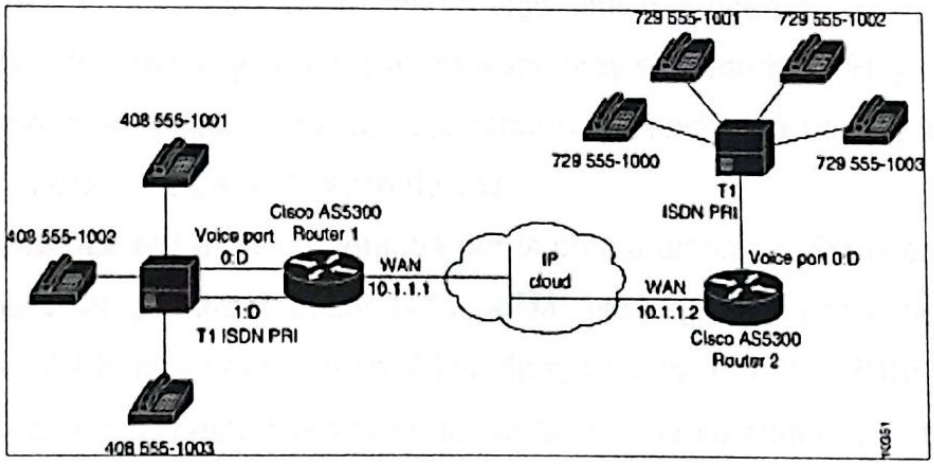


FIGURA 5

Figura. 5 Ejemplo de red con conexión de centralitas a routers que disponen de soporte VoIP

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP (Voz sobre IP), no podía hacerse esperar. La aparición del VoIP (Voz sobre IP) junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías. Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP (Voz sobre IP) de fabricantes como Cisco Systems o Nortel-Bay Networks. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

Por lo dicho hasta ahora, vemos que nos podemos encontrar con tres tipos de redes IP:

- **Internet.** El estado actual de la red no permite un uso profesional para el tráfico de voz.
- **Red IP Pública.** Los operadores ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local en lo que al tráfico IP se refiere. Se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad. Hay operadores que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- **Intranet.** La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet conmutada, ATM, etc.) que se interconectan mediante redes WAN tipo Frame-Relay/ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

A finales de 1997 el VoIP Forum del IMTC ha llegado a un acuerdo que permite la interoperabilidad de los distintos elementos que pueden integrarse en una red VoIP (Voz sobre IP). Debido a la ya existencia del estándar H.323 del ITU, que cubría la mayor parte de las necesidades para la integración de la voz, se decidió que el H.323

fuera la base del VoIP (Voz sobre IP). De este modo, el VoIP(Voz sobre IP) debe considerarse como una clarificación del H.323, de tal forma que en caso de conflicto, y a fin de evitar divergencias entre los estándares, se decidió que H.323 tendría prioridad sobre el VoIP (Voz sobre IP). El VoIP (Voz sobre IP) tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, codificación de la voz y direccionamiento, estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).
El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- **Direccionamiento:**

1. RAS (Registration, Admision and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

- **Señalización:**

1. Q.931 Señalización inicial de llamada.
2. H.225 Control de llamada: señalización, registro y admisión, y paquetización/ sincronización del stream (flujo) de voz.
3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.

- **Compresión de voz:**

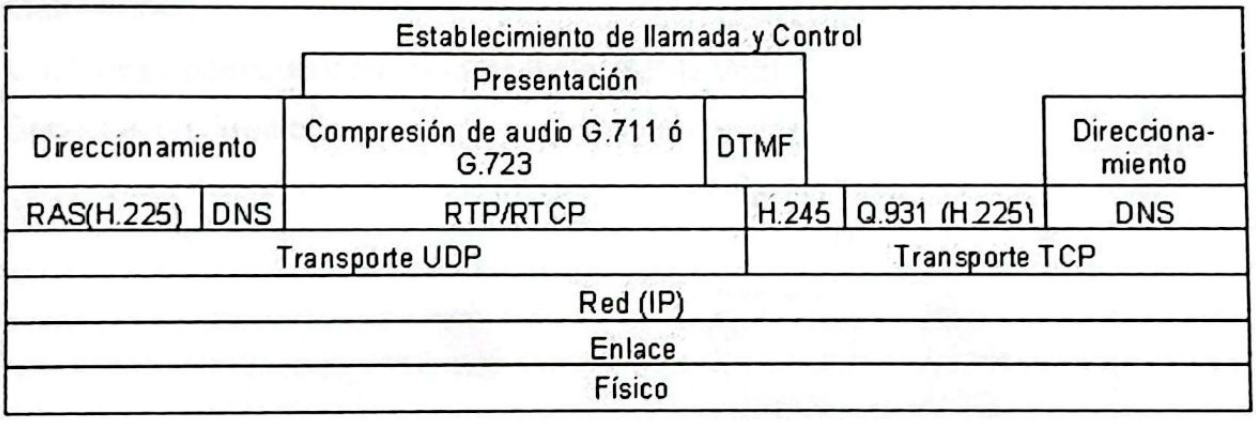
1. Requeridos: G.711 y G.723.
2. Opcionales: G.728, G.729 y G.722.

- **Transmisión de voz:**

1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

- **Control de la transmisión:**

1. RTCP (Real Time Control Protocol). Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras.



Pila de protocolos en VoIP (Voz sobre IP)

Hasta ahora hemos visto la posibilidad de utilizar nuestra red IP para conectar las centralitas a la misma, pero el hecho de que VoIP se apoye en un protocolo de nivel 3, como es IP, nos permite una flexibilidad en las configuraciones que en muchos casos está todavía por descubrir. Una idea que parece inmediata es que el papel tradicional de la centralita telefónica quedaría distribuido entre los distintos elementos de la red VoIP. En este escenario, tecnologías como CTI (computer-telephony integration)

tendrán una implantación mucho más simple. Será el paso del tiempo y la imaginación de las personas involucradas en estos entornos, los que irán definiendo aplicaciones y servicios basados en VoIP.

Actualmente podemos partir de una serie de elementos ya disponibles en el mercado y que, según diferentes diseños, nos permitirán construir las aplicaciones VoIP.

Estos elementos son:

Teléfonos IP.

Adaptadores para PC.

Hubs Telefónicos.

Gateways (pasarelas RTC / IP).

Gatekeeper.

Unidades de audioconferencia múltiple. (MCU Voz)

Servicios de directorio

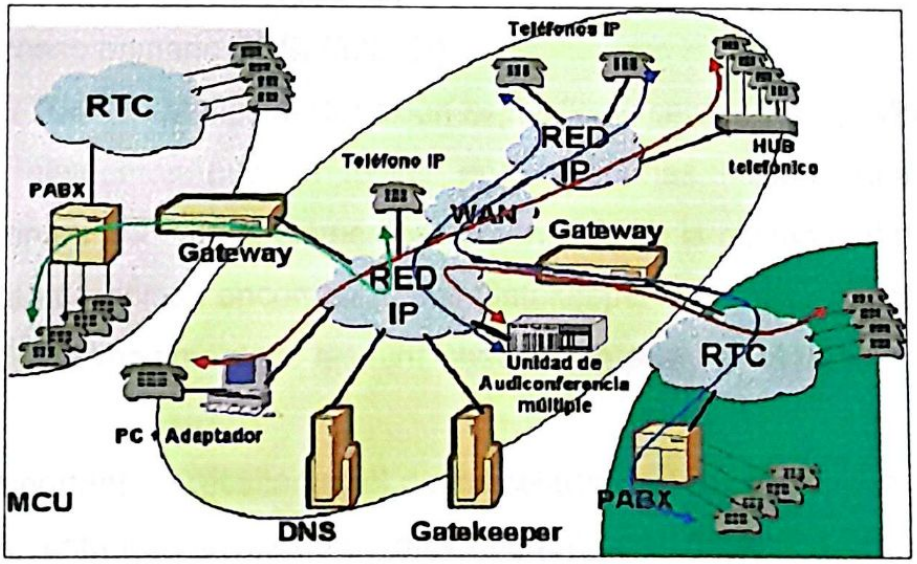


FIGURA 6

3.1.6 Funciones de los Elementos de una red VoIP (Voz sobre IP – Figura 6)

Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura anterior, si bien merece la pena recalcar algunas ideas.

El Gatekeeper es un elemento opcional en la red, pero cuando está presente, todos los demás elementos que contacten dicha red deben hacer uso de él. Su función es la de gestión y control de los recursos de la red, de manera que no se produzcan situaciones de saturación de la misma.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o RDSI. Podemos considerar al Gateway como una caja que por un lado tiene una interfase LAN y por el otro dispone de uno o varios de las siguientes interfaces:

- FXO. Para conexión a extensiones de centralitas ó a la red telefónica básica.
- FXS. Para conexión a enlaces de centralitas o a teléfonos analógicos.
- E&M. Para conexión específica a centralitas.
- BRI. Acceso básico RDSI (2B+D).
- PRI. Acceso primario RDSI (30B+D).
- G703/G.704. (E&M digital) Conexión especifica a centralitas a 2 Mbps.

Los distintos elementos pueden residir en plataformas físicas separadas, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway. También podemos ver cómo Cisco ha implementado las funciones de Gateway en el router.

Un aspecto importante a resaltar es el de los retardos en la transmisión de la voz. Hay que tener en cuenta que la voz no es muy tolerante con estos. De hecho, si el retardo introducido por la red es más de 300 milisegundos, resulta casi imposible tener una conversación fluida. Debido a que las redes de área local no están preparadas en principio para este tipo de tráfico, el problema puede parecer grave. Hay que tener en

cuenta que los paquetes IP son de longitud variable y el tráfico de datos suele ser a ráfagas. Para intentar obviar situaciones en las que la voz se pierde porque tenemos una ráfaga de datos en la red, se ha ideado el protocolo RSVP, cuya principal función es trocear los paquetes de datos grandes y dar prioridad a los paquetes de voz cuando hay una congestión en un router. Si bien este protocolo ayudará considerablemente al tráfico multimedia por la red, hay que tener en cuenta que RSVP no garantiza una calidad de servicio como ocurre en redes avanzadas tales como ATM que proporcionan QoS de forma estándar.

Podemos resumir diciendo que VoIP es una tecnología que tiene todos los elementos para su rápido desarrollo. Como muestra podemos ver que compañías como Cisco, la han incorporado a su catálogo de productos, los teléfonos IP están ya disponibles y los principales operadores mundiales, así como Telefónica, están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado tenemos ya un estándar que nos garantiza interoperabilidad entre los distintos fabricantes. La conclusión parece lógica: hay que estudiar cómo podemos implantar VoIP en nuestra red.

Arquitectura de red

El propio estándar define tres elementos fundamentales en su estructura:

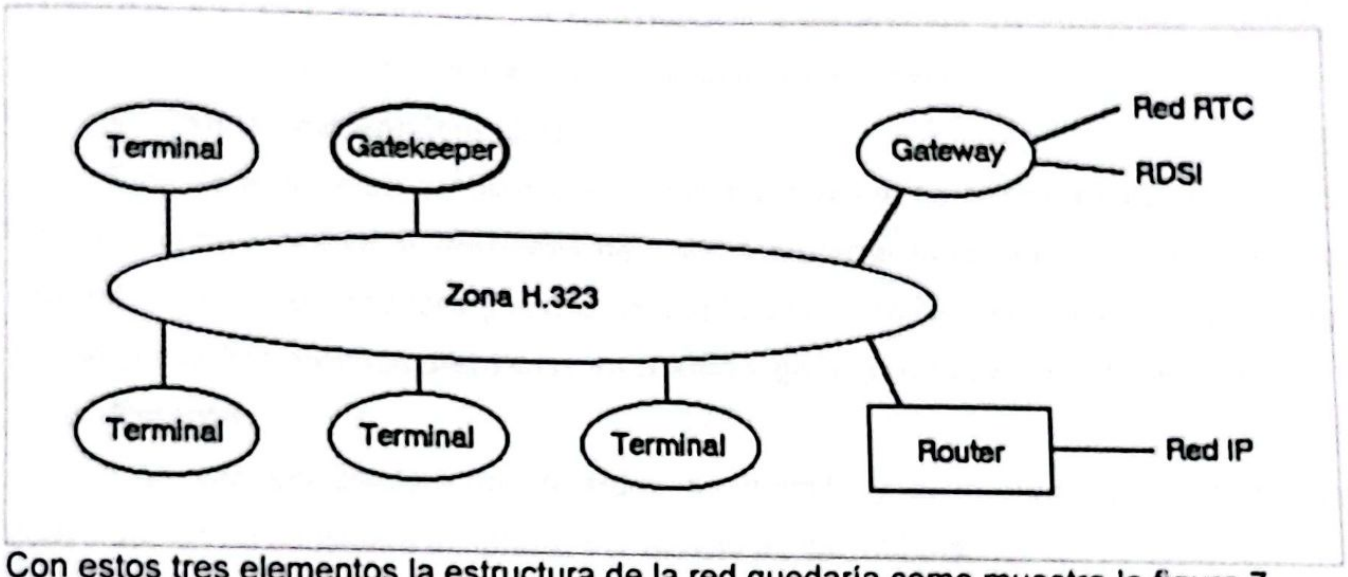
- **Terminales:** Son los sustitutos de los actuales teléfonos. Se pueden implementar tanto en software como en hardware. Algunos ejemplos de Hardware:

Teléfono IP 

Video Teléfono IP 

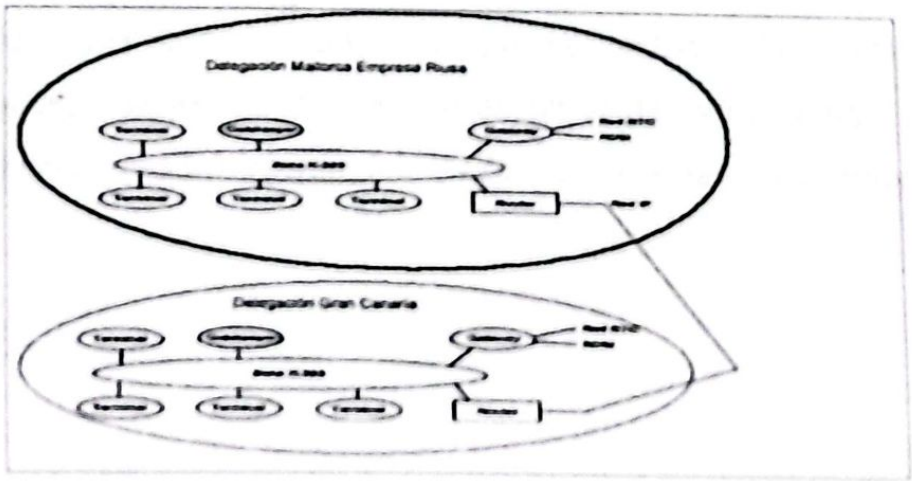
- **Gatekeepers:** Son el centro de toda la organización VoIP, y serian el sustituto para las actuales centralitas. Normalmente implementadas en software, en caso de existir, todas las comunicaciones pasarían por él.

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



Con estos tres elementos la estructura de la red quedaría como muestra la figura 7

El Gateway sirve de enlace entre la RTC /RDSI y la zona H.323 (VoIP). A su vez existe un Gatekeeper que realiza el control de llamadas y la gestión del sistema de direccionamiento. El router permitiría enlazar con otras redes H.323 sin necesidad de utilizar la RTC, resultando todas las llamadas a zonas H.323 totalmente gratuitas, con la ventaja de ahorro de costos que esto supone para las empresas.



La figura 8: muestra la conexión entre dos delegaciones de una misma empresa conectadas mediante VoIP. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas. Este mismo esquema se podría aplicar para proveedores, con el consiguiente ahorro que esto conlleva.

Como hemos visto VoIP presenta una gran cantidad de ventajas, tanto para las empresas como para los usuarios comunes. La pregunta sería ¿por qué no se ha implantado aún esta tecnología?. A continuación analizaremos los aparentes motivos, por los que VoIP aún no se ha impuesto a las telefonías convencionales.

- **Calidad del Servicio (QoS)**

Este es el principal problema que presenta hoy en día la implantación tanto de VoIP como de todas las aplicaciones de XoIP. 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.

- **Retardo:**

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

- **Calidad de 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. Las tendencias actuales son: CQ (Custom Queuing). Asigna un porcentaje del ancho de banda disponible. PQ (Priority Queuing). Establece prioridad en las colas. WFQ (Weight Fair Queuing). Se asigna la prioridad al tráfico de menos carga. DiffServ: Evita tablas de encaminados intermedios y establece decisiones de rutas por paquete.

- La implantación de IPv6 que proporciona mayor espacio de direccionamiento y la posibilidad de tunneling.

4. INICIOS DE LA TECNOLOGÍA DE VOZ SOBRE IP

4.1 Inicios

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

4.2 Mercado de Servicios de la Voz sobre IP: es tan solo el comienzo

Evolución del mercado de la Voz sobre IP	
1995	Año del aficionado
1996	Año del cliente
1997	Año del gateway
1998	Año del gatekeeper
1999	Año de la aplicación

A fines de 1996, la Voz sobre IP aún era considerada una especie de "radio de aficionados" en Internet, una aplicación para un pequeño grupo de amateurs que poseían estaciones de trabajo con PC (Computadora) ataviadas con configuraciones elaboradas de parlantes, micrófonos y shareware de Voz sobre IP (VoIP). La calidad

era terrible, no existían normas, y para poder hablar con alguien era necesario llamar primero por teléfono de la manera tradicional para averiguar si estaban conectados.

4.2.1 Las Primeras Barreras

Tráfico mundial de voz sobre IP por región, 1997-2005

A pesar de que en ese año (1996) proliferó el software nuevo de VoIP (Voz sobre IP) para clientes, la falta de normas y la necesidad de utilizar una tosca PC (computadora) como dispositivo de usuario final desalentaron a los primeros posibles seguidores que esperaban calidad y eficiencia así como originalidad. La tecnología de VoIP (Voz sobre IP) para el mercado empresarial era prácticamente inexistente y los primeros gateways (dispositivos de acceso que pasan las llamadas hacia y desde Internet u otras redes IP, que permiten utilizar teléfonos convencionales) estaban muy lejos de la "clase carrier".

Pero no cabe duda de que las cosas hayan cambiado. Varios años de investigación y desarrollo intensos en todas las áreas de las industrias de las redes y las telecomunicaciones dieron lugar a un mercado en el cual las grandes empresas telefónicas tradicionales no sólo reconocen que la telefonía sobre IP es viable sino que también la están adoptando. Hoy en día, la telefonía sobre IP no constituye una simple fuente potencial de ingresos para los proveedores de servicios de todas las formas y tamaños; los analistas y los actores industriales la consideran cada vez más el nuevo paradigma de las comunicaciones de voz y datos del próximo siglo.

4.2.2 El Mercado Decide

Al lograr normas de interoperabilidad y la existencia de gateways de clase carrier disponibles, los proveedores de equipos y servicios por igual pueden concentrarse en desarrollar las aplicaciones de valor agregado que se necesitan para llevar la demanda de la telefonía sobre IP más allá de su uso inicial como una alternativa de bajo costo ante los servicios tradicionales de larga distancia. Se estima que el mercado de los servicios de telefonía sobre IP superará los $7.000 millones para el año 2005. La

empresa International Data Corp. informó que para el año 2000 los servicios de telefonía sobre IP alcanzaron el mercado mundial de $8.500 millones, y para el2002 alcanzando la cifra de $24.000 millones.

4.3 Comparación Voz sobre IP y Telefonía Tradicional

Voz sobre IP es transmitir Voz utilizando IP. Si bien es una tecnología novedosa, tiene muchas características similares y otras diferentes a las de la telefonía tradicional.
Por eso, a continuación se explica brevemente el esquema de una red telefónica tradicional, y luego las coincidencias y diferencias con la tecnología de Voz sobre IP (Voz sobre IP).

4.3.1 Telefonía Tradicional

El servicio telefónico es, junto con la red eléctrica, uno de los más confiables que conocemos y usamos, ya que todo es muy redundante y está pensado para funcionar siempre. Una central telefónica esta diseñada para minimizar los tiempos de interrupción del servicio.

Es una tecnología en que la interfaz es muy importante, la gente la conoce, espera que cuando levanta el tubo se escuche el tono, y si no es el mismo que el que esperaba escuchar, molesta; además es muy universal y difundida. Todo esto se tiene en cuenta a la hora de prestar el servicio telefónico.

4.3.2 Arquitectura de una Central Telefónica

Todos tenemos un teléfono en nuestra casa. Y, en general, sabemos que el cable del teléfono tiene una ficha (RJ-11) parecida a la del cable de red, y que dentro tiene dos cables de cobre, al que se denomina par telefónico. Ese par telefónico es el que va hasta la central telefónica, a una placa que se la suele denominar placa de abonado. Es la placa que controla nuestra línea.

En realidad, puede controlar muchas líneas, no una sola, y tiene una densidad de puertos que depende del fabricante, ronda entre los 8 y 16 abonados (a veces más, a veces menos). El valor exacto depende del equipo en particular. La central telefónica es un conjunto de equipos relacionados. Todo este conjunto forma un equipo muy grande que puede llegar a ocupar varias habitaciones.

Como mencionamos, las centrales telefónicas suelen estar diseñadas para tener una muy alta disponibilidad (se suele decir que son carrier class, dado que se dice están disponibles el 99.9% del tiempo, que representa alrededor de 5 minutos al año de interrupción de servicio). Para lograr este objetivo, cuentan con redundancia en múltiples niveles (procesadores, enlaces, etc.); y en general se conectan a un sistema de energía interrumpida, que tiene un buen número de baterías que se conectan a un grupo electrógeno que se activa cuando se corta la luz.

4.3.3 Procesamiento de Llamadas

Hasta la central, la voz va en forma analógica. Actualmente ya no existen centrales analógicas, todo lo que hay desde que llega la señal a la central y sale de la otra central hacia el otro abonado, es digital.

La placa de abonado es la que se encarga de hacer la conversión de una señal analógica a una digital y viceversa. La señal se convierte a un PCM de 64kbps, que es una señal digital sin pérdida de información y sin compresión, es el formato que se está utilizando desde prácticamente sus comienzos. También es la placa de abonado la que decodifica los tonos de discado (DTMF). Es decir que, se utiliza el concepto de señalización en banda: comandar a la central utilizando la misma banda por la que se habla.

4.3.4 Conexión entre Centrales

La llamada que sale de nuestra central tiene que llegar hasta la central donde está la persona con la que queremos hablar. No hay doscientos millones de cables entre una y

otra, sino que hay un enlace, el cual puede ser de diversos tipos. Este enlace se debe multiplexar para que todos los abonados de la central puedan hablar por teléfono.
Esta multiplexación es la que hace una diferencia a la hora de la calidad del servicio para el usuario. El sistema de multiplexación que utilizan las centrales telefónicas se llama TDM: Time División Multiplex. Consiste en dividir el stream de datos en partes iguales de 64k (llamadas time-slots), de manera que los datos correspondientes al primer abonado van en el primer time-slot, los correspondientes al segundo en el segundo, y así sucesivamente.
Suponiendo un enlace de 2 Mbps de ancho de banda, como se transmiten 64k, podría haber hasta 32 abonados hablando a la vez. Con esta multiplexación en tiempo se separan y luego vuelven a unir los streams de voz que van de una central a otra, de manera transparente para el que lo está utilizando.
Lo bueno de esta tecnología es que como se divide por un tiempo fijo, se puede garantizar el time-slot y saber que siempre lo que corresponde al primer abonado va en el primer time-slot y así. Una vez establecida la comunicación, sea de acá a una cuadra o de acá a China, está garantizado el ancho de banda necesario para poder hablar sin interrupciones.
Esto, en particular, es muy opuesto a lo que es IP, o cualquier enlace de paquetes en los que pueda haber colisiones, se pierdan paquetes, etc. Ya que en esos enlaces es muy difícil garantizar que la calidad inicial se mantenga a lo largo de toda la conversación, puede pasar que haya paquetes que lleguen antes que otros, que se sature la conexión y muchos otros factores que afectan a la calidad final del audio.
En definitiva, TDM es una de las diferencias esenciales entre la telefonía común y la de Voz sobre IP, permite tener una red predictiva y garantizar calidad.

4.3.5 Ruteo, Señalización y Protocolos

Un tema importante es el "ruteo" entre centrales, es decir, como sabe la central del abonado con que central se tiene que conectar.

Vamos a denominar señalización a la información relacionada con una llamada que se transmite entre dos equipos (la definición en sí es mas amplia, pero esto es en particular lo mas relevante para el caso). Podemos dividirla en dos grupos: la que refiere al abonado y las llamadas en sí (levantó, marcó, cortó), y otra parte entre las centrales (que se le caiga algo y le quiera avisar, etc).

A través de la señalización, la central puede ubicar a qué otra central tiene que llamar, a qué abonado dentro de esa central hay que llamar, saber que se cortó la comunicación, que dio ocupado, etc.

Las centrales entre sí se comunican utilizando diversos protocolos, los cuales generalmente son estándares públicos, aunque en muchos casos las especificaciones no son fáciles (o baratas) de conseguir. Los protocolos más comunes son tres: R2, PRI y SS7.

R2 es uno de los mas viejos y tiene muchas variantes distintas, hay -incluso- una variante Argentina, y pasa toda su información utilizando 4 bits. SS7 es, por otra parte, uno de los más nuevos y complejos.

Se necesita que las dos centrales que se están queriendo comunicar puedan hablar un mismo protocolo, de manera que si se quieren intercomunicar dos centrales que no soportan los mismos protocolos, es necesario que utilicen una central intermedia que traduzca la información.

Acerca del enlace por el cual se pasa tanto la señalización como la voz en sí, existen muchísimos tipos. Los más conocidos y comunes son E1 o E3 (europeos), con sus variantes T1 o T3 (utilizadas principalmente en los Estados Unidos). Son cables de cobre, muy parecidos al cable coaxial, que pueden ser de 75 o 120 ohms. El E1 tiene 2Mbps (32 canales de 64kbps), el E3 tiene 32Mbps (512 canales de 64kbps).

En muchos ámbitos cuando se habla de este tipo de enlaces se le da importancia solo al ancho de banda; sin embargo en nuestro caso también nos interesa el número de times-lots en el cual se puede dividir.

Sin embargo, no se pueden ocupar todos los canales para pasar todos los abonados. En necesario poder avisar que hay llamadas y ese tipo de información. Por ejemplo, en

el caso de una E1 se suelen utilizar 30 canales para el paso de la voz, 1 para framing (el 0) y 1 para señalización (el 15). En el de framing se suele encontrar (entre otras cosas) el CRC de los otros 31 (aunque depende de la configuración), de manera que si un determinado frame esta corrupto, se lo puede notar y actuar en consecuencia.

4.4 Protocolos Voz sobre IP

Para telefonía IP hay muchos protocolos. Los vamos a separar en 3 partes: codificación de la voz, transmisión de la voz y señalización.

4.4.1 Codificación de la Voz

La transmisión ya no se va a hacer en PCM (protocolo G.711), como en la telefonía tradicional. La voz se puede comprimir: si una persona se queda callada, por ejemplo, no es necesario transmitir el sonido completo del silencio. Hay muchos codecs de compresión. Como todo codec, cuanto más se comprime, más
procesador se necesita. Hay codecs con pérdida que comprimen de 64k a 4k, incluso hasta 3.1k. Hay algunos que son sin pérdida, pero la mayoría son con pérdida.
Hay muchos estudios al respecto, ya que lo más importante es la percepción que tiene la gente de lo que se escucha, y es muy difícil medir la percepción humana. Para la realización de estos estudios, se comprime el audio y se pide a grupos de personas que lo escuchen y que manifiesten si les parece que es de buena calidad o no, se les asignan puntajes, etc.
En general se elige un balance entre compresión y percepción. Hay muchos balances distintos. Hay muchos codecs que están patentados, para los que hay que pagar las licencias de uso (no la implementación, sino el uso en sí). Un ejemplo de un buen codec es el GSM, utilizado en los teléfonos celulares. Es un codec libre, que se escucha bastante bien, comprime bastante bien, y consume muy poco procesador. Que consuma poco procesador es importante cuando se está trabajando a gran escala (200, 1000 líneas). En el caso de los celulares, la voz se comprime en el mismo aparato

celular y se transmite ya comprimida. Para este protocolo, en GNU/Linux existe la libgsm que es una biblioteca pequeña y útil.

4.4.2 señalización

Tal como vimos anteriormente, es necesario tener un protocolo para poder indicar a qué máquina se quiere llamar y demás. Existen actualmente varios protocolos para señalización.

Uno que esta cayendo muy en desuso es el H323. No es lindo, no es fácil, y no anda con NAT; pero es muy importante porque fue el primero que se empezó a usar en VoIP (Voz sobre IP) de forma masiva. Actualmente se está dejando de usar, y probablemente en el futuro no se use más. Los programas NetMeeting, y su equivalente libre GnomeMeeting utilizan este protocolo.

El protocolo que más se está usando actualmente es SIP: Session Initiation Protocol. Se trata de un protocolo que tiene una característica muy particular: está estandarizado por la IETF (Internet Engineering Task Force, es decir, los que hacen las RFCs) y, en consecuencia, es muy abierto y de fácil acceso.

SIP es un protocolo de texto plano que se utiliza sobre TCP, ya que en el caso de la señalización es importante que no se pierda la información. Tiene una arquitectura que está muy bien pensada, no trata de meter todo el mundo telefónico

en IP, ni todo IP en el mundo telefónico. Sin embargo, también tiene problemas para atravesar NAT.

Normalmente, cuando se usa SIP, el protocolo que se utiliza para enviar la voz es RTP (Real Time Protocol), que se usa sobre UDP. El programa linphone es un cliente SIP. Existe linphonec para consola (paquete linphone-nox en Debian

4.4.3 Ejemplo de Conexión Voz sobre IP usando IP

A modo de ejemplo, vamos a considerar dos PCs (computadora), que están conectadas a través de Internet. Juan, que está conectado desde una PC (computadora), quiere hablar con María, que está conectada desde otra. A María le llega un invite que le

indica que Juan quiere hablar con ella (equivalente a un RING), y si acepta la comunicación (equivalente a levantar el teléfono), puede hablar con Juan.
La conexión se establece usando SIP sobre TCP y luego la transmisión se hace usando RTP sobre UDP. Cuando se termina la conversación, por SIP se transmite la terminación de la conexión. Esto permite que dos usuarios de PC
(computadoras) puedan hablar por teléfono, sin tener una central telefónica en el medio, utilizando la estructura IP existente para establecer una comunicación.
Durante la inicialización se pasan las IPs y los puertos a utilizar y por eso es que es difícil hacerlo a través de NAT.

4.4.4 Conexión de muchas Computadoras

Si en lugar de 2 PCs (computadoras), se quiere conectar un número importante de computadoras, que quieren hablar entre sí sin tener que estar transmitiéndose los números de IP, y el que les está proveyendo el servicio quiere poder tener un registro de las comunicaciones establecidas, se utiliza un Server SIP (que vendría a ser el equivalente a un Gatekeeper en H323). También se lo suele llamar Proxy SIP o Router SIP, que si bien teóricamente cumplen funciones específicas, en general se utilizan los términos de manera indistinta.
Teniendo un server, cuando Juan quiere hablar por teléfono, le envía una señal al server indicándole que quiere hablar con María, y este le avisa a María que Juan quiere hablar con ella. A partir de que se acepta la comunicación, se pasan algunos mensajes más a través del server (utilizando SIP) para negociar IPs, puertos, protocolo de compresión a utilizar, etc. Pero una vez que comienza la comunicación, el canal UDP ya no pasa por el server. Una vez terminada la conversación, se utiliza SIP para avisar que se terminó la conversación.
Esta es una de las mejores cosas que tiene la telefonía IP, porque por un lado separa la señalización de la transmisión de voz, y por el otro lado la transmisión se hace peer to peer. Pero trae consigo que el server debe confiar en la buena fe de los clientes para saber cuándo una comunicación se terminó realmente.

Un cliente que tenga DHCP tiene que avisarle al server en qué IP está, para esto puede autenticarse contra él, utilizando un nombre de usuario y una clave. De manera que el server puede saber que un determinado usuario no está y poner un contestador, dar ocupado, etc.

Con este principio se puede hacer que un teléfono VOIP (Voz sobre IP) se enchufe en cualquier lugar del mundo donde haya banda ancha y siempre sigue siendo el mismo teléfono. Y de hecho este servicio existe y se vende: Por ejemplo, si a usted le dan una línea en Buenos Aires o en cualquier otro país, y usted quiere llevarse el teléfono VOIP (Voz sobre IP) a cualquier lugar del mundo, lo puede enchufar a un ADSL y puede hablar o lo pueden llamar como si usted estuviera en Buenos Aires.

De la misma manera que con las centrales telefónicas, puede haber varios servers que se comuniquen entre sí, y solamente van a intercambiar la parte correspondiente al protocolo SIP, la parte de RDP/UDP se hace directo entre los
dos puntos que se están comunicando. La implementación de referencia del server SIP es Open Source.

Por otro lado, se puede hablar desde una computadora a teléfonos comunes, para esto se necesita un gateway (gw) que haga la conversión de una tecnología a otra.

4.4.5 Implementaciones

A nivel personal, por ejemplo usted o puede hablar con una tía que viva en algún lugar distante a través de VOIP (Voz sobre IP), y otro día, hablar por teléfono de verdad. Es una opción para ahorrar costos.

Pero, cuando se habla de una implementación a nivel telefonía real (como la de las tarjetas para hacer llamadas baratas) es diferente, tiene que ir por un enlace controlado. Si se tiene un enlace de fibra de Chitré a Panamá, es posible pasar muchos más abonados por el mismo enlace E1 por el que se pasaban 30; pero es necesario poner controles en ambas puntas. Hay que tener mucha inteligencia en los equipos de control. Una posibilidad para tener una red de VOIP (Voz sobre IP) interna, por ejemplo, es tener unos auriculares y un micrófono en cada estación (Computador).

amigos podrán hablar con usted por sólo el costo de una llamada local mientras usted paga por el consumo de minutos.

- **Ahorro en llamadas de larga distancia.**

Las mayores ventajas que va a ver un usuario hogareño es la del ahorro en las llamadas de larga distancia ya que las comunicaciones no dependerán del tiempo en el aire. Es decir no dependerá de la duración de la llamada, como estamos acostumbrados hasta ahora, sino más bien por el precio de mercado del proveedor de Internet, ya que estaremos pagando por un servicio más dentro del paquete de datos que nos brinda la red.

- **Llamadas a teléfonos fijos o celulares.**

Otra gran ventaja de la telefonía IP es que se puede llamar a un teléfono fijo o móvil en cualquier lugar del mundo para transmitir fax, voz, vídeo, correo electrónico por teléfono, mensajería y comercio electrónico. Es decir, la gran variedad de servicios brindados por un solo operador es una de las grandes ventajas que ven los usuarios hogareños y corporativos.

- **Reducción del abono telefónico.**

Además, para el usuario común, este sistema reduce los costos de las llamadas (hasta un 74%), cuyo precio depende del mercado pero no del tiempo de conexión, como sucede en la telefonía tradicional; así, donde antes "cabía" una conversación ahora "caben" 10, lo cual reducirá las tarifas para el usuario final.

- **Mensajería unificada y Correo de voz.**

Cuando está de viaje o fuera de su casa u oficina en vez de marcar su teléfono y clave para escuchar su casilla de mensajes imagínese un sistema telefónico que le proporcione, en su computadora, un listado de esos mensajes y que le permita escucharlos y marcar teléfonos de su libro electrónico de direcciones con un simple click en su ratón. La tecnología VoIP le permite realizar llamadas telefónicas y enviar faxes a través de una red de datos IP como si estuviese utilizando una red tradicional.

- **Ventajas para las empresas.**

Esta convergencia de servicios de voz, datos y vídeo en una sola red implica para una empresa que lo adopte, un menor costo de capital, procedimientos simplificados de soporte y configuración de la red y una mayor integración de las ubicaciones remotas y oficinas sucursales en las instalaciones de la red corporativa. La Telefonía IP utiliza la red de datos para proporcionar comunicaciones de voz a toda la empresa, a través de una sola red de voz y datos.

Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier organización. VoIP proporcionaría a las sucursales de una misma empresa, comunicaciones gratuitas entre ellas, con el ahorro de costes que esto supondría. No solo entre sus sucursales, sino entre proveedores, intermediarios y vendedores finales, las comunicaciones se podrían realizar de forma completamente gratuita. Además, la red de comunicaciones de la empresa se vería enormemente simplificada, ya que no

habría que cablear por duplicado la red, debido a que se aprovecharía la red de datos para voz. Esta capacidad permite a las compañías reducir los costes de fax y teléfono, agrupar los servicios de datos, voz, fax y vídeo, y construir nuevas infraestructuras de red para aplicaciones avanzadas de comercio electrónico.

- **Centros de llamadas por el WEB.**

Partiendo de una tienda que ofrece sus productos en línea, los visitantes de la Web no solo tendrán acceso a la información que la Web les proporciona, sino que además podrían establecer comunicación directa con una persona del departamento de ventas sin necesidad de cortar la conexión. Esta cualidad reduciría el enorme temor del usuario a hacer sus compras por Internet por primera vez. Al establecer una conversación directa, le da una confianza que finalmente supondrá una mejora en su relación con el comercio electrónico.

- **Videoconferencia integrada o Multiconferencia.**

Con los datos de ancho de banda requeridos actualmente (de 8 a 16kbps por llamada), se podrían establecer de 15 a 30 comunicaciones simultáneas con una línea ADSL estándar, que podría satisfacer los requerimientos de una mediana empresa.

- **Posibilidad de usar Push 2 Talk.**

De esta forma, con el simple gesto de pulsar un botón se establece comunicación directa con la persona que lo ha elaborado.

- **Ventajas para los operadores o proveedores del servicio.**

Es obvio que este tipo de redes proporciona a los operadores una relación ingreso/recursos mayor, es decir, con la misma cantidad de inversión en

infraestructura de red, obtienen mayores ingresos con las redes de conmutación de paquetes, pues puede prestar más servicio a sus clientes. Otra posibilidad sería que prestará más calidad de servicio, velocidad de transmisión, por el mismo precio.

4. 5.2 Desventajas

- **Calidad de la comunicación.**

Algunas de sus desventajas son la calidad de la comunicación (ecos, interferencias, interrupciones, sonidos de fondo, distorsiones de sonido, etc.), que puede variar según la conexión a Internet y la velocidad de conexión del Proveedor de servicios de Internet.

Garantizar la calidad de servicio sobre una red IP, actualmente no es posible por los retardos que se presentan en el tránsito de los paquetes y los retardos de procesado de la conversación. Por otro lado el ancho de banda el cual no siempre está garantizado, hace desmejorar el servicio. Estos problemas de calidad en el servicio telefónico en el protocolo IP van disminuyendo a medida que las tecnologías involucradas van evolucionando, ya en los Estados Unidos hay servicios que garantizan una excelente calidad en la comunicación.

- **Conexión a Internet**

Sólo lo pueden usar aquellas personas que posean una conexión con Internet, tengan computadora con módem y una línea telefónica; algunos servicios no ofrecen la posibilidad de que el computador reciba una llamada, ni tampoco funcionan a través de un servidor proxy.

- **Pérdida de información**

Este tipo de redes transportan la información dividida en paquetes, por lo que una conexión suele consistir en la transmisión de más de un paquete. Estos paquetes pueden perderse, y además no hay una garantía sobre el tiempo que tardarán en llegar de un extremo al otro de la comunicación. Imaginemos una conversación de voz en la cual se pierde de vez en cuando información emitida y que sufre retrasos importantes en su cadencia. Si alguna vez han chateado, entenderán la situación. A veces durante estas conversaciones de Chat, recibimos dos o tres preguntas seguidas de nuestro interlocutor, y es que como lo que nosotros escribimos no le llega, pues él sigue con otras preguntas. Estos problemas de calidad de servicio telefónico a través de redes de conmutación de paquetes van disminuyendo con la evolución de las tecnologías involucradas, y poco a poco se va acercando el momento de la integración de las redes de comunicaciones de voz y datos.

- **Incompatibilidad de proveedores del servicio.**

No todos los sistemas utilizados por los Proveedores de Servicios de Telefonía por Internet son compatibles (Gateway, Gatekeeper) entre sí. Este ha sido uno de los motivos que ha impedido que la telefonía IP se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados en el protocolo H.323. El estándar VoIP o protocolo fue definido en 1996 por la ITU (International Telecommunications Union) y proporciona a los diversos fabricantes una serie de normas con el fin de que puedan evolucionar en conjunto. Por su estructura el

estándar proporciona las siguientes ventajas: Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos. Proporciona el enlace a la red telefónica tradicional. Al tratarse de una tecnología soportada en IP es independiente del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales. Es independiente del hardware utilizado. Y permite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.

La promesa de la Voz sobre IP: mejorar la calidad del sonido

Existen opiniones encontradas acerca de la calidad de las llamadas de voz que se realizan por la Internet pública. Vale la pena destacar que los carriers utilizarán particiones de backbones de IP bien diseñadas para transportar el tráfico de voz sobre IP, simplemente debido a que la Internet pública tiene patrones de tráfico impredecibles y no fue desarrollada para manejar el tráfico de la telefonía de clase carrier. La demora y la pérdida de paquetes durante los períodos de alto nivel de tráfico en la Internet pública degradan la calidad del tráfico altamente sensible a las demoras como ocurre en el caso de la voz en tiempo real. La transformación de la voz en la Internet públicas puede mejorarse de manera notoria mediante el uso de algoritmos tales como la corrección de errores sin retorno y la protección de paquetes.

La voz sobre IP pronto podrá proveer una calidad de voz con una fidelidad significativamente superior a la que existe hoy en día.

Las redes analógicas conmutadas por circuitos están limitadas por el legado de la red multiplex por división de tiempo subyacente, que se basa en 8.000 muestras de voz, o cuatro kilohertz, por segundo. Para ponerlo en perspectiva, la voz humana genera hasta 10khz/segundo y el oído humano puede detectar sonidos de hasta 20.000 khz/segundo. Dado que la telefonía sobre IP no está limitada a la multiplexión por división de tiempo, tanto las empresas como los consumidores por igual podrán, en poco tiempo, beneficiarse por una calidad de sonido notablemente superior.

seguridad total mediante la prevención de errores aislados que comprometan o impacten el sistema. Más aún, una política de seguridad integral incluye más que tecnología avanzada de seguridad, comprende procesos operacionales que aseguren un rápido despliegue de parches para los softwares y aplicaciones, instalación de tecnologías de seguridad en el momento adecuado y finalmente la realización y evaluación de auditorias de seguridad. Desde que se despachó el primer Teléfono a la fecha, la seguridad en la telefonía IP ha avanzado vertiginosamente.

Por el contrario, con los sistemas PBX digitales tradicionales, tenemos que protegernos contra el fraude de llamadas, "masquerading" (personas que se hacen pasar por otras para tomar control del sistema PBX) y "war dialing", asimismo los accesos no autorizados pueden ser frecuentemente ejecutados con técnicas tan simples como usar un par de pinzas, pero probablemente no habrá que preocuparse de los gusanos que vienen del Internet. Sin embargo, algunas personas piensan que no es necesario preocuparse de la seguridad de red si se opta por un sistema de telefonía híbrido que son promovidos por fabricantes tradicionales de telefonía.

Típicamente, el primer paso en el proceso de migración a un sistema híbrido es separar el CPU y el procesamiento de llamadas fuera de la "caja" y ponerlo en la red LAN. Es aquí donde tenemos que asegurarnos que la red LAN esta completamente segura, dado que un ataque a los componentes que procesan las llamadas afectaría a cada usuario en el sistema, no solo a los usuarios de los teléfonos IP. En este escenario, no solo es necesario tener las mismas consideraciones de seguridad como cuando todo el sistema estuviese sobre la red IP, sino también es necesario administrar dos redes separadas, sin notar los beneficios de tener una solución integrada en una única red convergente.

Sería una falacia negar que la seguridad no sea un factor importante cuando una empresa decide implementar un sistema de Telefonía IP, ya sea híbrido o IP puro. La compañía Cisco es el único fabricante que aborda la seguridad en todos los niveles de la infraestructura de Comunicaciones IP: red IP, sistemas de voz y aplicaciones,

proveyendo la defensa necesaria para hacer el sistema de Comunicaciones IP tan seguro como estos pueden ser.

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) y SSL 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, IDSs e IDPs combaten las amenazas originadas interna y externamente.

- **Control:** Provisto vía sistemas de identidad y confiabilidad. Servidores de control de acceso y el Network Admission Control (NAC) de la compañía Cisco por ejemplo hacen posible que las organizaciones puedan controlar el acceso a la información, permitiendo que solo la gente correcta pueda tener acceso a la información en el momento correcto.

En el caso de Cisco, las comunicaciones seguras empiezan con los teléfonos IP y el Cisco CallManager (el software de procesamiento de llamadas). Los teléfonos IP de Cisco pueden clasificar automáticamente el tráfico de voz el cual es pasado a una cola de alta prioridad que minimiza la latencia y el jitter. Ellos son el primer punto en el cual la red es dinámicamente particionada en dos redes lógicamente separadas, una para voz y otra para datos. 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. Para una protección adicional, las imágenes del software que corren en los teléfonos IP solo pueden ser instaladas si éstas tienen la firma apropiada. Todo esto

es posible gracias a las capacidades de confiabilidad basadas en certificados digitales y tecnologías relacionadas de autorización y autenticación.

La protección contra amenazas es suministrada en todo el sistema también. En el CallManager, el Cisco Security Agent es usado para la protección contra intrusos y la arquitectura NAC ayuda a que las políticas de seguridad corporativas sean ejecutadas constantemente en toda la red. En la red, los sensores de detección de intrusos del host detectan e identifican actividad inusual y la aísla antes de que ésta pueda afectar a la red. Usando inspección de estado de paquetes, el firewall bloquea puertos de aplicaciones no necesarias y ayuda a asegurar que solo tráfico autorizado es permitido a acceder a segmentos críticos de la red interna.

En unas pruebas de laboratorio realizadas por Miercom (firma independiente especializada en probar y analizar productos de comunicaciones y networking), una solución de Comunicaciones IP de Cisco recibió la más alta calificación posible en seguridad y fue catalogado como la solución de telefonía IP más segura de entre todas las soluciones que pasaron la prueba.

Debido a esta capacidad de las soluciones de Cisco de proveer confiabilidad y seguridad, es posible lograr niveles más altos de seguridad que con sistemas PBX tradicionales basados en TDM. Se ha podido probar que, implementando seguridad siguiendo las guías de diseño de Cisco SAFE, una solución de Comunicaciones IP puede ser la solución de voz (IP) más segura disponible.

5.2 Seguridad en el protocolo VoIP

Consideremos las limitaciones de seguridad en un sistema de Voz sobre IP. En el proceso de ahorrar dinero (factor necesario) e incrementar la eficacia, dos porciones cruciales de cualquier infraestructura, voz y datos, fueron combinadas. Los servidores de VoIP actúan como puertas de enlace; así, routers especiales, teléfonos, nuevos protocolos y sistemas operativos están ahora entremezclándose con esta nueva tecnología.

5. 2.1 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 información sobre una llamada es tan valiosa como el contenido de la voz. Por ejemplo, una señal comprometida en un servidor puede ser usada para configurar y dirigir llamadas, del siguiente modo: una lista de entradas y salidas de llamadas, su duración y sus parámetros. Usando esta información, un atacante puede obtener un mapa detallado de todas las llamadas realizadas en la red, creando grabaciones completas de conversaciones y datos de usuario.

La conversación es en sí misma 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 (public switched telephone network), la disponibilidad era raramente un problema. Pero es mucho más sencillo hackear una red VoIP. Todos estamos familiarizados con los efectos demoledores de los ataques de denegación de servicio. Si se dirigen a puntos clave de la red, podrían incluso destruir la posibilidad de comunicarse 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.

5.2.2 Spoofing

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: 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. Y como los anillos de confianza basados en estas características tan fácilmente falsificables son aún demasiado abundantes, el spoofing sigue siendo en la actualidad un ataque no trivial, pero factible contra cualquier tipo de organización.
Como hemos visto, en el spoofing entran en juego tres máquinas: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el pirata pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque. Probablemente esto último no le sea muy difícil de conseguir: a pesar de que existen múltiples formas de dejar fuera de juego al sistema suplantado - al menos a los ojos del atacado - que no son triviales (modificar rutas de red, ubicar un filtrado de paquetes entre ambos sistemas), lo más fácil en la mayoría de ocasiones es simplemente lanzar una negación de servicio contra el sistema en cuestión. No suele ser difícil "tumbar", o al menos bloquear parcialmente, un sistema medio; si a pesar de todo el atacante no lo consigue, simplemente puede esperar a que desconecten de la red a la máquina a la que desea suplantar (por ejemplo, por cuestiones de puro mantenimiento).

El otro punto importante del ataque, la comunicación falseada entre dos equipos, no es tan inmediato como el anterior y es donde reside la principal dificultad del spoofing. En un escenario típico del ataque, un pirata envía una trama SYN a su objetivo indicando como dirección origen la de esa tercera máquina que está fuera de servicio y que mantiene algún tipo de relación de confianza con la atacada. El host objetivo responde con un SYN+ACK a la tercera máquina, que simplemente lo ignorará por estar fuera de servicio (si no lo hiciera, la conexión se resetearía y el ataque no sería posible), y el atacante enviará ahora una trama ACK a su objetivo, también con la dirección origen de la tercera máquina. Para que la conexión llegue a establecerse, esta última trama deberá enviarse con el número de secuencia adecuado; el pirata ha de predecir correctamente este número: si no lo hace, la trama será descartada, y si lo consigue la conexión se establecerá y podrá comenzar a enviar datos a su objetivo, generalmente para tratar de insertar una puerta trasera que permita una conexión normal entre las dos máquinas.

Podemos comprobar que el spoofing no es inmediato; de entrada, el atacante ha de hacerse una idea de cómo son generados e incrementados los números de secuencia TCP, y una vez que lo sepa ha de conseguir "engañar" a su objetivo utilizando estos números para establecer la comunicación; cuanto más robusta sea esta generación por parte del objetivo, más difícil lo tendrá el pirata para realizar el ataque con éxito. Además, es necesario recordar que el spoofing es un ataque ciego: el atacante no ve en ningún momento las respuestas que emite su objetivo, ya que estas van dirigidas a la máquina que previamente ha sido deshabilitada, por lo que debe presuponer qué está sucediendo en cada momento y responder de forma adecuada en base a esas suposiciones. Sería imposible tratar con el detenimiento que merecen todos los detalles relativos al spoofing.

Para evitar ataques de spoofing exitosos 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. Hasta ahora hemos hablado del ataque genérico contra un host denominado spoofing o, para ser más exactos, IP Spoofing; existen otros ataques de falseamiento relacionados en mayor o menor medida con este, entre los que destacan el DNS Spoofing, el ARP Spoofing y el Web Spoofing.

DNS Spoofing

Este ataque hace referencia al falseamiento de una dirección IP ante una consulta de resolución de nombre (esto es, resolver con una dirección falsa un cierto nombre DNS), o viceversa (resolver con un nombre falso una cierta dirección IP). Esto se puede conseguir de diferentes formas, desde modificando las entradas del servidor encargado de resolver una cierta petición para falsear las relaciones dirección-nombre, hasta comprometiendo un servidor que infecte la caché de otro (lo que se conoce como DNS Poisoning); incluso sin acceso a un servidor DNS real, un atacante puede enviar datos falseados como respuesta a una petición de su víctima sin más que averiguar los números de secuencia correctos.

ARP Spoofing

El ataque denominado ARP Spoofing hace referencia a la construcción de tramas de solicitud y respuesta ARP falseadas, de forma que en una red local se puede forzar a una determinada máquina a que envíe los paquetes a un host atacante en lugar de hacerlo a su destino legítimo. La idea es sencilla, y los efectos del ataque pueden ser muy negativos: desde negaciones de servicio hasta interceptación de datos, incluyendo algunos Man in the Middle contra ciertos protocolos cifrados.

Web Spoofing

Este ataque permite a un pirata visualizar y modificar cualquier página web que su víctima solicite a través de un navegador, incluyendo las conexiones seguras vía SSL. Para ello, mediante código malicioso un atacante crea una ventana del navegador correspondiente, de apariencia inofensiva, en la máquina de su víctima; a partir de ahí, enruta todas las páginas dirigidas al equipo atacado - incluyendo las cargadas en nuevas ventanas del navegador - a través de su propia máquina, donde son modificadas para que cualquier evento generado por el cliente sea registrado (esto implica registrar cualquier dato introducido en un formulario, cualquier click en un enlace, etc.).

5.2.3 Herramientas del Hacker

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además son motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros más gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

Recolección de información

Generalmente, el primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar esta información:

- El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.

- El programa TraceRoute puede revelar el número de redes intermedias y los ruteadores en torno al servidor específico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Servidores DNS pueden accesarce para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

Sondeo del sistema para debilitar la seguridad

Después que se obtienen la información de red perteneciente a dicha organización, el hacker trata de probar cada uno de los servidores para debilitar la seguridad.

Estos son algunos usos de las herramientas que un hacker puede utilizar automáticamente para explorar individualmente los servidores residentes en una red:

- Una vez obtenida una lista no obstantemente pequeña de la vulnerabilidad de servicios en la red, un hacker bien instruido puede escribir un pequeño programa que intente conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor en cuestión. La corrida del programa presenta una lista de los servidores que soportan servicio de Internet y están expuestos al ataque.
- Están disponibles varias herramientas del dominio publico, tal es el caso como el Rastreador de Seguridad en Internet (ISS) o la Herramienta para Análisis de

Seguridad para Auditar Redes (SATAN), el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad. Estos programas determinan la debilidad de cada uno de los sistemas con respecto a varios puntos de vulnerabilidad comunes en un sistema. El intruso usa la información colectada por este tipo de rastreadores para intentar el acceso no autorizado al sistema de la organización puesta en la mira.

Un administrador de redes hábil puede usar estas herramientas en su red privada para descubrir los puntos potenciales donde esta debilitada su seguridad y así determina que servidores necesitan ser remendados y actualizados en el software.

Acceso a sistemas protegidos

El intruso utiliza los resultados obtenidos a través de las pruebas para poder intentar acceder a los servicios específicos de un sistema.

Después de tener el acceso al sistema protegido, el hacker tiene disponibles las siguientes opciones:

- Puede atentar destruyendo toda evidencia del asalto y además podrá crear nuevas fugas en el sistema o en partes subalternas con el compromiso de seguir teniendo acceso sin que el ataque original sea descubierto.
- Pueden instalar paquetes de sondeo que incluyan códigos binarios conocidos como "Caballos de Troya" protegiendo su actividad de forma transparente. Los paquetes de sondeo colectan las cuentas y contraseñas para los servicios de Telnet y FTP permitiendo al hacker expandir su ataque a otras maquinas.
- Pueden encontrar otros servidores que realmente comprometan al sistema. Esto permite al hacker explotar vulnerablemente desde un servidor sencillo todos aquellos que se encuentren a través de la red corporativa.
- Si el hacker puede obtener acceso privilegiado en un sistema compartido, podrá leer el correo, buscar en archivos

5.2.4 Defenderse

Ya hemos hablado de las maravillas de la tecnología de Voz sobre IP, y nos hemos encontrado con graves problemas de seguridad. Afortunadamente, la situación no es irremediable. En resumidas cuentas, los riesgos que comporta usar el protocolo VoIP no son muy diferentes de los que nos podemos encontrar en las redes habituales de IP. Desafortunadamente, en los "rollouts" iniciales y en diseños de hardware para voz, software y protocolos, la seguridad no es su punto fuerte. Pero seamos sinceros; esto es lo que siempre suele pasar cada vez que aparece una nueva tecnología. Examinemos ahora algunas pruebas que puedan alivia las amenazas sobre esta tecnología.

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. Desafortunadamente, toma ancho de banda. Por tanto... ¿Qué podemos hacer? Existen múltiples métodos de encriptación o posibilidades de encriptación: VPN (virtual personal network), el protocolo Ipsec (IP segura) y otros protocolos como SRTP (secure RTP). La clave, de cualquier forma, es elegir un algoritmo de encriptación rápido, eficiente, y emplear un procesador dedicado de encriptación.

Esto debería aliviar cualquier riesgo de amenaza. Otra opción podría ser QoS (Quality of Service); los requerimientos para QoS asegurarán que la voz se maneja siempre de manera oportuna, reduciendo la pérdida de calidad.

Lo próximo, como debería esperarse, podría ser el proceso de securizar todos los elementos que componen la red VoIP: servidores de llamadas, routers, switches, centros de trabajo y teléfonos. Necesitas 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. Se trata del

mismo tipo de precauciones que podrías tomar cuando añades nuevos elementos a la red de datos; únicamente habrá que extender este proceso a la porción que le compete a la red VoIP. Tal y como hemos mencionado, la disponibilidad de tu red VoIP es otra de nuestras preocupaciones. Una pérdida de potencia puede provocar que la red se caiga y los ataques DdoS son difíciles de contrarrestar. Aparte de configurar con propiedad el router, recordemos que estos ataques no solo irán dirigidos a los servicios de datos, sino también a los de voz.

Por último, podemos emplear un firewall y un IDS (Intrusion Detection System) para ayudar a proteger la red de voz. Los firewalls de VoIP son complicados de manejar y tienen múltiples requerimientos. Los servidores de llamada están constantemente abriendo y cerrando puertos para las nuevas conexiones. Este elemento dinámico hace que su manejo sea más dificultoso. Pero el coste está lejos de verse oscurecido por la cantidad de beneficios, así que aconsejamos pasar algo de tiempo perfeccionando los controles de acceso. Un IDS puede monitorizar la red para detectar cualquier anomalía en el servicio o un abuso potencial. Las advertencias son una clave para prevenir los ataques posteriores. Y sin duda no hay mejor defensa que estar prevenido para el ataque.

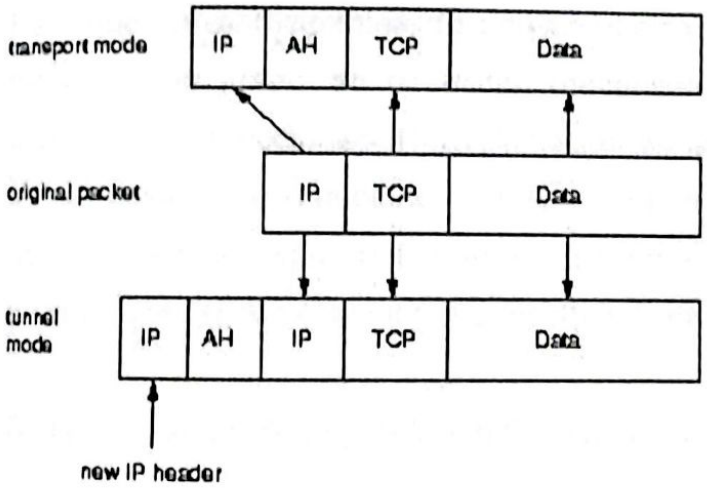
5.2.5 IPSec

La meta de este protocolo es proporcionar varios servicios de seguridad para el tráfico de la capa IP, tanto a través de IPv4 e IPv6. Los componentes fundamentales de la arquitectura de seguridad IPSec son los siguientes:

- Protocolos de Seguridad: Cabecera de autenticación (AH) y los Datos Seguros Encapsulados (ESP).
- Asociaciones de Seguridad.
- Manejo de Clave: manual y automática (Internet Key Exchange, IKE).
- Algoritmos para la autenticación y encriptación.

IPsec es una extensión al protocolo IP que proporciona seguridad a IP y a los protocolos de capas superiores. Fue desarrollado para el nuevo estándar IPv6 y después fue portado a IPv4. La arquitectura IPsec se describe en el RFC2401. Los siguientes párrafos dan una pequeña introducción a IPsec.

IPsec emplea dos protocolos diferentes - AH y ESP - para asegurar la autenticación, integridad y confidencialidad de la comunicación. Puede proteger el datagrama IP completo o sólo los protocolos de capas superiores. Estos modos se denominan, respectivamente, modo túnel y modo transporte. En modo túnel el datagrama IP se encapsula completamente dentro de un nuevo datagrama IP que emplea el protocolo IPsec. En modo transporte IPsec sólo maneja la carga del datagrama IP, insertándose la cabecera IPsec entre la cabecera IP y la cabecera del protocolo de capas superiores.



IPsec: modos túnel y transporte

Para proteger la integridad de los datagramas IP, los protocolos IPsec emplean códigos de autenticación de mensaje basados en resúmenes (HMAC - Hash Message Authentication Codes). Para el cálculo de estos HMAC los protocolos HMAC emplean algoritmos de resumen como MD5 y SHA para calcular un resumen basado en una clave secreta y en los contenidos del datagrama IP. El HMAC se incluye en la cabecera

del protocolo IPsec y el receptor del paquete puede comprobar el HMAC si tiene acceso a la clave secreta.

Para proteger la confidencialidad de lo datagramas IP, los protocolos IPsec emplean algoritmos estándar de cifrado simétrico. El estándar IPsec exige la implementación de NULL y DES. En la actualidad se suelen emplear algoritmos más fuertes: 3DES, AES y Blowfish.

Para protegerse contra ataques por denegación de servicio, los protocolos IPsec emplean ventanas deslizantes. Cada paquete recibe un número de secuencia y sólo se acepta su recepción si el número de paquete se encuentra dentro de la ventana o es posterior. Los paquetes anteriores son descartados inmediatamente. Esta es una medida de protección eficaz contra ataques por repetición de mensajes en los que el atacante almacena los paquetes originales y los reproduce posteriormente.

Para que los participantes de una comunicación puedan encapsular y desencapsular los paquetes IPsec, se necesitan mecanismos para almacenar las claves secretas, algoritmos y direcciones IP involucradas en la comunicación. Todos estos parámetros se almacenan en asociaciones de seguridad (SA - Security Associations). Las asociaciones de seguridad, a su vez, se almacenan en bases de datos de asociaciones de seguridad (SAD - Security Asocciation Databases).

Cada asociación de seguridad define los siguientes parámetros:

- Dirección IP origen y destino de la cabecera IPsec resultante. Estas son las direcciones IP de los participantes de la comunicación IPsec que protegen los paquetes.
- Protocolo IPsec (AH o ESP). A veces, se permite compresión (IPCOMP).
- El algoritmo y clave secreta empleados por el protocolo IPsec.
- Índice de parámetro de seguridad (SPI - Security Parameter Index). Es un número de 32 bits que identifica la asociación de seguridad.

Algunas implementaciones de la base de datos de asociaciones de seguridad permiten almacenar más parámetros:

- Modo IPsec (túnel o transporte)
- Tamaño de la ventana deslizante para protegerse de ataques por repetición.
- Tiempo de vida de una asociación de seguridad.

En una asociación de seguridad se definen las direcciones IP de origen y destino de la comunicación. Por ello, mediante una única SA sólo se puede proteger un sentido del tráfico en una comunicación IPsec full duplex. Para proteger ambos sentidos de la comunicación, IPsec necesita de dos asociaciones de seguridad unidireccionales.
Las asociaciones de seguridad sólo especifican cómo se supone que IPsec protegerá el tráfico. Para definir qué tráfico proteger, y cuándo hacerlo, se necesita información adicional. Esta información se almacena en la política de seguridad (SP - Security Policy), que a su vez se almacena en la base de datos de políticas de seguridad (SPD - Security Policy Database).

Una política de seguridad suele especificar los siguientes parámetros:

- Direcciones de origen y destino de los paquetes por proteger. En modo transportes estas serán las mismas direcciones que en la SA. En modo túnel pueden ser distintas.
- Protocolos y puertos a proteger. Algunas implementaciones no permiten la definición de protocolos específicos a proteger. En este caso, se protege todo el tráfico entre las direcciones IP indicadas.
- La asociación de seguridad a emplear para proteger los paquetes.

La configuración manual de la asociación de seguridad es proclive a errores, y no es muy segura. Las claves secretas y algoritmos de cifrado deben compartirse entre todos los participantes de la VPN. Uno de los problemas críticos a los que se enfrenta el

administrador de sistemas es el intercambio de claves: ¿cómo intercambiar claves simétricas cuando aún no se ha establecido ningún tipo de cifrado?

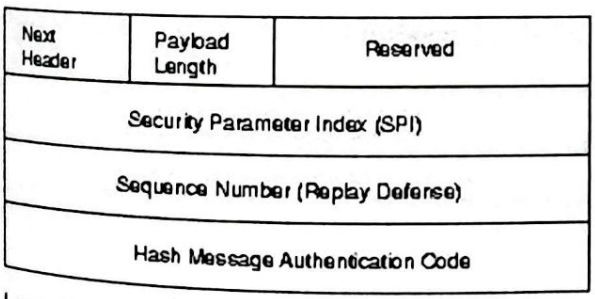
Para resolver este problema se desarrolló el protocolo de intercambio de claves por Internet (IKE - Internet Key Exchange Protocol). Este protocolo autentica a los participantes en una primera fase. En una segunda fase se negocian las asociaciones de seguridad y se escogen las claves secretas simétricas a través de un intercambio de claves Diffie Hellmann. El protocolo IKE se ocupa incluso de renovar periódicamente las claves para asegurar su confidencialidad.

Los protocolos IPsec

La familia de protocolos IPsec está formada por dos protocolos: el AH (Authentication Header - Cabecera de autenticación) y el ESP (Encapsulated Security Payload - Carga de seguridad encapsulada). Ambos son protocolos IP independientes. AH es el protocolo IP 51 y ESP el protocolo IP 50.

AH - Cabecera de autenticación

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.



La cabecera AH protege la integridad del paquete

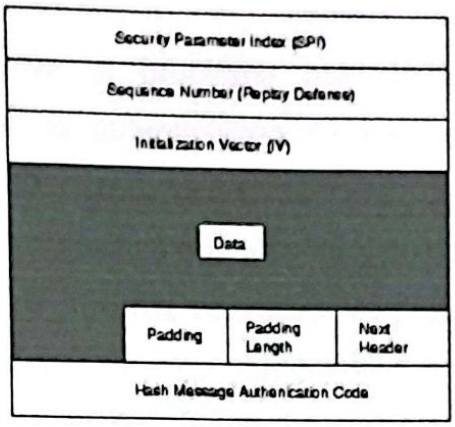
La cabecera AH mide 24 bytes. El primer byte es el campo Siguiente cabecera. Este campo especifica el protocolo de la siguiente cabecera. En modo túnel se encapsula un datagrama IP completo, por lo que el valor de este campo es 4. Al encapsular un datagrama TCP en modo transporte, el valor correspondiente es 6. El siguiente byte especifica la longitud del contenido del paquete. Este campo está seguido de dos bytes reservados. Los siguientes 4 bytes especifican en Índice de Parámetro de Seguridad (SPI). El SPI especifica la asociación de seguridad (SA) a emplear para el desencapsulado del paquete. El Número de Secuencia de 32 bit protege frente a ataques por repetición. Finalmente, los últimos 96 bit almacenan el código de resumen para la autenticación de mensaje (HMAC). Este HMAC protege la integridad de los paquetes ya que sólo los miembros de la comunicación que conozcan la clave secreta pueden crear y comprobar HMACs.

Como el protocolo AH protege la cabecera IP incluyendo las partes inmutables de la cabecera IP como las direcciones IP, el protocolo AH no permite NAT. NAT (Network address translation - Traducción de direcciones de red) también conocido como Enmascaramiento de direcciones reemplaza una dirección IP de la cabecera IP (normalmente la IP de origen) por una dirección IP diferente. Tras el intercambio, la HMAC ya no es válida. La extensión a IPsec NAT-transversal implementa métodos que evitan esta restricción.

ESP - Carga de Seguridad Encapsulada

El protocolo ESP puede asegurar la integridad del paquete empleando una HMAC y la confidencialidad empleando cifrado. La cabecera ESP se genera y añade al paquete tras cifrarlo y calcular su HMAC. La cabecera ESP consta de dos partes.

La cabecera ESP



Los primeros 32 bits de la cabecera ESP especifican el Índice de Parámetros de Seguridad (SPI). Este SPI especifica qué SA emplear para desencapsular el paquete ESP. Los siguientes 32 bits almacenan el Número de Secuencia. Este número de secuencia se emplea para protegerse de ataques por repetición de mensajes. Los siguientes 32 bits especifican el Vector de Inicialización (IV - Initialization Vector) que se emplea para el proceso de cifrado. Los algoritmos de cifrado simétrico pueden ser vulnerables a ataques por análisis de frecuencias si no se emplean IVs. El IV asegura que dos cargas idénticas generan dos cargas cifradas diferentes.

IPsec emplea cifradores de bloque para el proceso de cifrado. Por ello, puede ser necesario rellenar la carga del paquete si la longitud de la carga no es un múltiplo de la longitud del paquete. En ese caso se añade la longitud del relleno (pad length). Tras la longitud del relleno se coloca el campo de 2 bytes Siguiente cabecera que especifica la siguiente cabecera. Por último, se añaden los 96 bit de HMAC para asegurar la integridad del paquete. Esta HMAC sólo tiene en cuenta la carga del paquete: la cabecera IP no se incluye dentro de su proceso de cálculo.

El uso de NAT, por lo tanto, no rompe el protocolo ESP. Sin embargo, en la mayoría de los casos, NAT aún no es compatible en combinación con IPsec. NAT- Transversal ofrece una solución para este problema encapsulando los paquetes ESP dentro de paquetes UDP.

El protocolo IKE

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas. Tras ello, crea las asociaciones de seguridad y rellena la SAD. El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

El protocolo IKE funciona en dos fases. La primera fase establece un ISAKMP SA (Internet Security Association Key Management Security Association - Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

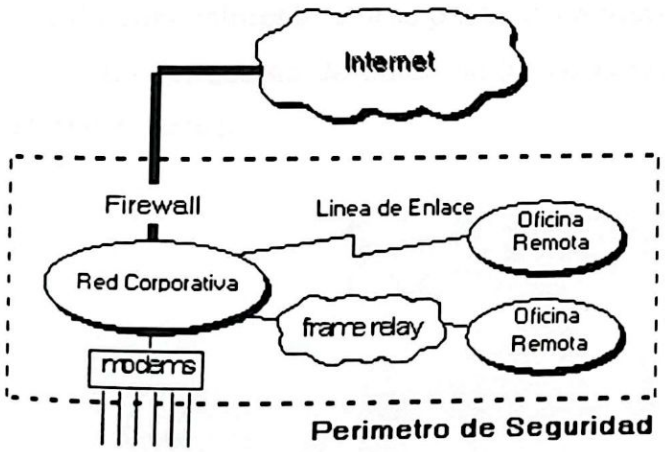
La autenticación de los participantes en la primera fase suele basarse en claves compartidas con anterioridad (PSK - Pre-shared keys), claves RSA y certificados X.509. La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo. Esto, sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto, es susceptible a un ataque man-in-the-middle (por escucha y repetición de mensajes en un nodo intermedio) si se emplea junto a claves compartidas con anterioridad (PSK). Pero sin embargo este es el único objetivo del modo agresivo, ya que los mecanismos internos del modo principal no permiten el uso de distintas claves compartidas con anterioridad con participantes desconocidos. El modo agresivo no permite la protección de identidades y transmite la identidad del cliente en claro. Por lo tanto, los participantes de la comunicación se conocen antes de que la autenticación se lleve a cabo, y se pueden emplear distintas claves pre-compartidas con distintos comunicantes.

En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA. La

ISAKMP SA proporciona autenticación para protegerse de ataques man-in-the-middle. Esta segunda fase emplea el modo rápido.
Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias (al menos dos) IPsec SAs unidireccionales.

5.2.6 Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.



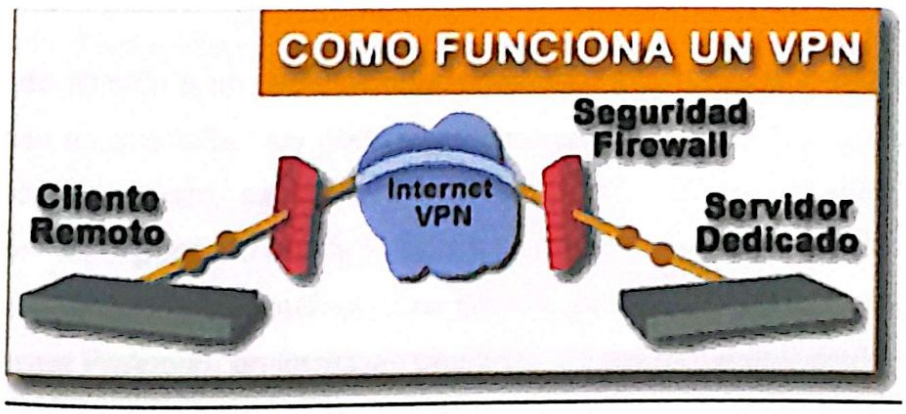
La Política De Seguridad Crea Un Perímetro De Defensa.

Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

5.2.7 Redes Privadas Virtuales - VPN

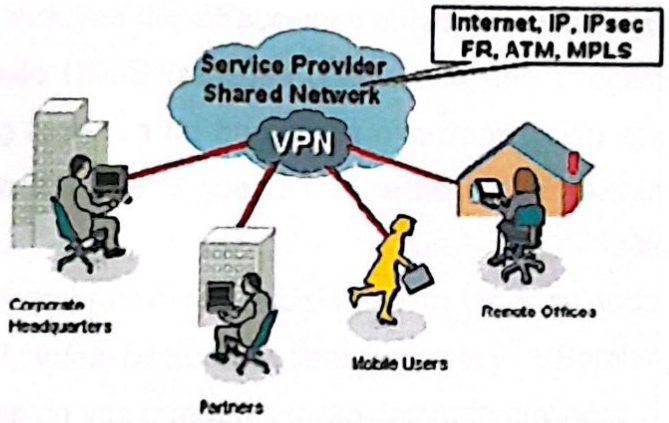
Es una red privada que se extiende, mediante un proceso de encapsulación y en su caso de encriptación, de los paquetes de datos a distintos puntos remotos mediante el uso de unas infraestructuras públicas de transporte.

Los paquetes de datos de la red privada viajan por medio de un "túnel" definido en la red pública.



En la figura anterior se muestra como viajan los datos a través de una VPN ya que el servidor dedicado es del cual parten los datos, llegando a firewall que hace la función de una pared para engañar a los intrusos a la red, después los datos llegan a nube de internet donde se genera un túnel dedicado únicamente para nuestros datos para que estos con una velocidad garantizada, con un ancho de banda también garantizado y lleguen a su vez al firewall remoto y terminen en el servidor remoto.

Las VPN pueden enlazar oficinas corporativas con los socios, con usuarios móviles, con oficinas remotas mediante los protocolos como internet, IP, Ipsec, Frame Relay, ATM como lo muestra la figura siguiente.



5.3 Debate: Seguridad en los sistemas VoIP

Haciendo alusión a un reciente debate en línea sobre temas de seguridad, los expertos coinciden en que falta muy poco para que los sistemas de "Voice Over IP" (VoIP), sean inundados de spam, se abran a los piratas informáticos, y sean derribados por los gusanos. Es importante que la industria se adelante a estas expectativas.

Voz sobre IP, es una tecnología que permite la transmisión de la voz a través de redes IP (Internet Protocol), en forma de paquetes de datos. La aplicación más notoria de esta tecnología, es la realización de llamadas telefónicas ordinarias a través de la red.

"Nosotros ya hemos visto casos donde empresas importantes han tenido sus infraestructuras de VoIP, afectadas por un gusano," dijo Chris Thatcher de Dimension Data Holdings, empresa dedicada a servicios globales de TI (Tecnologías de la Información).

"Existe una falta de seguridad en el diseño y el desarrollo de VoIP, y los compradores no toman el tema de la seguridad en consideración," dijo Thatcher. Las empresas se han enfocado casi exclusivamente en el precio, las características y el desempeño, a menudo liberando nuevos sistemas que están abiertos a insospechadas amenazas.

Según Andrew Graydon de BorderWare Technologies Inc., otro de los panelistas, los riesgos incluyen las infracciones comunes de la seguridad que las empresas tratan hoy, incluyendo DDoS (ataques distribuidos de denegación de servicio), código malicioso, spoofing (práctica de hacer que una transmisión aparezca como venida de un usuario diferente al usuario que realizó la acción) y phishing (atraer mediante engaños a un usuario hacia un sitio Web falso).

Pero las empresas necesitan también tener cuidado respecto a las amenazas propias de VoIP, tales como escuchas furtivas y "VBombing", donde centenares o miles de mensajes de voz pueden ser rápidamente enviados a una sola consola VoIP.

Graydon opina que los vendedores son reacios a admitir que estas debilidades existen. "Es un mercado tan nuevo, nadie quiere espantar al consumidor", dijo. "Pero ya se pueden encontrar scripts para estos ataques a sistemas VoIP en el propio Internet".

La mayoría de estos ataques, pueden alcanzarse al nivel de las aplicaciones, que para la mayoría de los grandes vendedores se basa en el SIP (Session Initiation Protocol). SIP es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de Internet.

Los cortafuegos y las redes privadas virtuales (VPN), pueden manejar de forma adecuada la seguridad en la capa de transporte para VoIP, pero SIP puede compararse con el SMTP y el HTTP para las aplicaciones de la Web y el correo electrónico, que fueron ignorados hasta que surgieron los problemas de seguridad.

"Todas las vulnerabilidades que existen para el correo electrónico, existen también para VoIP", dijo Graydon. "No cometamos los mismos errores."
Chris Thatcher por su parte, también habló acerca del aumento en el número de agujeros y las capas que deben ser protegidas en una infraestructura de VoIP.
"Al mezclar la voz con los datos, y compartiendo una infraestructura común, existen muchas más maneras para que un atacante pueda entrar," dijo. "Usted no puede depender de un único control de seguridad como si se tratara de una bala de plata."
¿Y para cuándo pueden esperar las empresas estos ataques?. "Será más pronto de lo que se piensa," expresó Thatcher. "Como el mercado de VoIP crece, los piratas informáticos y los remitentes de spam se enfocarán en él cada vez mas."

5.3.1 VOIPSA (VoIP Security Alliance)

Los líderes en VoIP se unen para probar e investigar la SEGURIDAD VoIP
Entre los miembros iniciales se encuentran 3Com, Alcatel, Avaya, Codenomicon, la Universidad de Columbia, el Centro de Seguridad Avanzada Giuliani de Ernst and Young, Insightix, NetCentrex, Qualys, SecureLogix, Siemens, Sourcefire, la Universidad Metodista del Sur, Spirent, Symantec, el Instituto SANS y Tenable Network Security.
TippingPoint, división de 3Com (Nasdaq: COMS) y líder en prevención de intrusiones, anuncia la creación de la primera Alianza de Seguridad de Voz sobre IP de la industria, junto con otros fabricantes, proveedores, investigadores de seguridad y líderes de opinión, con el fin de analizar y reducir los riesgos que afectan a la seguridad de la Voz sobre IP.
La creciente convergencia de las redes de voz y datos duplica los riesgos contra la seguridad por los tradicionales ataques informáticos. Los ataques contra las redes de voz y datos pueden paralizar una empresa y detener las comunicaciones que se requieren para lograr la productividad, produciendo la pérdida de ingresos y la irritación de los clientes. Los despliegues VoIP se están expandiendo, la tecnología se está haciendo más atractiva para los hackers, aumentando el potencial de daño de los

ciberataques. La emergencia de ataques a las aplicaciones VoIP proliferará a medida que los hackers se familiaricen con la tecnología mediante la exposición y el fácil acceso.

VOIPSA (VoIP Security Alliance) se centra en ayudar a las organizaciones a entender y evitar los ataques contra la seguridad de VoIP mediante listas de discusión, patrocinio de proyectos de investigación en seguridad VoIP, y el desarrollo de herramientas y metodologías de uso público. VOIPSA es el primer y único grupo que se dedica en exclusiva a la seguridad en VoIP respaldada por un amplio abanico de organizaciones representadas por universidades, investigadores en seguridad, fabricantes de VoIP y proveedores de VoIP. Con la colaboración de VOIPSA, TippingPoint espera utilizar y mejorar una herramienta para pruebas de seguridad VoIP que desarrolló para encontrar e investigar posibles vulnerabilidades de VoIP.

"A pesar de las ventajas de VoIP, si la tecnología no se implanta de la forma adecuada y segura, probablemente engañaremos a los controles de seguridad y expondremos nuestras redes", señala Brian Kelly, director del Centro de Seguridad Avanzada Giuliani *de Ernst & Young.* "Esta alianza es una importante iniciativa para ayudarnos a potenciar la tecnología, pero también para entender y gestionar los riesgos".

Joseph Curcio, vicepresidente de desarrollo de tecnología de seguridad de Avaya, apunta que "una vez que se toma la decisión de implantar VoIP en el centro del negocio, las empresas necesitan resolver todas las cuestiones de seguridad - en las aplicaciones, sistemas y niveles de servicio. Avaya cree que la VoIP Security Alliance permitirá a las empresas experimentar los beneficios de IP, mientras que garantiza la seguridad de la red y preserva la continuidad del negocio".

"VoIP está empezando a cobrar importancia en el mercado pero atajar de forma proactiva las cuestiones de seguridad ayudará a ampliar mucho más esta adopción", afirma Gerhard Eschelbeck, VP de Ingeniería y CTO de Qualys. *"Qualys* está muy satisfecho de participar en este esfuerzo de la industria para continuar con este trabajo y desarrollar soluciones para satisfacer los requisitos de seguridad de VoIP".

"VoIP tiene el potencial para implantarse en las infraestructuras críticas pero sin una comunidad activa en seguridad VoIP, la calidad y fiabilidad de VoIP pueden tener que someterse a un proceso de revisiones y enmiendas como los que hemos presenciado con otras herramientas de software de comunicación ahora ampliamente desplegadas", añade Ari Takanen, CEO y cofundador de Codenomicon Ltd. *"Desde 2002, Codenomicon* y nuestros partners de desarrollo, la Universidad de Oulu, hemos estado trabajando activamente en seguridad VoIP con el lanzamiento de suites de pruebas PROTOS gratuitas y herramientas de pruebas comerciales para mejorar la seguridad y robustez de VoIP".

"Las empresas están implantando soluciones VoIP para reducir costes e incrementar la eficacia, pero esto también supone nuevos riesgos contra la seguridad que podrían contrarrestar esos ahorros y demandar mayores recursos si no se gestionan adecuadamente", comenta Martín Roesch, creador de Snort y fundador y CTO de Sourcefire. "Somos optimistas porque este grupo generará soluciones más resistentes que ayudarán a los usuarios finales a proteger mejor sus bienes".

"La VoIP ha llegado por fin pero las vulnerabilidades en los equipos y servicios que permiten esta tecnología necesitan ser descubiertos y mitigados", subraya Ron Gula, CTO de Tenable Network Security.

"La VoIP Security Alliance es el marco de trabajo perfecto para impulsar la adopción de la telefonía IP", destaca Dave Hattey, vicepresidente y director general de soluciones empresariales de voz de 3Com. "Como miembro charter, creemos que es nuestra labor impulsar esta alianza y sus mejoras para la seguridad VoIP".

"El pasado año, TippingPoint anunció la formación del Laboratorio de Investigación en Seguridad VoIP para descubrir y analizar las amenazas de la VoIP", subraya Marc Willebeek-LeMair, director de tecnología y estrategia de TippingPoint. "VOIPSA es la culminación de nuestros esfuerzos para trabajar con los líderes en VoIP con el fin de analizar las debilidades de las arquitecturas VoIP y descubrir las nuevas vulnerabilidades mediante la prueba de los protocolos. La investigación de VOIPSA

promocionará el conocimiento en la industria y ayudará a reducir los riesgos de las amenazas".

TippingPoint está proporcionando sus servicios administrativos para la formación de VOIPSA, reclutando miembros y facilitando las reuniones de la organización.

Acerca de TippingPoint, una división de 3Com

TippingPoint, una división de 3Com, es el proveedor líder en sistemas de prevención de intrusiones basados en red que ofrece protección exhaustiva de las aplicaciones, las infraestructuras y el rendimiento para grandes corporaciones, organismos estatales, proveedores de servicios e instituciones académicas. TippingPoint tiene su sede en Austin (Texas).

6. PRESENTE Y FUTURO DE LAS COMUNICACIONES DE VOZ

6.1 Empresas relacionadas con el Estándar VoIP (Voz sobre IP)

6.1.1 3com Corporation y Siemens Public Communications Networks

La plataforma Total Control de 3Com y el switch digital EWSD de Siemens perr na nueva generación de funciones de llamadas personalizadas, incluyendo Voz sobre IP (VoIP).

3Com Corporation y Siemens Public Communications Networks, poseen un acuerdo conjunto de desarrollo que combina un sistema de red de voz y datos para producir el primer y único switch multi-servicio de la oficina central. Las compañías han integrado la plataforma multi-servicio Total Control de 3Com con el sistema digital de switches Class 5 EWSD (Elektronisches Wahlsystem Digital) de Siemens para simplificar el acceso remoto a Internet y permitir la entrega de una nueva generación total en servicios de llamadas personalizadas, incluyendo Voz sobre IP (VoIP).

Este acuerdo conjunto de desarrollo entre dos compañías los ubica en la vanguardia de la convergencia de redes. La implementación de la vía de acceso a Internet de Total

usa el sistema de mensajes de voz basados en la red. Esta información se recibe en el teléfono del usuario, sin la necesidad de encender la PC (computadora). La información de espera de un mensaje se señala a través del panel de visualización del teléfono – un LED - o un tono de discado especial "entrecortado" similar a un correo de voz.

- Entrada controlada por el usuario: utilizando la tecnología basada en la Web, los usuarios pueden por sí mismos configurar estos servicios de llamadas personalizadas para sus líneas telefónicas con la ayuda de una interfaz gráfica fácil para el usuario en sus PCs (computadoras). También pueden obtener una visualización online (en línea) de los gastos actuales de servicios.

"El esfuerzo conjunto entre Siemens y 3Com lleva a la industria a la futura frontera de las comunicaciones y une, de manera eficaz, la red de switches de circuitos con la red de comunicaciones de datos para entregar nuevos servicios," dijo Ross Manire, vice presidente senior, 3Com Carrier Systems. "La combinación de los switches EWSD de Siemens y la tecnología Total Control de 3Com suministrará a los proveedores de servicios la capacidad de desplegar sistemas modulares, de alta densidad, escalables en sus redes e inigualables por ninguna otra oferta del mercado."
En enero de 1999, 3Com lanzó con éxito las capacidades de VoIP(Voz sobre IP), construido en parte sobre la base del servidor de Microsoft Windows NT , en la plataforma Total Control multi-servicio, un sistema avanzado basado en DSP considerado por las firmas de investigación de industrias como el sistema de acceso remoto líder en el mundo de los mercados. Cambiando la definición de acceso remoto, la plataforma Total Control multi-servicio de 3Com es un sistema de última generación, totalmente modular, con acceso tipo portador basado en la tecnología HiPero DSP de 3Com que puede entregar servicios de valor tales como voz, fax, video, sistema de red privada virtual y sus contenidos– todo en un sistema simple con un software que se puede actualizar. Más de tres millones de puertos Total Control se han desarrollado hasta la fecha.

Además, 300 proveedores, que ofrecen servicios a más de 150 millones de suscriptores en 100 países, utilizan el sistema EWSD de Siemens, convirtiéndolo en el switch digital líder en el mundo y confirmando la larga tradición de Siemens como el primer proveedor de soluciones para los sistemas con infraestructuras de telecomunicaciones.

La integración de la tecnología Total Control al switch Class 5 de la oficina central de Siemens suministra una oportunidad estratégica para los servicios de acceso remoto tipo portador, Voz sobre IP y un host para otros servicios adicionales de Internet," dijo Hans-Eugen Binder, presidente de Switching Networks Business Unit de Siemens Public Communications Networks Group. "Cada switch EWSD de Siemens instalado se puede actualizar fácilmente para convertirlo en un switch multi-servicio, ofreciendo reducciones en los costos para proveedores que entregan servicios de acceso a Internet."

"Esta iniciativa confirma el rol de Windows NT como una plataforma estándar para los servicios de red comerciales en la convergencia emergente de redes de voz, video y datos," dijo Cameron Myhrvold, vice presidente, Internet Customer Unit, Microsoft. "Microsoft está ansioso por ver a 3Com y Siemens utilizar el servidor de Windows NT para desarrollar los servicios de última generación dentro de la red pública."

6.1.2 Cisco

La Compañía Cisco Systems anuncia la introducción de mejoras en software y hardware para su línea de productos de acceso de múltiples servicios. Esta línea permite ahora a los proveedores de servicio y a los clientes corporativos desarrollar infraestructuras de red a gran escala y de voz basadas en paquetes, a una fracción del precio de tecnologías tradicionales.

Con las nuevas funciones incorporadas, los clientes pueden aprovechar la integración de voz, video y datos sobre sus redes.

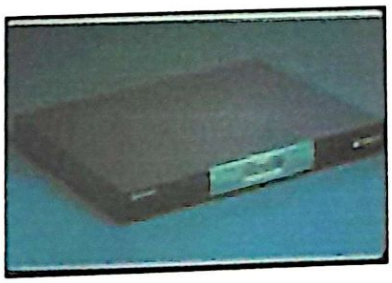
En software, las nuevas características ofrecen voz sobre Frame Relay -VoFR- en los routers de acceso de múltiples servicios Cisco 2600, Cisco 3600, Cisco 7200 y en los concentradores de acceso de múltiples servicios Cisco MC permiten al usuario ofrecer

voz y evitar los PBXs a través de múltiples circuitos permanentes virtuales, con base en el número telefónico marcado. Adicionalmente, aportan a los clientes una red de voz sobre IP (VoIP) confiable y escalable con posibilidad de integrar con facilidad locaciones internacionales. Las interfases soportan VoFR o VoIP, haciendo posible las conexiones a los PBXs (private branch exchanges) con interfases Base Rate (BRI), así como con las tradicionales interfases de telefonía.

Arquitectura de Voz común

El marco de voz con el software integrador Cisco IOS ofrece la integración completa y sin fisura de voz, video y datos. Permite a los clientes corporativos y a los proveedores de servicio manejar grandes redes y servicios basados en VoIP (Voz sobre IP) o VoFR. Por ejemplo, el marco de voz común de Cisco basado sobre la arquitectura Open Packet Telephony de Cisco, ofrece escalabilidad e interoperabilidad de voz sobre servicios de paquetes desde routers de múltiples servicios de baja densidad VoIP/VoFR, hasta gateways VoIP (Voz sobre IP) de tipo carrier. Adicionalmente, los routers de acceso de múltiples servicios de Cisco, en combinación con su H.323 Gatekeeper, permite a los clientes construir redes muy grandes de VoIP (Voz sobre IP). A los proveedores de servicio, las nuevas características incluye el Integrated Voice Response (IVR), características de seguridad AAA para autenticación de usuarios e historiales detallados sobre las llamadas realizadas. Los routers de acceso de múltiples servicios como los de las series Cisco 2600 y 3600, trabajan con el Gateway Cisco 5300 VoIP (Voz sobre IP), haciendo que sea una solución ideal para el proveedor de servicios que esté lanzando servicios administrados de VoIP (Voz sobre IP).

6.1.3 Motorola



Vanguard 320. Solución multimedia modular de bajo costo

Equipos Multimedia y Multiprotocolo

El objetivo de Motorola ING es minimizar los costos de comunicaciones, un aspecto cada vez más crítico. Esta reducción de costes se puede conseguir por dos caminos: por un lado, con equipos flexibles, capaces de adaptarse a distintos entornos LAN (Ethernet, Token Ring, SDLC) y WAN (X.25, FR, PPP); y por otro, con equipos con capacidad de tráfico multimedia (voz y vídeo), a fin de sacar el máximo rendimiento de las líneas de comunicaciones.

Los equipos de Motorola ING son a la vez router y conmutador y pueden comunicarse utilizando redes WAN, públicas o privadas, de líneas punto a punto, RDSI, X.25, Frame Relay o IP. Además, dependiendo del modelo, los routers de Motorola tienen interfaces Ethernet, Token Ring, Serie y RDSI. Este amplio abanico de interfaces, junto con las funcionalidades de routing disponibles (RIP, OSPF, NAT), permiten procesar distintos tipos de tráfico con un único equipo.

Por otro lado, Motorola ING es pionera en la implementación de tráfico multimedia sobre redes de datos; ello nos permite poder ofrecer la posibilidad de aumentar el rendimiento de los enlaces de datos mediante la multiplexación de datos, voz y vídeo vigilancia, con el consiguiente ahorro de costes que ello implica.

En este campo Motorola ING es el único fabricante del mundo capaz de ofrecer soluciones para voz sobre Frame Relay y voz sobre IP con el mismo equipo.

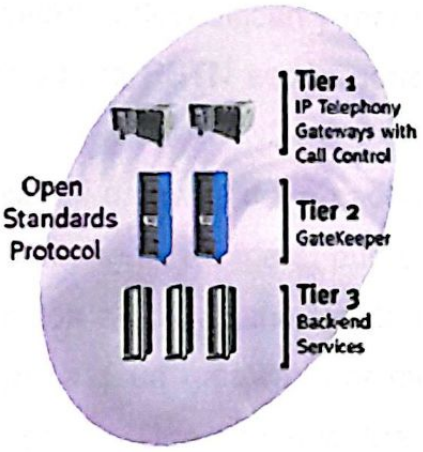
Motorola ING presenta VOFR (Voz sobre Frame Relay) y VOIP (Voz sobre IP) utilizando la misma plataforma hardware.

Motorola ING fue pionera en 1995 al integrar la transmisión de voz en redes WAN Frame Relay. Aprovechando esa experiencia, única en el mercado, Motorola ING lanza ahora VOIP, voz sobre IP, utilizando los mismos equipos, empleando tanto protocolos propietarios (SoTCP) como protocolos estándar (H.323).

Los equipos de Motorola ING ofrecen una calidad excelente en transmisión de voz, tanto analógica (FXS, FXO, E&M) como digital (T0, E1), sobre líneas Frame Relay y/o IP.

Hoy en día Motorola ING es el único fabricante del mundo que ofrece soluciones de voz sobre redes Frame Relay y voz sobre redes IP con el mismo equipo, incluso de manera simultánea. Este hecho permite a los equipos de Motorola ING funcionar de forma simultánea como VoIP Gateway y router voz/datos sobre Frame Relay.

6.2 La Solución de Telefonía sobre IP de 3com



El sistema de telefonía sobre IP de clase carrier de 3Com se basa en una arquitectura abierta de tres niveles de gateways, gatekeepers y servidores de backend interconectados mediante protocolos abiertos basados en normas. La arquitectura modular de 3Com presenta APIs estándar en cada nivel a fin de brindarle a los carriers flexibilidad para personalizar el sistema, facilitando la diferenciación de servicios y la

integración de las "mejores" aplicaciones de oficina back-to-back "de su clase". Este sistema modular llave en mano basado en normas soporta la telefonía sobre IP de teléfono a teléfono y de PC a teléfono en redes conmutadas por paquetes.
Sobre la base de la plataforma de acceso Total Control Multiservice Access Platform de 3Com, el sistema de VoIP (Voz sobre IP) de clase carrier está basado en normas y acepta protocolos internacionales entre los que se incluyen las especificaciones ITU T.120 y H.323v2. Además, el sistema utiliza la codificación de voz G.711, G.723.1 y G.729a para garantizar la compatibilidad con los sistemas de telefonía mundiales. Este desarrollo representa el próximo paso lógico para una plataforma diseñada para servicios múltiples. Además de la voz, la plataforma también brindará un soporte extensivo a los servicios de fax y video.

6.2.1 Gateway de Voz sobre IP

Los gateways de VoIP (Voz sobre IP) proveen un acceso interrumpido a la red IP. Las llamadas de voz se digitalizan, codifican, comprimen y paquetizan en un gateway de origen y luego, se descomprimen, decodifican y rearman en el gateway de destino. Los gateways se interconectan con la PSTN según corresponda a fin de asegurar que la solución sea ubicua.
El procesamiento que realiza el gateway de la cadena de audio que atraviesa una red IP es transparente para los usuarios. Desde el punto de vista de la persona que llama, la experiencia es muy parecida a utilizar una tarjeta de llamada telefónica. La persona que realiza la llamada ingresa a un gateway por medio de un teléfono convencional discando un número de acceso. Una vez que fue autenticada, la persona disca el número deseado y oye los tonos de llamada habituales hasta que alguien responde del otro lado. Tanto quien llama como quien responde se sienten como en una llamada telefónica "típica".

6.2.2 Gatekeeper de Voz sobre IP

Los gateways se conectan con los gatekeepers de VoIP (Voz sobre IP) mediante enlaces estándar H.323v2, utilizando el protocolo RAS H.225. Los gatekeepers actúan como controladores del sistema y cumplen con el segundo nivel de funciones esenciales en el sistema de VoIP (Voz sobre IP) de clase carrier, es decir, autenticación, enrutamiento del servidor de directorios, contabilidad de llamadas y determinación de tarifas. Los gatekeepers utilizan la interfaz estándar de la industria ODBC-32 (Open Data Base Connectivity – Conectividad abierta de bases de datos) para acceder a los servidores de backend en el centro de cómputos del carrier y así autenticar a las personas que llaman como abonados válidos al servicio, optimizar la selección del gateway de destino y sus alternativas, hacer un seguimiento y una actualización de los registros de llamadas y la información de facturación, y guardar detalles del plan de facturación de la persona que efectúa la llamada.

6.2.3 Servidores de Backend

El tercer nivel de la arquitectura de VoIP (Voz sobre IP) de clase carrier de 3Com corresponde a la serie de aplicaciones de backoffice que constituyen el corazón del sistema operativo de un proveedor de servicios. Las bases de datos inteligentes y redundantes almacenan información crítica que intercambian con los gatekeepers durante las fases de inicio y terminación de las llamadas. En el entorno de una oficina central, resulta vital preservar la integridad de los datos de las bases de datos de backend. La solución de 3Com ofrece un enfoque único que garantiza la resistencia de los servidores de backend y la seguridad de sus bases de datos. Los servidores SQL de Microsoft están integrados dentro de la arquitectura del sistema de Backend y administran las bases de datos SQL para las funciones de autenticación, mapeo de directorios, contabilidad y determinación de tarifas. Este nivel de la arquitectura fue optimizado a fin de responder a las necesidades exclusivas de seguridad y disponibilidad de los proveedores de servicios. Para implementaciones a menor escala,

el sistema ofrece flexibilidad para consolidar las bases de datos en un solo servidor robusto o en la plataforma de un gatekeeper.

6.2.4 Otras Soluciones de VoIP (Voz sobre IP) DE 3COM

Este nuevo sistema se expande sobre la estrategia de convergencia de 3Com para segmentos de mercado clave. 3Com también ofrece soluciones de VoIP (Voz sobre IP) para empresas que permiten que los usuarios actuales de routers agreguen voz a su infraestructura empresarial de área amplia ya existente. Los sistemas para empresas también se basan en normas y forman parte de las soluciones end-to-end de la compañía.

6.3 Futuro de la Tecnología de Voz sobre IP

En la actualidad, son cada vez más numerosas las compañías que ven esta tecnología como una herramienta de comunicaciones comercialmente viable. Recientemente, los consultores financieros Merrill Lynch llevaron a cabo un proyecto de VoIP, aunque no fue hasta los ataques terroristas a los Estados Unidos del 11 de septiembre que la compañía decidió adoptar este sistema en toda su red de datos. Esta compañía multinacional descubrió que sus enlaces VoIP eran los únicos que seguían funcionando después de que los ataques al World Trade Center destruyeran las redes de comunicaciones conmutadas de Manhattan.

6.3.1 Las Predicciones del Mercado

El servicio de voz en protocolos de Internet está atravesando poco a poco el umbral que separa lo novedoso de lo que está generalmente aceptado. Muchas de las portadoras que ofrecen servicios de voz a través de IP fueron creadas principalmente con ese fin, y la industria se encuentra en crecimiento constante.

Sin lugar a dudas, los primeros que van a aprovechar las ventajas de la voz sobre IP serán las grandes compañías que, en general, se encuentran geográficamente distribuidas. Según diversas consultoras de nivel internacional, como Frost & Sullivan,

IDC y Probe Research, los pronósticos indican un crecimiento significativo en el mercado de voz sobre IP:

- Hacia el 2001, los ingresos obtenidos por las ventas de gateways se estimaron en mil 800 millones de dólares; y se calcularon, para este mismo año, que la cantidad de minutos de telefonía sobre IP podría llegar a los 12 mil 500 millones.
- Hacia el 2010 se estima que un 25 por ciento de las llamadas telefónicas en todo el mundo será efectuado sobre redes basadas en IP.

7. UTILIZACIÓN DE LA TECNOLOGÍA VOZ SOBRE IP EN COLOMBIA

7.1 Legislación de LA VOZ SOBRE IP EN COLOMBIA

En Colombia no existe una reglamentación para la transmisión de voz vía Internet y aunque ha sido tema de profundos debates, muchos de ellos promovidos por ismo Ministerio de Comunicaciones, lo cierto es que la legislación Colombiana al igual que la de la mayoría de los países se quedó corta.
La tendencia mundial es que la voz sobre Internet no debe ser objeto de regulación pues no se trata propiamente de un servicio de telecomunicaciones.

7.2 Proveedores y Servicio VOIP en Colombia.

Este servicio telefónico se ofrece en Colombia como una alternativa tradicional de voz que comparándola con la telefonía tradicional no requiere de una mayor inversión.

En Colombia los precios están predeterminados por el lugar de destino al que se quiere llamar, algunas compañías como **Orbitel, Telecom, ETB,** ofrecen planes desde $195 el minuto a llamadas nacionales y $695 el minuto a llamadas internacionales, los costos varían si se trata de llamadas a fijos o a móviles y dependiendo de la modalidad

de comunicación que quiera tener (teléfono-teléfono, computador-computador, teléfono-computador, computador-teléfono).

Para utilizar esta tecnología es necesario tener un software especial que facilita la compañía que presta el servicio, un micrófono, parlantes, tarjeta de sonido instalada en el computador y por supuesto una conexión a Internet que debe ser preferiblemente de banda ancha.

8. CONCLUSIÓNES

Podemos concluir diciendo que VoIP es una tecnología que tiene todos los elementos para su rápido desarrollo. Como muestra podemos ver que compañías como Cisco, la han incorporado a su catálogo de productos, los teléfonos IP están ya disponibles y los principales operadores mundiales, están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado tenemos ya un estándar que nos garantiza interoperabilidad entre los distintos fabricantes.

Ya existen empresas que brindan este servicio y que están utilizando esta tecnología, es por ello que predecimos un gran desarrollo de esta tecnología en nuestro país y que poco a poco muchas empresas se van a unir al empleo de Voz Sobre IP, teniendo en cuenta las muchas ventajas que nos ofrece esta tecnología. Sin duda alguna se adhiere a las nuevas corrientes tecnológicas existentes, lo que hace que nos encontremos actualizados con los nuevos avances tecnológicos mundiales.

VoIP hace parte fundamental de la visión próxima futura de las comunicaciones pues la tendencia mundial es la de la convergencia, es decir la conjunción de voz, datos, imágenes, video, televisión, bajo una misma red o canal, y todo a través del protocolo IP.

El estudio de la tecnología de Voz Sobre IP nos pareció muy interesante e importante, ya que es una tecnología que se está implementando en nuestra región y nosotros, ni el resto de nuestros compañeros conocíamos a fondo esta nueva tecnología que está cambiando la forma de comunicarnos.

9. GLOSARIO

Acrónimos

ATM Asynchronous Transfer Mode (Modo de Transferencia Asíncrona)

CCITT Consultative Committee for International Telegraph and Telephone (Comité Consultivo Internacional de Telefonía y Telegrafía)

CPE Customer Premises Equipment (Equipo en Instalaciones de Cliente)

TI Computer Telephony Integration (Integración Ordenador- Telefonía)

DiffServ Differentiated Services Internet QoS model (modelo de Calidad de Servicio en Internet basado en Servicios Diferenciados)

DNS Domain Name System (Sistema de Nombres de Dominio)

E.164 Recomendación de la ITU-T para la numeración telefónica internacional, eespecialmente para ISDN, BISDN y SMDS.

ENUM Telephone Number Mapping (Integración de Números de Teléfono en DNS)

FDM Frequency Division Multiplexing (Multiplexado por División de Frecuencia)

FoIP Fax over IP (Fax sobre IP)

H.323 Estándar de la ITU-T para voz y videoconferencia interactiva en tiempo real en redes de área local, LAN, e Internet.

IETF Internet Engineering Task Force (Grupo de Trabajo de Ingeniería de Internet)

IGMP Internet Group Management Protocol (Protocolo de Gestión de Grupos en Internet)

IN Intelligent Network (Red Inteligente)

IntServ Integrated Services Internet QoS model (modelo de Calidad de Servicio en Servicios Integrados de Internet)

IP Internet Protocol (Protocolo Internet)

IP Multicast Extensión del Protocolo Internet para dar soporte a comunicaciones multidifusión

IPBX Internet Protocol Private Branch Exchange (Centralita Privada basada en IP)

IPSec IP Security (Protocolo de Seguridad IP)

ISDN Integrated Services Data Network (Red Digital de Servicios Integrados, RDSI)

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

ITSP Internet Telephony Service Provider (Proveedor de Servicios de Telefonía Internet, PSTI)

ITU-T International Telecommunications Union - Telecommunications (Unión Internacional de Telecomunicaciones - Telecomunicaciones)

LDP Label Distribution Protocol (Protocolo de Distribución de Etiquetas)

LSR Label Switching Router (Encaminador de Conmutación de Etiquetas)

MBONE Multicast Backbone (Red Troncal de Multidifusión)

MCU Multipoint Control Unit (Unidad de Control Multipunto)

MEGACO Media Gateway Control (Control de Pasarela de Medios)

MGCP Media Gateway Control Protocol (Protocolo de Control de Pasarela de Medios)

MOS Mean Opinion Score (Nota Media de Resultado de Opinión)

MPLS Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo)

OLR Overall Loudness Rating (Índice de Sonoridad Global)

PBX Private Branch Exchange (Centralita Telefónica Privada)

PHB Per Hop Behaviour (Comportamiento por Salto)

PoP Point of Presence (Punto de Presencia)

POTS Plain Old Telephone Service (Servicio Telefónico Tradicional)

PPP Point to Point Protocol (Protocolo Punto a Punto)

PSTN Public Switched Telephone Network (Red de Telefonía Conmutada Pública)

QoS Quality of Service (Calidad de Servicio)

RAS Registration, Authentication and Status (Registro, Autentificación y Estado)

RSVP Reservation Protocol (Protocolo de Reserva)

RTCP Real Time Control Protocol (Protocolo de Control de Tiempo Real)

RTP Real Time Protocol (Protocolo de Tiempo Real)

SAP Session Annunciation Protocol (Protocolo de Anuncio de Sesión)

SCN Switched Circuit Network (Red de Circuitos Conmutados)

SDP Session Description Protocol (Protocolo de Descripción de Sesión)

SIP Session Initiation Protocol (Protocolo de Inicio de Sesión)

SLA Service Level Agreement (Acuerdo de Nivel de Servicio)

SS7 Signalling System Number 7 (Sistemas de Señales número 7)

STMR Side Tone Masking Rating (Índice de Enmascaramiento para el Efecto Local)

TCP Transmission Control Protocol (Protocolo de Control de Transmisión)

TDM Time Division Multiplexing (Multiplexado por División de Tiempo)

TIPHON Telecommunications and Internet Protocol Harmonization Over Networks (Armonización de Protocolos de Redes de Telecomunicación e Internet)

UDP User Datagram Protocol (Protocolo de Datagramas de Usuario)

UMTS Universal Mobile Telephone System (Sistema Universal de Telecomunicaciones Móviles)

VLAN Virtual Local Area Network (Red de Área Local Virtual)

VPN Virtual Private Network (Red Privada Virtual)

xDSL Cualquiera de las tecnologías de Líneas de SuscripciónDigital (por ejemplo, ADSL)

Algoritmo: Serie de instrucciones para realizar una función determinada ó solucionar un problema.

NAT: (Network Address Translation) tecnología usada por los firewalls y routers que permite que direcciones IP accedan a Internet con una sola dirección. NAT empieza su funcionamiento cuando una persona quiere acceder a Internet y dicha persona se encuentra en una red local (LAN) es allí cuando NAT recibe dicha información, remplaza la dirección original para después enviarla a un router.

RTP: Real Time Protocol, que permite la transmisión de datos en "tiempo real", pero provee mecanismos para el envío rápido de información.

UDP: (User Datagram Protocol), es el encargado de soportar los programas que tienen acceso a Internet, estas aplicaciones incluyen programas cliente-servidor, video conferencias. AES: (Advanced Encryption Standard), algoritmo de encripción que utilize

llaves de 128, 192 o 256 bits, que para mayor seguridad, deben tenerse paswords de mas de 32.

DES: (Data Encryption Standard), algoritmo que cifra la información tomando cadenas de 64 bits de largo, y haciendo procesos de cambios de base de binario a hexa.

SRTP: (Secure Real-time Transfer Protocol) Es el mismo protocolo RTP pero con funciones de Seguridad; tales como: confidencialidad y verificación de la información. Este protocolo es de gran utilidad para VoIP ya que no interfiere en la calidad del la conversación.

Debugging: Proceso por el cual se encuentran defectos en el código fuente de un programa.

10. TERMINOS

Circuit switching (conmutación de circuitos). Técnica de comunicación en la que se establece un canal (o circuito dedicado) durante toda la duración de la comunicación. La red de conmutación
de circuitos más ubicua es la red telefónica, que asigna recursos de comunicaciones (sean segmentos de cable, «ranuras» de tiempo o frecuencias) dedicados para cada llamada telefónica.

Codec (codec). Algoritmo software usado para comprimir/ descomprimir señales de voz o audio. Se caracterizan por varios parámetros como la cantidad de bits, el tamaño de la trama (frame), los retardos de proceso, etc. Algunos ejemplos de codecs típicos son G.711, G.723.1, G.729 o G.726.

Extranet (extranet). Red que permite a una empresa compartir información contenida en su Intranet con otras empresas y con sus clientes. Las extranets transmiten información a través de Internet y por ello incorporan mecanismos de seguridad para proteger los datos.

Gatekeeper (portero). Entidad de red H.323 que proporciona traducción de direcciones y controla el acceso a la red de los terminales, pasarelas y MCUs H.323. Puede proporcionar otros servicios como la localización de pasarelas.

Gateway (pasarela). Dispositivo empleado para conectar redes que usan diferentes protocolos de comunicación de forma que la información puede pasar de una a otra. En VoIP existen dos tipos principales de pasarelas: la Pasarela de Medios (Media Gateways), para la conversión de datos (voz), y la Pasarela de Señalización (Signalling Gateway), para convertir información de señalización.

Impairments (defectos). Efectos que degradan la calidad de la voz cuando se transmite a través de una red. Los defectos típicos los causan el ruido, el retardo el eco o la pérdida de paquetes.

Intranet (intranet). Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no conectada a Internet.

IP Telephony (Telefonía Internet). Ver «Voice over IP»

Jitter (variación de retardo). Es un término que se refiere al nivel de variación de retado que introduce una red. Una red con variación 0 tarda exactamente lo mismo en transferir cada paquete de información, mientras que una red con variación de retardo alta tarda mucho más tiempo en entregar algunos paquetes que en entregar otros. La variación de retardo es importante cuando se envía audio o video, que deben llegar a intervalos regulares si se quieren evitar desajustes o sonidos inintelegibles.

Packet switching (conmutación de paquetes). Técnica de conmutación en la cual los mensajes se dividen en paquetes antes de su envío. A continuación, cada paquete se transmite de forma individual y puede incluso seguir rutas diferentes hasta su destino. Una vez que los paquetes llegan a éste se agrupan para reconstruir el mensaje original.

Router (encaminador, enrutador). Dispositivo que distribuye tráfico entre redes. La decisión sobre a donde enviar los datos se realiza en base a información de nivel de red y tablas de direccionamiento. Es el nodo básico de una red IP.

Softswitch (conmutación por software). Programa que realiza las funciones de un conmutador telefónico y sustituye a éste al emular muchas de sus funciones de dirigir el tráfico de voz, pero además añade la flexibilidad y las prestaciones propias del tráfico de paquetes.

VoIP, Voice over IP (Voz sobre IP). Método de envío de voz por redes de conmutación de paquetes utilizando TCP/IP, tales como Internet.

11. BIBLIOGRAFIA

1. BLACK, U. (1999). Voice over IP. New Jersey: Prentice Hall PTR.

2. CUERVO, F., GREENE, N., HUITEMA, C., RAYHAN, A., ROSEN, B. y SEGERS, J. (2000). Megaco Protocol versión 0.8. RFC 2885, Agosto 2000.

3. DOUSKALIS, B. (2000). IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR.

4. GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol Architecture and Requeriments. RFC 2805, Abril 2000.

5. HAMDI, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P. (Mayo, 1999).Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999, pags. 104-111.

6. HERSENT,O., GURLE, D. y PETIT, J.P. (2000). IP telephony: packet – based multimedia communication systems. Great Britain: Addison – Wesley.

7. ITU-T Study Group 16 (1998). Recommendation H.246. Enero 1998.

8. ITU-T Study Group 16 (2000). Recommendation H.323v4 (draft). Noviembre 2000.

9. MINOLI, D. y MINOLI, E. (1998). Delivering Voice over IP Networks. New York: John Wiley & Sons, Inc.