INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

Técnico en REDES & SEGURIDAD

23

TELEFONIA IP

En este fascículo veremos los alcances de la tecnología VoIP y las ventajas que ofrece sobre la telefonía convencional. También conoceremos las plataformas más utilizadas y los peligros que existen, como el sniffing.

- ESTÁNDAR VOIP
- CENTRAL TELEFÓNICA
- PLATAFORMA FREESWITCH
- SEGURIDAD EN VOIP
- ATAQUE DE VISHING
- INTERNET BACKGROUND NOISE

USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Santiago Crocioni
Alejandro Gómez
Gilberto González
Javier Medina
Gustavo Martín Moglie
Juan Ortiz
Pablo Pagani
Gerardo Pedraza
Marcelo Soria

Curso visual y práctico **Técnico en redes y seguridad** es una publicación de Fox Andina en coedición con Dálaga S.A. Esta publicación no puede ser reproducida ni en todo ni en parte, por ningún medio actual o futuro sin el permiso previo y por escrito de Fox Andina S.A. Distribuidores en Argentina: Capital: Vaccaro Sánchez y Cía. S.C., Moreno 794 piso 9 (1091), Ciudad de Buenos Aires, Tel. 5411-4342-4031/4032; Interior: Distribuidora Interplazas S.A. (DISA) Pte. Luis Sáenz Peña 1832 (C1135ABN), Buenos Aires, Tel. 5411-4305-0114. Bolivia: Agencia Moderna, General Acha E-0132, Casilla de correo 462, Cochabamba, Tel. 5914-422-1414. Chile: META S.A., Williams Rebolledo 1717 - Ñuñoa - Santiago, Tel. 562-620-1700. Colombia: Distribuidoras Unidas S.A., Carrera 71 Nro. 21 - 73, Bogotá D.C., Tel. 571-486-8000. Ecuador: Disandes (Distribuidora de los Andes) Calle 7° y Av. Agustín Freire, Guayaquil, Tel. 59342-271651. México: Distribuidora Intermex, S.A. de C.V., Lucio Blanco #435, Col. San Juan Tlihuaca, México D.F. (02400), Tel. 5255 52 30 95 43. Perú: Distribuidora Bolivariana S.A., Av. República de Panamá 3635 piso 2 San Isidro, Lima, Tel. 511 4412948 anexo 21. Uruguay: Espert S.R.L., Paraguay 1924, Montevideo, Tel. 5982-924-0766. Venezuela: Distribuidora Continental Bloque de Armas, Edificio Bloque de Armas Piso 9no., Av. San Martín, cruce con final Av. La Paz, Caracas, Tel. 58212-406-4250.

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Los aspectos fundamentales de la telefonía IP; también, analizaremos las plataformas existentes y entregaremos importantes recomendaciones sobre la seguridad de esta tecnología.

En la clase anterior, vimos las características y el funcionamiento de las redes privadas virtuales, analizamos sus conceptos fundamentales y conocimos las ventajas que nos ofrecen. Analizamos los protocolos asociados y los tipos de VPN, así como también sus modos de funcionamiento. Revisamos los mecanismos y protocolos de seguridad en redes privadas virtuales, el funcionamiento de Hamachi y, además, describimos la plataforma libre OpenVPN.

En este fascículo, conoceremos todos los detalles de la telefonía IP, veremos el estándar VoIP, conoceremos una central telefónica y la plataforma FreeSWITCH. Continuaremos analizando las ventajas de Cisco Unified Communications Manager y profundizaremos en la seguridad relacionada con VoIP. Para terminar, veremos qué es un ataque de vishing, cuáles son los principales problemas que podría ocasionar y de qué forma podemos protegernos; también analizaremos el ruido de fondo de Internet y sus posibles causas.

Qué es la telefonía IP

En esta sección, veremos la definición, el funcionamiento y los beneficios de la telefonía IP; su implementación a nivel hogareño y corporativo; además, sus ventajas y desventajas.

La telefonía IP o **Voice over IP** (**VoIP**) permite la transmisión de comunicaciones multimedia sobre redes IP, sean estas públicas (Internet) o privadas. Algunos de los estándares más difundidos son **H.323** y **SIP** (*Session Initiation Protocol*). También existen implementaciones que utilizan protocolos propietarios.
El principal reto de la telefonía IP radica en la calidad y confiabilidad del servicio. Reemplaza las redes de telefonía tradicionales (PSTN) y típicamente oligopólicas, con estándares abiertos , los cuales ofrecen menores costos y también una mayor flexibilidad y funcionalidad.

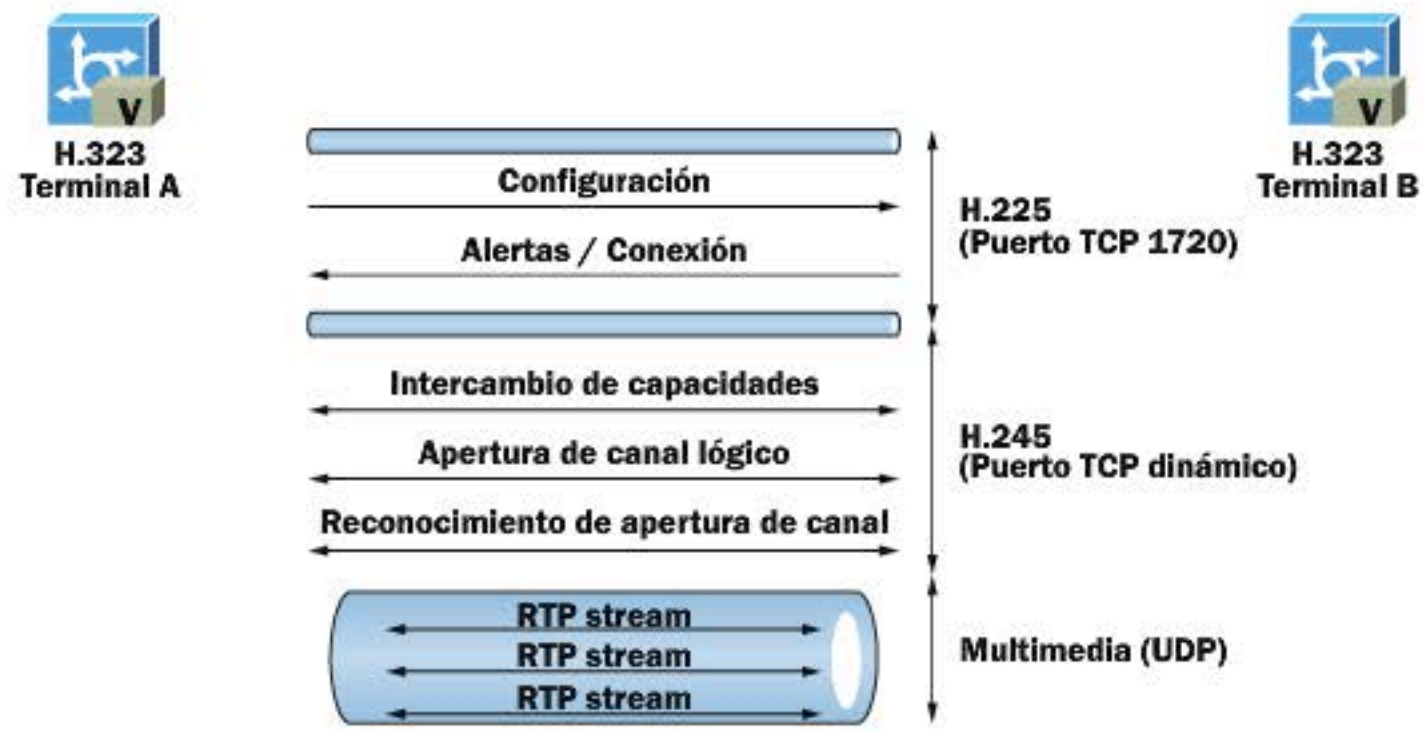
Características

La telefonía IP realiza el proceso de conversión de la voz, una onda analógica, en paquetes de datos digitales; luego de esto, se encarga de transmitirlos utilizando las redes de datos.
A través de los años de desarrollo, la telefonía IP ha superado muchos de los obstáculos que presentaba en sus inicios.
Las redes se han hecho más confiables, y la tecnología ha evolucionado para ofrecer más y mejores prestaciones.

La telefonía IP provee las siguientes características:

- Menor costo por tiempo de llamada.
- Menor costo de administración del equipamiento e infraestructura, dado que se aprovechan las redes de datos existentes.
- Administración y control centralizado de la red.
- Mayor capacidad de comunicación y productividad para usuarios remotos y móviles.
- Aumento de la satisfacción de los clientes gracias al uso de aplicaciones para call centers distribuidos.

Al principio, la migración hacia la telefonía IP respondía solo al ahorro de costos, en especial en las llamadas de media y larga distancia, así como en las llamadas entre sucursales o usuarios de un mismo organismo. Dada esta tendencia, las empresas de telefonía tradicional han reducido y flexibilizado sus planes de larga distancia. Pero, gracias al avance de las tecnologías que proveen calidad de servicio, hoy es común encontrar que VoIP viaja en enlaces compartidos con los datos, por lo que los costos disminuyen.



En este diagrama, vemos el señalamiento previo al establecimiento de una llamada bajo el protocolo H.323.

Softphone Panasonic permite realizar las mismas funciones que un teléfono físico. Es posible utilizar el interno remotamente.

Funcionamiento

La telefonía sobre Internet y los servicios que soporta (voz, fax, SMS y otras aplicaciones de mensajería) son transportados vía enlaces de datos en lugar de la red **PSTN** (*Public Switched Telephone Network*). Los pasos involucrados en una llamada VoIP son:

- Señalamiento y establecimiento del canal.
- Digitalización de la señal de voz analógica.
- Codificación.
- Paquetización.
- Transmisión sobre el protocolo IP.

En el lado receptor, los pasos se realizan en el orden inverso:

- Recepción de los paquetes IP.
- Despaquetización.
- Decodificación.
- Conversión de digital a analógico para reproducir el flujo de voz original.

Arquitectura

Los primeros proveedores de soluciones VoIP ofrecían una arquitectura similar a la de la red telefónica tradicional. La segunda generación de proveedores brindaba un servicio cerrado solo a destinos VoIP dentro de su propia red. La tercera generación habilita la interconexión de distintos sistemas sobre Internet, permitiendo que el usuario tenga mayor flexibilidad.

Los sistemas VoIP utilizan protocolos de control de sesión para monitorear el establecimiento de las llamadas, como así también códecs de audio para codificar la voz permitiendo la transmisión de audio sobre una red IP digital. Los códecs son el corazón de cualquier implementación VoIP. Algunas implementaciones utilizan códecs para banda estrecha mientas que otras soportan códecs de alta fidelidad en estéreo. Algunos de los códecs más populares tanto abiertos como propietarios son:

- **G.711**: conocido como *Pulse Code Modulation* (PCM). Se lo utiliza para modular la voz a 64 kbits (banda estrecha). La versión u-law se utiliza en los Estados Unidos y a-law se usa en otros países.
- **G.722**: es un códec de alta fidelidad debido a que utiliza mayor ancho de banda comparado con G.711.
- **iLBC**: un códec de voz open source muy utilizado; algunas de las aplicaciones que lo utilizan son, por ejemplo, Google Talk y Yahoo! Messenger.
- **G.729**: un códec que usa solo 8 kbit/s para cada canal, lo que lo hace eficiente para aplicaciones como conferencias telefónicas.

Algunos de los protocolos más populares tanto de código abierto como propietarios o comerciales son los que mencionamos y describimos a continuación:

- **H.323**: este protocolo fue el primer protocolo VoIP implementado a gran escala para tráfico de largas y cortas distancias. Sin embargo, con el desarrollo de protocolos nuevos y menos complejos, como **MGCP** y **SIP**, el uso de H.323 ha disminuido notoriamente.
- **Media Gateway Control Protocol (MGCP)**: protocolo para señalamiento y control de llamadas VoIP que interoperan con la PSTN.
- **Session Initiation Protocol (SIP)**: el estándar con mayor penetración utilizado actualmente para VoIP.

Quality of Service (QoS)

Cuando la carga de un enlace crece tan rápido que se desbordan las colas de los switches, se genera congestionamiento y se pierden paquetes de datos. Esto desencadena que el protocolo **TCP** reduzca su tasa de transmisión para aliviar la congestión. Pero VoIP usualmente utiliza **UDP**, no TCP, ya que la retransmisión de paquetes carece de sentido. Los mecanismos **QoS** pueden evitar la pérdida de paquetes VoIP transmitiéndolos de inmediato por encima de cualquier tráfico encolado, aun cuando la cola se esté desbordando.

- **Real-time Transport Protocol (RTP)**: permite la transmisión de audio y video sobre redes IP.
- **Session Description Protocol (SDP)**: su propósito es el de inicializar y negociar las sesiones de streaming. Se usa en conjunto con RTP.
- **Inter-Asterisk eXchange (IAX)**: protocolo open source desarrollado por el proyecto Asterisk, se encarga de realizar la comunicación entre servidores.
- **Jingle (XMPP)**: protocolo open source desarrollado por Google para establecer comunicaciones P2P.
- **Skype**: el protocolo propietario implementado por la aplicación homónima para comunicaciones P2P.

EN LO REFERENTE A LA CALIDAD DEL SERVICIO, LAS REDES IP SON MENOS CONFIABLES QUE LAS UTILIZADAS EN TELEFONÍA CONVENCIONAL.

Soporte

El soporte para VoIP está disponible para diversos dispositivos, los cuales mencionamos y describimos a continuación:

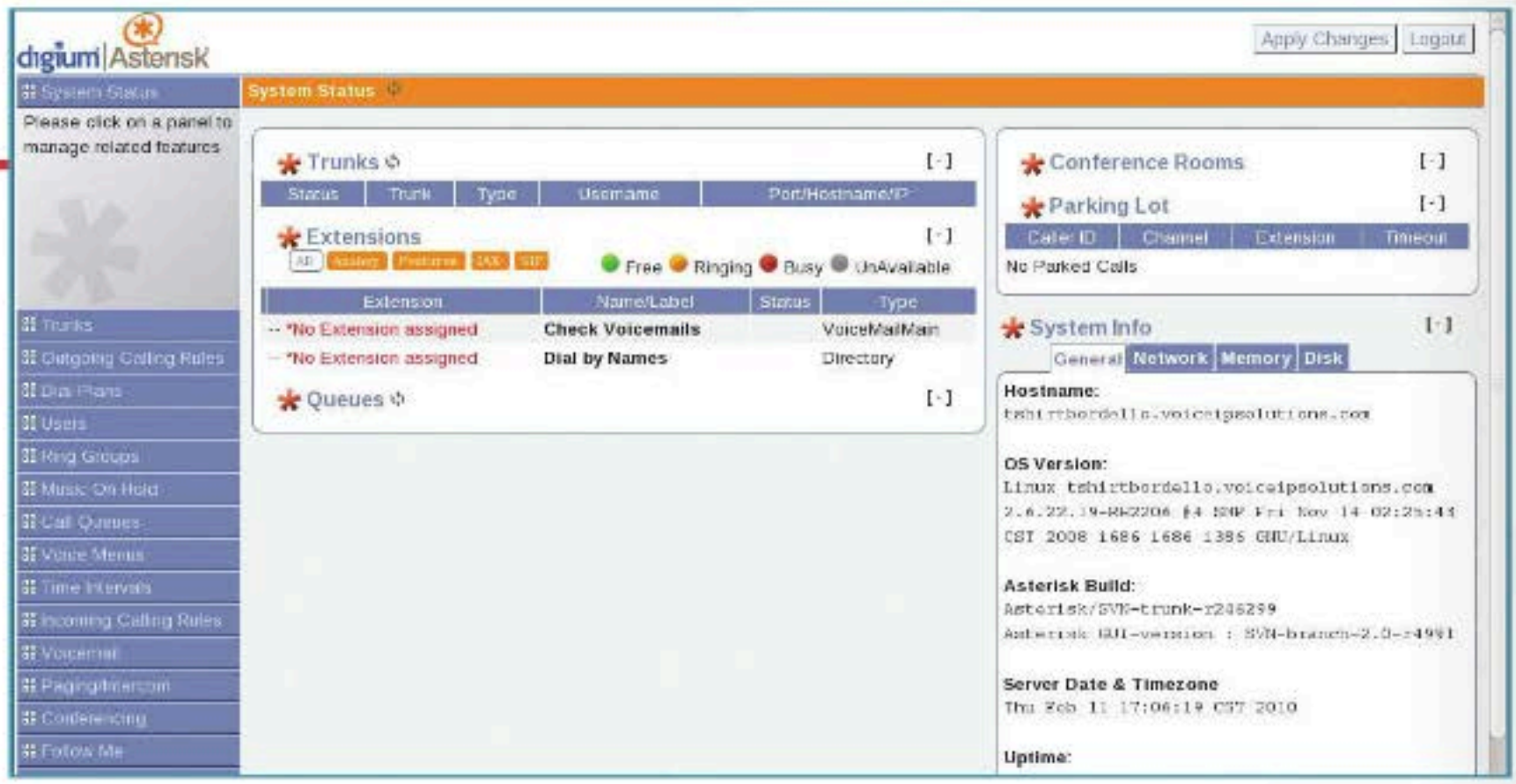
- **Dispositivos analógicos** (teléfonos tradicionales) que estén conectados con un adaptador ATA (*Analog Telephone Adapter*). Este dispositivo permite conectar un teléfono estándar con una conexión a Internet o una PBX VoIP.
- **Teléfonos IP** que se ven como un teléfono tradicional, pero, en vez de tener un conector RJ-11, tienen un conector RJ45 que se conecta a la red Ethernet. También existen teléfonos IP con capacidad Wi-Fi. Además, existen smartphones y dispositivos conectados a Internet, tales como tablets, que pueden realizar llamadas y enviar SMS utilizando redes LTE/3G o Wi-Fi.
- **Aplicaciones que corren sobre computadoras**. Esta es una forma simple y económica de utilizar VoIP. Existen aplicaciones muy populares, como por ejemplo, Skype y Google Talk. Es posible comunicarse con usuarios alrededor del mundo ya sea usuarios de las aplicaciones o, incluso, teléfonos de línea tradicionales.

Dada la eficiencia y el bajo costo de la tecnología VoIP, las empresas ya han migrado la mayoría de sus instalaciones del cableado de cobre a sistemas VoIP. De esta forma, se reducen significativamente los costos mensuales de telefonía. Se calcula que hoy en día el 80% de las líneas que se instalan son VoIP. Las soluciones VoIP han evolucionado en sistemas de comunicación unificados que incluyen llamadas telefónicas, fax, casilla de mensajes, e-mail, conferencias, mensajería instantánea y más. Existe gran variedad de soluciones orientadas en especial para grandes empresas o para pequeñas y medianas empresas (SMB).

Actualidad

Hoy en día, la tecnología VoIP permite que la voz y los datos se transmitan sobre la misma red, lo que reduce en gran parte los costos de infraestructura. Por otro lado, las PBX VoIP pueden ejecutarse sobre hardware con bajos requerimientos, incluso sobre equipos obsoletos. La ventaja radica también en el uso de arquitectura sobre estándares abiertos en lugar de los sistemas propietarios PBX tradicionales.
Los dispositivos VoIP, al poseer menús de configuración visuales con interfaces de usuario intuitivas, son más fáciles de configurar que los tradicionales teléfonos o centrales que se configuraban por tonos. Los teléfonos duales permiten que los usuarios continúen sus conversaciones mientras se mueven entre las redes

Asterisk permite gestionar toda la red VoIP desde la interfaz web.



Central telefónica **Yeastar** con un puerto para conexión de trama E1/T1, que soporta 30 líneas de teléfono normales y 2 de señalización.

celulares o la red Wi-Fi interna de la empresa. Por lo tanto, no es necesario poseer un teléfono celular y un interno en la empresa. De esta manera, se simplifica el mantenimiento y se agiliza la gestión de los dispositivos.

Ventajas

Como sabemos, una de las mayores ventajas de la telefonía IP es el menor costo en la realización de llamadas, pero debemos tener en cuenta que también existen otras ventajas importantes, por ejemplo que existen numerosos sistemas VoIP que no cobran las llamadas entre los usuarios de sistemas VoIP. Otros beneficios son:

- Reutilización de los enlaces de datos.
- La posibilidad de transmitir varias llamadas telefónicas simultáneas sobre un único enlace de banda ancha.
- Llamadas seguras utilizando protocolos estándares.

En referencia a la calidad del servicio, las redes IP son inherentemente menos confiables en comparación con la telefonía tradicional, ya que no proveen mecanismos que aseguren que los paquetes no se pierdan y que lleguen en orden secuencial. Los protocolos QoS mejoran la calidad priorizando las llamadas de voz sobre el resto de los datos, pero aun así no solucionan completamente los problemas con la latencia y el jitter. En forma predeterminada, los routers transmiten utilizando el método **FIFO**, es decir, el primer paquete en llegar es el primero en salir. El volumen de tráfico puede generar latencia que exceda el máximo tolerable por VoIP. El delay fijo no puede controlarse, ya que es causado por la distancia que los paquetes deben recorrer. Pero la latencia puede minimizarse marcando los paquetes de voz como sensibles al delay con métodos como **DiffServ**.

Paquetes

Un paquete VoIP normalmente debe esperar la finalización del paquete actual. Aun cuando es posible cancelar la transmisión de un paquete menos importante, esto por lo común no se realiza, en especial en enlaces de alta velocidad. Una alternativa a la cancelación de paquetes en enlaces de banda estrecha (dial-up, DSL, etc.) consiste en reducir la unidad máxima de transmisión. Para que esto sea posible, cada paquete debe contener un encabezado con información sobre prioridad, lo que incrementa el *overhead* en cada red por la que es encaminado. Los módems DSL proveen una conexión Ethernet, pero, en la mayoría de los casos, son módems ATM. Usan AAL5 (*ATM Adaptation Layer 5*) para segmentar cada paquete Ethernet en series de celdas ATM de 53 byte. Un identificador de circuito virtual (VCI) es parte del encabezado de 5 byte en cada celda ATM, para que el transmisor pueda multiplexar el circuito virtual activo (VCs) en un orden aleatorio. Las celdas del mismo VC se envían siempre en forma secuencial. De todas maneras, la mayoría de las telcos utilizan un único VC para cada cliente, incluso aquellos que tienen servicio VoIP contratado. Cada paquete Ethernet debe ser completamente transmitido antes de que otro pueda comenzar. Si un segundo VC fuera establecido y reservado para VoIP, entonces un paquete de datos de baja prioridad podría ser suspendido en el medio de la transmisión y un paquete VoIP enviado en forma instantánea sobre el VC de alta prioridad. Al término de este, el paquete de baja prioridad sería enviado desde donde se suspendió. Como los vínculos ATM son multiplexados, un paquete de alta prioridad debería esperar 53 byte como máximo para comenzar su transmisión. En este caso, no sería necesario reducir la interfaz MTU (*Maximun Transfer Unit*) y, por lo tanto, aceptar un incremento del overhead, ni tampoco abortar paquetes de baja prioridad que deban luego ser enviados nuevamente.

Latencia

La latencia de los enlaces ATM es mayor en vínculos lentos, ya que esta disminuye al incrementar la velocidad del vínculo. Un frame Ethernet completo (1500 bytes) toma 94 ms para transmitir a 128 kbits/s, pero solo 8 ms a 1.5 Mbit/s. Si este último es el vínculo cuello de botella, esta latencia es quizás suficientemente pequeña como para asegurar una buena performance VoIP sin reducir el MTU o que sean necesarias múltiples VCs. La segunda generación de VDSL2 transmite Ethernet sin intermediaciones ATM/AAL5 y, por lo general, soporta etiquetas de prioridad IEEE 802.1p, por lo que VoIP es encolado menos tiempo y se le da mayor prioridad. ■

Dispositivo **ATA Linksys**; permite conectar dos teléfonos tradicionales a una red VoIP.

Estándar VoIP

En la actualidad, el estándar VoIP es muy importante en las telecomunicaciones; en estas páginas conoceremos sus detalles, así como también su arquitectura y los protocolos asociados a él.

Hoy en día, VoIP se ha convertido en un estándar de suma utilidad en el ámbito de las telecomunicaciones. Literalmente, VoIP es un término compuesto que hace referencia a la emisión de voz a través de Internet (**IP** o *Internet Protocol*). A menudo, esta tecnología es empleada por la mayoría de las organizaciones para lograr la comunicación a través de una red de datos. Aunque pudiéramos pensar que **Voz sobre IP** se trata de una tecnología recientemente impulsada, es necesario destacar que se halla vigente desde los años 90, solo que hace muy poco tiempo ha alcanzado un nivel de madurez bastante importante. La meta principal que alcanzó en sus orígenes la telefonía tradicional consistió en hacer audible la palabra hablada y proyectarla a distancia. Esto desencadenó una serie de innovaciones que hoy hacen posible una forma más eficiente, rápida y funcional de comunicarnos a través de Internet. Ahora, conoceremos cómo se encuentra integrada la arquitectura VoIP, sus características, elementos físicos, de hardware, herramientas de software y su implementación.

Arquitectura de la red

Llevar a cabo la instalación de recursos VoIP sobre una red de cómputo no es algo complejo, pero requiere paciencia, conocimientos básicos y mucha destreza. La incorporación de estos recursos es cada vez más común en las organizaciones. Por ejemplo, algunas pequeñas y medianas empresas emplean esta tecnología para realizar llamadas y mantener la comunicación con otros sectores o sucursales. Esta, a menudo, puede ser incluso ejecutada sobre redes 3G y Wi-Fi. Para comprender la esencia de la tecnología VoIP y los principios de su implementación, vamos a describir el conjunto de componentes que la integran; de esta forma, nos encontramos con un escenario en el que podemos hallar elementos de hardware (configurado con aplicaciones de software), conexión e interacción. Estos últimos se tratan de agentes involucrados en los menesteres del estándar VoIP. A continuación, mencionaremos los elementos más representativos de esta arquitectura.

Los medios físicos y de conexión que debemos considerar son los siguientes:

- **Teléfonos IP (hardphone)**: este tipo de dispositivos incorporan un conector RJ-45 para su conexión directa a la red Ethernet. No pueden ser conectados a líneas telefónicas tradicionales.
- **Adaptadores analógicos IP**: estos equipos generalmente, transforman la señal analógica de los teléfonos tradicionales en los protocolos de Voz IP.

LA TECNOLOGÍA DE VOZ SOBRE IP SE HALLA VIGENTE DESDE LOS AÑOS 90.

- **Softphones**: son programas que permiten emitir llamadas desde una PC mediante el uso de tecnologías Voz IP. Más adelante, se citarán algunos ejemplos de este tipo de programas.
- **Centralitas telefónicas IP**: permiten hacer uso tanto de las tecnologías de Voz IP en combinación con las IP, o exclusivamente IP.

Los medios de interacción son los que mencionamos a continuación:

Skype

Según estudios realizados a finales del año 2012, se develó que, en cuanto a aplicaciones VoIP se refiere, Skype **sigue siendo el preferido no solo de muchos usuarios, sino también de varias compañías. La causa reside en que es el más completo (Wi-Fi, 3G, 3GS), compatible (Blackberry, iPhone) y con el menor consumo de datos. Por fin, después de tantos años (desde 2003), Skype se coloca a la cabeza por encima de cualquier sistema VoIP. En la actualidad, Microsoft ha dado un importante apoyo a esta aplicación a ponerla como reemplazo definitivo del cliente de mensajería más usado de todos los tiempos, MSN Messenger.**

Zoiper

Zoiper se presenta como un cliente para VozIP de alta calidad, el cual nos permite realizar la conexión con centralitas Asterisk, por lo tanto es una buena opción de comunicación telefónica por Internet. Entre las características más importantes de Zoiper podemos destacar el soporte para protocolos SIP + IAX / IAX 2, soporte para STUN, TCP con SIP y TLS con SIP. Además es multilenguaje e integra un servicio de conferencias en forma nativa. Lo podemos encontrar en el sitio web **www.zoiper.com/softphone**.

- **Usuarios Voz IP**: utilizan tecnologías VoIP para la emisión de llamadas.
- **Proveedores de servicio**: generalmente cobran por los servicios contratados (delegan privilegios a los usuarios).
- **Carrier de Voz IP**: se encargan de la venta de rutas y tiempo (minutos) VoIP a los proveedores.
- **Terminadores Voz IP**: se encargan de la venta directa de líneas telefónicas tradicionales a los proveedores de VoIP.
- **Integrador de soluciones Voz IP**: por lo regular, se dedican a la conexión de elementos y medios de transmisión VoIP (centralitas, servidores dedicados, conexiones CRM, softphones, etc).

La tecnología VoIP, cuenta con una serie de interesantes características, que vale la pena mencionar y recordar:

- **Integra una infraestructura convergente**: los servicios que ofrece la tecnología a menudo se encuentran unificados para garantizar la comunicación en una única red.
- **Se basa en estándares abiertos e internacionales**: por lo general, establecidos por las empresas de telecomunicaciones: ISO, ANSI, ITU, IEEE.
- **Soportan los conocidos protocolos estándar**: SIP, IAX2 y H323 habitualmente. Es posible también la integración de protocolos de ciertos propietarios como SKYPE.
- **Permite la expansión de las redes de datos**: esto implica redes más robustas y compatibles (LAN, WAN, Internet: ADSL, ADSL2+, VDSL, WI-FI, WiMax).
- **Posibilidad de desarrollar nuevos servicios**: por encima de otras tecnologías, VoIP ha alcanzado niveles importantes de éxito gracias a la implementación de nuevos servicios.

Centralitas telefónicas

Un elemento predominante en el estándar VoIP es, sin duda, la **centralita telefónica** o **PBX** (*Private Branch Exchange*) y **PABX** (*Private Automatic Branch Exchange*), que consiste en un equipo privado que hace posible gestionar llamadas telefónicas internas en una empresa. Además, permite compartir las líneas de acceso a la red pública entre varios usuarios, quienes se encargan de enviar y recibir llamadas desde cualquier lugar permitido.
Otro elemento es la línea telefónica para la conexión a Internet (banda ancha), que puede estar conectada a un concentrador independiente y, desde allí, a la centralita. Una central telefónica tiene un lugar reservado en el cuarto de telecomunicaciones.

Softphones en VoIP

Como se ha mencionado, un **softphone** consiste en un programa que hace posible concretar llamadas (de un equipo a otro) mediante la concepción de un VSP (*VoIP Services Provider*, proveedor de servicios VoIP). Algunos ejemplos de softphone son: **Skype** (aplicación pionera), **X-Lite**, **QuteCom**, **GoogleTalk**, **Blink** (Windows y GNU-Linux), **Sipdroid** (softphone de Android). Con respecto a lo anterior, vale mencionar que algunos de ellos funcionan incluso de manera muy similar al **WhatsApp** que conocemos, e incorporan Voz sobre IP en 3G y Wi-Fi, tal es el caso de **VIber**.
En la actualidad, muchas compañías desarrolladoras de teléfonos móviles han optado por incorporar, en sus equipos, el estándar VoIP. Desde luego que comenzamos con iphone y su novedosa integración **Fring** (primer softphone abierto), pasando por Nokia y finalizando con Blackberry (con su elegante interfaz **TringMe**). Seguramente, cada día somos más los aficionados al tema de Voz sobre IP, lo que hace que muchos tengamos la inquietud de conocer más sobre algunas de las empresas desarrolladoras de softphone en el mundo; para esta tarea, no dudemos en consultar información relacionada con **CounterPath** y **Digium**.
Ahora, si lo que queremos es incorporar VoIP a nuestro sitio web, la mejor opción se encuentra en: **www.phono.com**.

Establecer la comunicación

Para lograr la comunicación de un dispositivo de red a otro, es necesario el uso de uno o más protocolos.

Aquí podemos apreciar la interfaz de uso del softphone puesto a disposición de los los usuarios por Cisco.

Muchas son las compañías que ofrecen servicios de tecnología VoIP desde Internet. Por lo regular, cada uno cuenta con un portal en la Web.

Un protocolo es definido como un estándar de comunicación que permite a dos equipos de cómputo hablar un mismo lenguaje. Los protocolos más importantes en el estándar VoIP son: **SIP**, **H323**, **IAX2**, **MGCP**.

SIP es un protocolo de inicio de sesión (*Session Initiation Protocol*) asociado a un User Agent. Se sabe que el protocolo se encuentra ligado al IETF para voz, texto y sesiones multimedia, además de que no es capaz de transportar los datos de voz o video por sí mismo. Por esta razón, necesita el auxilio de otro protocolo, en este caso se trata de uno dedicado al transporte en tiempo real (**RTP**, *Real-time Transport Protocol*).

Otro parámetro para establecer la comunicación en el estándar IP son los códecs, término originalmente definido como una forma para digitalizar la voz humana, que será enviada por las redes de datos. Su función se centra en convertir la señal de voz analógica en una versión digital. Como sabemos, algunos ejemplos de códecs son los siguientes: **G.711**, **G.729A**, **GSM** y **Speex**, entre otros. Debemos tener en cuenta que la elección entre todos los códecs que se encuentran disponibles dependerá de las necesidades específicas que exhiba el usuario o la empresa, y también de la plataforma que utilicemos para implementar la solución de telefonía IP.

G.711

G.711 se presenta como un estándar de la ITU-T para realizar la codificación de audio en forma eficiente. Se trata de un estándar utilizado principalmente en telefonía, liberado para su uso en 1972. Es un estándar de codificación digital para representar una señal de audio en frecuencias correspondientes a la voz humana, usando palabras de 8 bits de resolución, con una tasa de 8000 muestras por segundo. Este estándar se encarga de conseguir una relación señal a ruido optimizada.

En la actualidad, los softphones, hardphones, centralitas IP y otros elementos, tienden a soportar una serie de códecs por unidad. Por otro lado, el protocolo **IAX2** (*Inter Asterisk eXchange*) es un estándar definido por **Asterisk**. Este, por lo general, establece el uso del puerto 4569 e incorpora la posibilidad de enviar varias conversaciones por un mismo flujo de datos (**Trunking**).

Por su parte, el protocolo **H.323 30** consiste en un estándar del **ITU** (*International Telecommunications Union*) que provee especificaciones para sistemas y servicios multimedia por redes que no proveen calidad de servicio. La razón de esto se encuentra en que el protocolo incorpora un **QoS** de manera interna.

SIP ES UN PROTOCOLO DE INICIO DE SESIÓN QUE TRABAJA CON EL PROTOCOLO RTP.

Servicios VoIP

La calidad de servicio o **Qos** (*Quality of service*) es una técnica que permite realizar la separación física entre las redes VoIP y las redes de datos; de esta forma logramos evitar la saturación de tráfico en la red. De no hacerse esto, se podrían provocar cortes en el audio o ruido en la red.

QoS nos deja establecer colas de paquetes conforme van llegando, además de permitirnos acelerar aquellos paquetes que tengan mayor prioridad que otros, a través de una etiqueta. De esta forma, el funcionamiento de VoIP asegura un mejor servicio.

Es importante mencionar que cada switch o router tiene su propia interfaz de administración de QoS, por lo que tendremos que aprender a utilizarlo si queremos usar QoS en nuestra red.

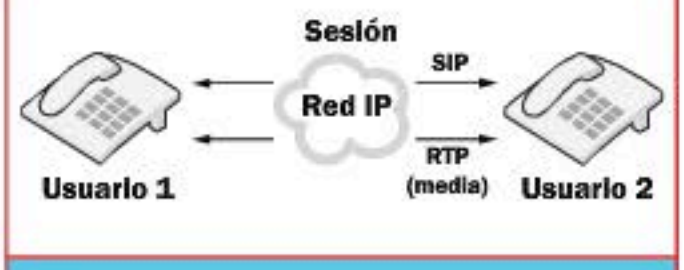
Si somos aficionados al manejo de alguna solución IP (por ejemplo, Asterisk), y deseamos configurar los servicios para recibir paquetes de datos y controlar el tráfico habido y por haber, podemos hacer uso de la herramienta **Traffic Control** también conocida como **TC**.

Entre los proveedores de servicios más notables en el rubro del estándar VoIP, se encuentran: Skype, VoipBuster, Jajah, Gizmo Project, FWD, Vonage, 4G Phone, Justdial, Sarenet, Fring, entre otros. Como vemos, se trata de una oferta amplia, y se encuentra cada vez más presente en nuestra vida coridiana, con productos pensados en usuarios comunes.

Funcionamiento

Para comenzar la implementación VoIP en una red de cómputo (empresa, negocio, institución educativa, etc.), hace falta en primera instancia verificar que se cuente con todos los recursos necesarios para el equipamiento de nuestro entorno. Una vez cubierta esta expectativa, podemos proceder a montar nuestra propia arquitectura. Para ello, es fundamental comprender en detalle la forma en que funciona la tecnología VoIP. A continuación, se describe de manera breve su funcionamiento general:

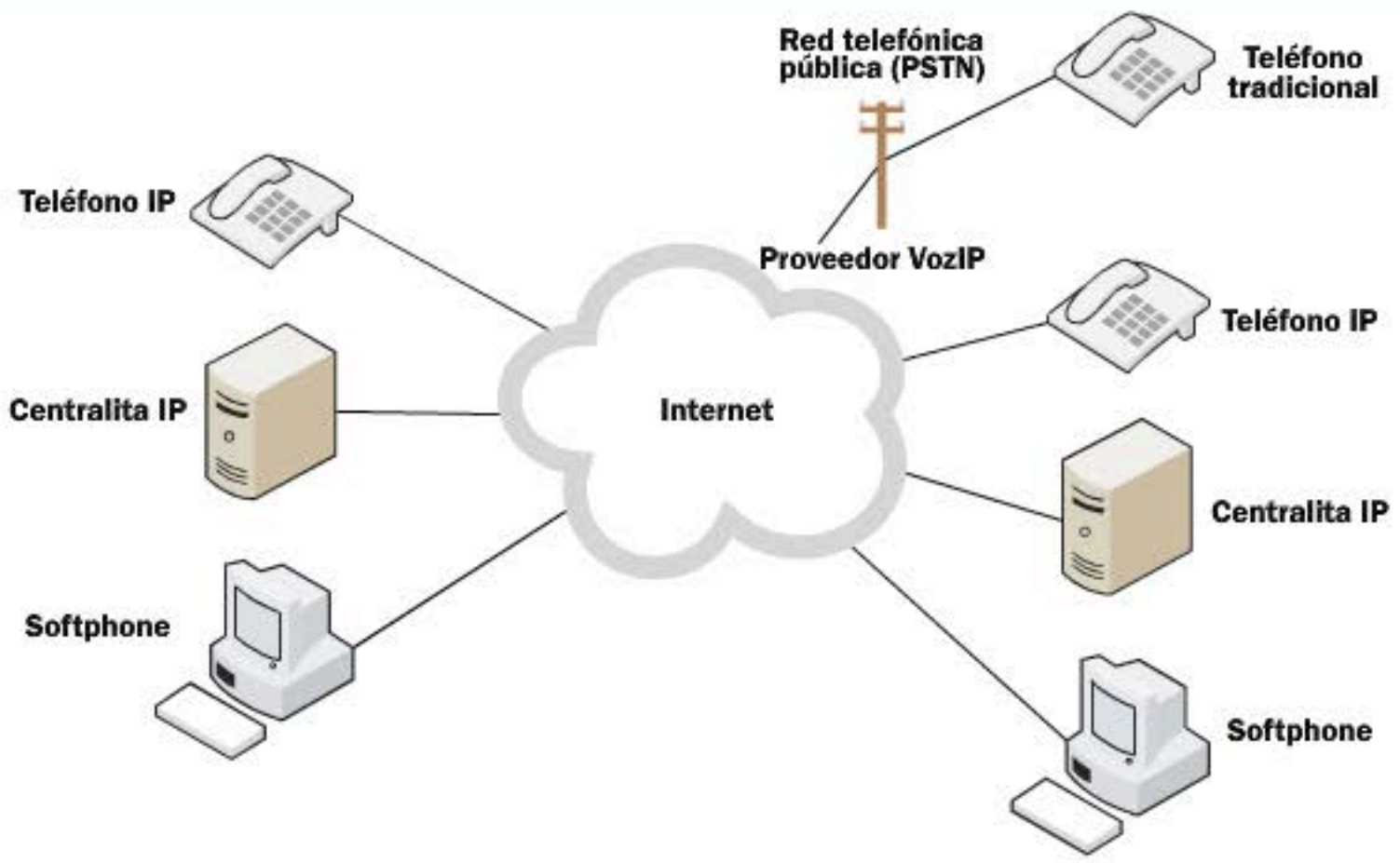
- **Registro**: se necesitan, por lo menos, un emisor y un receptor. Ambos deben registrarse a través de sus teléfonos (puede ser un hardphone o un softphone) en un servidor VoIP designado.
- **Inicio de la comunicación**: en este momento el emisor busca tener comunicación con el equipo receptor.
- **Servidor**: aquí el server se encarga de devolver los datos de contacto al emisor, como puertos y direcciones IP.
- **Fin de la comunicación**: se establece una comunicación entre los interlocutores. Lo anterior es posible desde luego, gracias al uso de los protocolos necesarios.



El protocolo SIP es de forma nativa una topología punto a punto: dos **User Agents** pueden establecer una sesión entre sí.

Perspectiva del futuro

Poco se sabe con respecto a que algunas compañías, como Google, Yahoo y Microsoft, ya han comenzado a preparar su jugada en el marco de VoIP, dando por entendido que dicha implementación no es concebida únicamente como la transmisión de la Voz sobre redes IP, sino mucho más allá. Hoy en día, estas organizaciones hacen posible la concepción de redes convergentes, las cuales se hallan casi siempre integradas por diversos medios y servicios para la comunicación (mensajería instantánea, videoconferencia, multimedia, entre otros). Algunas otras empresas (más cercanas a las telecomunicaciones), como Cisco, Siemens, Alcatel, 3Com, Nortel y Avaya, NEC, buscan desde ahora mantener actualizados sus sistemas con el único propósito de conseguir acercar el estándar VoIP a cada uno de sus clientes. La tecnología ha alcanzando una madurez extraordinaria con el paso del tiempo, así que solo queda estar preparados para la llegada de futuras implementaciones y nuevos servicios. ■



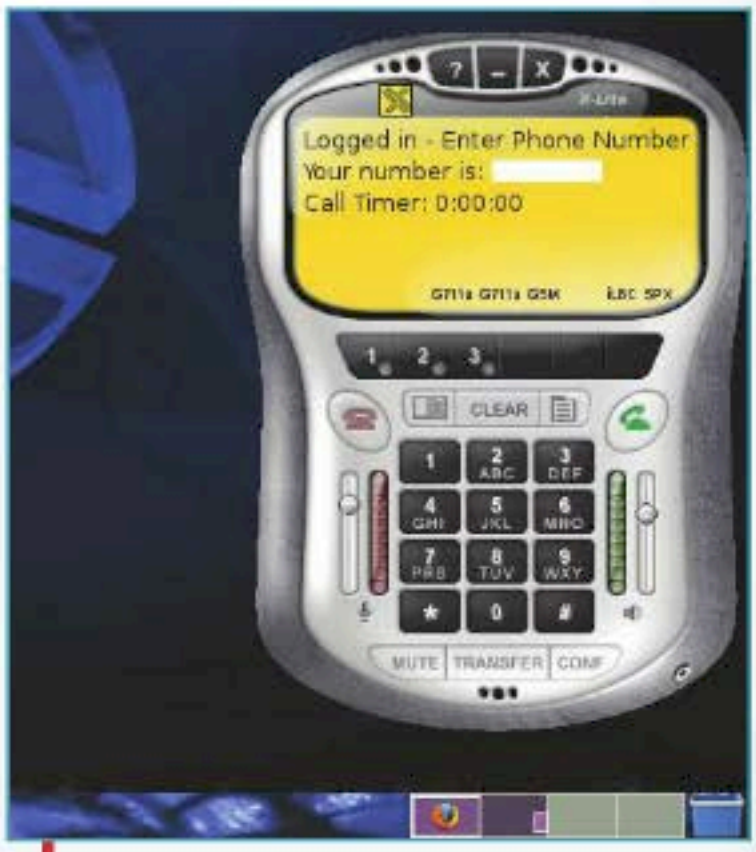
En el presente esquema, se muestra una serie de elementos que componen la arquitectura de red VoIP.

Central telefónica IP

Una central telefónica IP (PBX IP) gestiona señales de voz utilizando el protocolo IP. Puede existir como un hardware dedicado o realizar sus funciones como un componente de software.

Una **central IP** provee numerosas funcionalidades adicionales respecto de una PBX tradicional, como por ejemplo audio, video y mensajería instantánea, a través de una serie de protocolos basados en TCP/IP e interconectada a través de la **PSTN** (*Public Switched Telephone Network*). Los gateways **VoIP** (*Voice over Internet Protocol*) pueden complementarse con centrales telefónicas tradicionales permitiendo utilizar Internet para realizar llamadas entre distintas locaciones sin incrementar el costo de telefonía. Otro beneficio de las centrales telefónicas IP es que requieren el despliegue de una sola red que puede compartirse para datos y telefonía. De esta manera, se simplifica y abarata la instalación y el mantenimiento del cableado.

Como gran parte de la central se compone de software, agregar nuevas funcionalidades es simple y económico. Por ejemplo, es posible configurar números para conferencias, control de llamadas activas, **IVRs** (*Interactive voice response*), **TTS/ASR** (*text to speech/automatic speech recognition*) e interconexión con la red telefónica (PSTN).



Un softphone ofrece las mismas prestaciones que un teléfono fijo, pero puede ser utilizado desde una computadora.

UN SOFTPHONE ES UN PROGRAMA QUE PERMITE RECIBIR Y REALIZAR LLAMADAS DESDE UNA PC EN LUGAR DE UN TELÉFONO TRADICIONAL.

Llamadas

Una central telefónica maneja el tráfico de llamadas entre internos y las líneas de telefonía públicas. Básicamente, una central interconecta líneas e internos. Las líneas denominadas **trunk** se conectan con la red de telefonía pública (PSTN). Los internos pueden ser teléfonos, fax, módems o terminales de tarjetas de crédito. La misión original de la central telefónica es permitir, a una gran cantidad de internos, utilizar un número limitado de líneas públicas.

En las primeras centrales telefónicas, cuando un llamado ingresaba, una operadora conectaba, en forma manual, la línea con un interno libre. Debemos considerar que estos primeros sistemas para ruteo de llamadas se denominaron simplemente conmutadores (*switch boards*).

Con la evolución de la tecnología electromecánica y la electrónica, se automatizó la administración de las líneas, y se fueron agregando nuevas funcionalidades, como el ruteo automático y la transferencia de llamadas entre internos según reglas predefinidas. Con el avance de la tecnología, se añadieron sistemas anexos que permitían grabación de voz y encolamiento de llamados. Hoy en día, todos estos servicios son estándares y cualquier central puede proveerlos. Las centrales analógicas ya se encuentran en vías de extinción, y las centrales IP que utilizan enlaces de Internet para proveer servicios VoIP llegaron para quedarse. Una central IP puede hacer todo lo que una **central PBX** puede hacer y más aún, por ejemplo, gestionar Voz sobre IP como así también líneas terrestres tradicionales.

Centrales analógicas

Cuando las **centrales analógicas** se desarrollaron, la telefonía era prácticamente el único método de comunicación. Hoy en día,

las comunicaciones VoIP son solo uno de los métodos disponibles. También contamos con el e-mail, la mensajería instantánea, la videoconferencia, los SMS y la telefonía celular. A partir de la existencia de todas estas tecnologías y su complejidad para administrarlas se han desarrollado sistemas de **Comunicaciones Unificadas** (*Unified Communications*). Los sistemas de comunicación unificada permiten gestionar en forma centralizada todas las funcionalidades de una manera simple y eficiente. Es posible utilizar teléfonos IP que pueden compartir la conexión con una computadora, o directamente un softphone, que no requiere de ningún hardware más allá de la computadora donde se ejecuta y un headset (micrófono y auricular). De esta forma, gracias a la implementación de una central telefónica IP, el ámbito empresarial se ve altamente beneficiado pues solo tendremos que desplegar una red de datos, así encontramos un ahorro considerable en comparación con la implementación de una central tradicional.

Implementación de una Central IP

En el mercado, existen diversas soluciones para implementar una central IP. Las hay open source como así también pagas. Cisco ofrece para las pequeñas y medianas empresas una solución denominada **UCM Express** (*Unified Communications Manager Express*). Este combina una central IP con funciones de telefonía que una central tradicional no puede proveer. Posee una amplia variedad de funciones, pero permite un despliegue y una administración simples. Una implementación típica requiere tres componentes principales: la central en sí, los teléfonos IP (o softphones) y el gateway que interconecta la red IP con la red telefónica tradicional. A estos componentes principales, debemos sumarle el cableado y los switches utilizados para la red de datos que, en una migración, serán típicamente preexistentes.

Funcionamiento de Asterisk

Un ejemplo de central telefónica IP open source es **Asterisk**. Fue creada originalmente como el motor de una central telefónica e incluye muchos de los componentes necesarios para construir un sistema telefónico robusto y escalable. Incluye funcionalidades que, en una central telefónica comercial, pueden tener un costo extra, o comercializarse vía licencias. Algunos ejemplos son: casilla de correo, preatendedor automático, encolamiento de llamadas, conferencias, paging y llamados entre internos.
Asterisk es una tecnología con soporte para múltiples protocolos; incluye soporte para cualquier teléfono IP y drivers para SIP, entre otros protocolos. Existen algunas empresas, como Digium, que ofrecen una línea de teléfonos especialmente diseñados para sacar el máximo provecho de la central telefónica Asterisk. Esta tecnología está en permanente evolución, y es posible realizar actualizaciones en forma constante sin necesidad de efectuar el recambio del hardware.
Es posible realizar la implementar de Asterisk de tres formas principales, las cuales describimos a continuación:

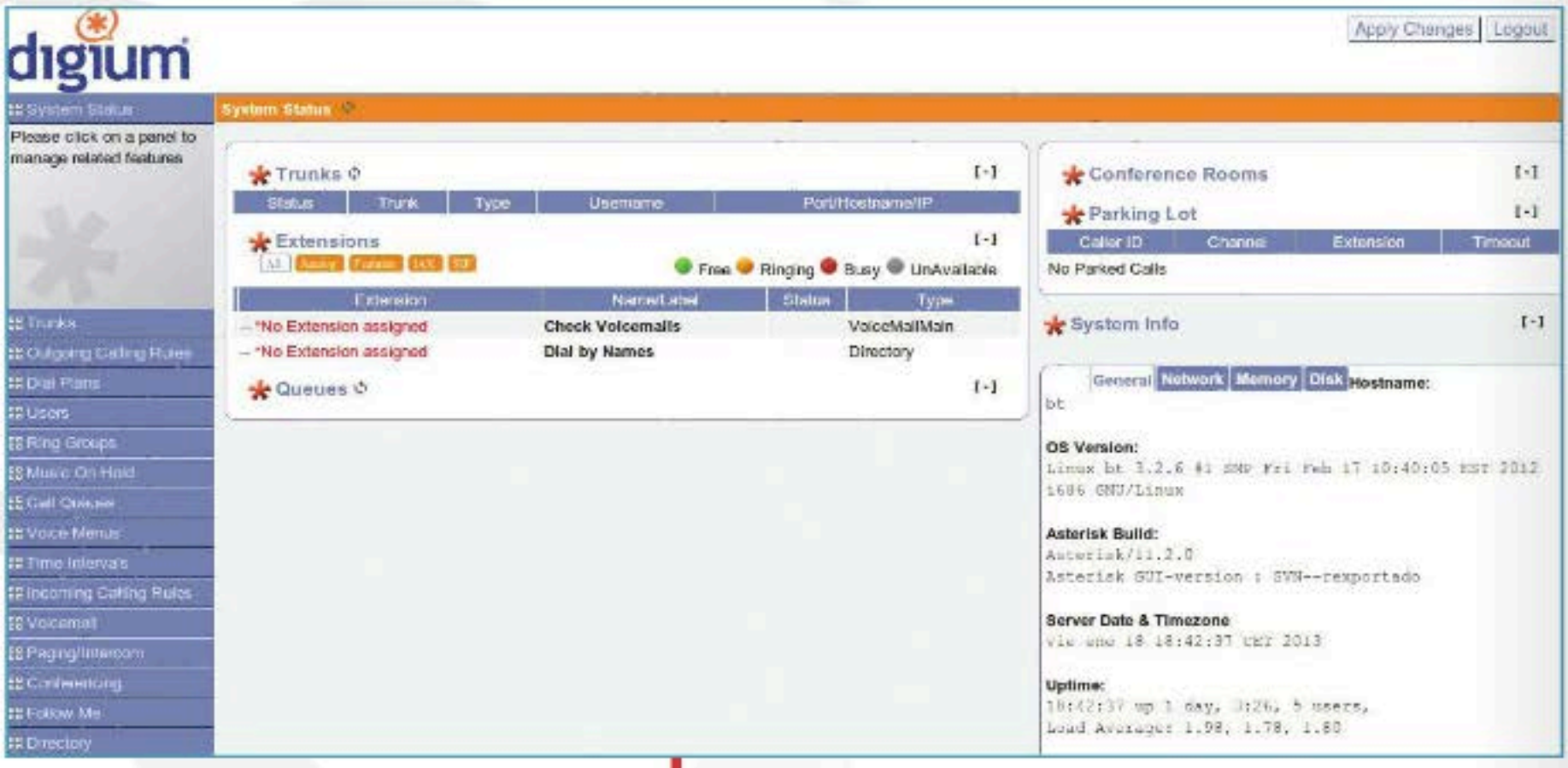
Calidad de servicio

En una red utilizada para Voz sobre IP, el tráfico de voz y el resto de los datos viaja en paquetes por redes IP con una capacidad máxima fija. Este sistema puede sufrir la congestión y los ataques DoS, más aún que los circuitos tradicionales, ya que un circuito tradicional simplemente rechaza las conexiones que sobrepasan su capacidad. Pero los vínculos IP aceptan el exceso de capacidad, lo que genera que la calidad del servicio decaiga. Para ayudar a reducir este problema, se utiliza el protocolo QoS, que prioriza ciertos paquetes que requieren transporte en tiempo real.

- Adquirir una solución tipo appliance que provee hardware y software integrado y testeado.
- Desde cero, instalando el sistema operativo y, luego, el software.
- Desde una ISO booteable que instala todo lo necesario.

La primera opción es adquirir una aplicación que utilice Asterisk como motor; un ejemplo de ello es la empresa **Digium**, la cual ofrece **VoIP Gateways** basados en Asterisk. Estos incluyen una interfaz de administración simple e intuitiva junto con funciones avanzadas, como mensajería instantánea, casillas de mensajes y convergencia móvil y fija, entre otras tareas.
La segunda solución requiere disponer de un servidor e instalar el sistema GNU/Linux y luego manualmente el motor de Asterisk y los componentes restantes. Esto brinda un control granular

Teléfono IP Polycom. Se conecta a la red Ethernet mediante un conector RJ45.



Aquí vemos la interfaz de administración para Asterisk provista por los productos Digium.

sobre el producto instalado y la funcionalidad, pero requiere de un conocimiento más profundo de cómo implementar cada componente. No es la solución indicada si no se cuenta con un conocimiento específico del producto.

La tercera alternativa requiere también que se disponga de un servidor, pero se simplifica al utilizar un software appliance como **AsteriskNOW**, ya que instala el sistema operativo, los drivers para los teléfonos y las tarjetas necesarias, las interfaces de administración, entre otros.

La instalación se realiza en forma prácticamente automática sin mayor intervención del administrador y se realiza en pocos minutos, solo debemos seguir los pasos del asistente.

Cisco Catalyst Express 520, parte de la suite Cisco Unified Communications Manager Express.

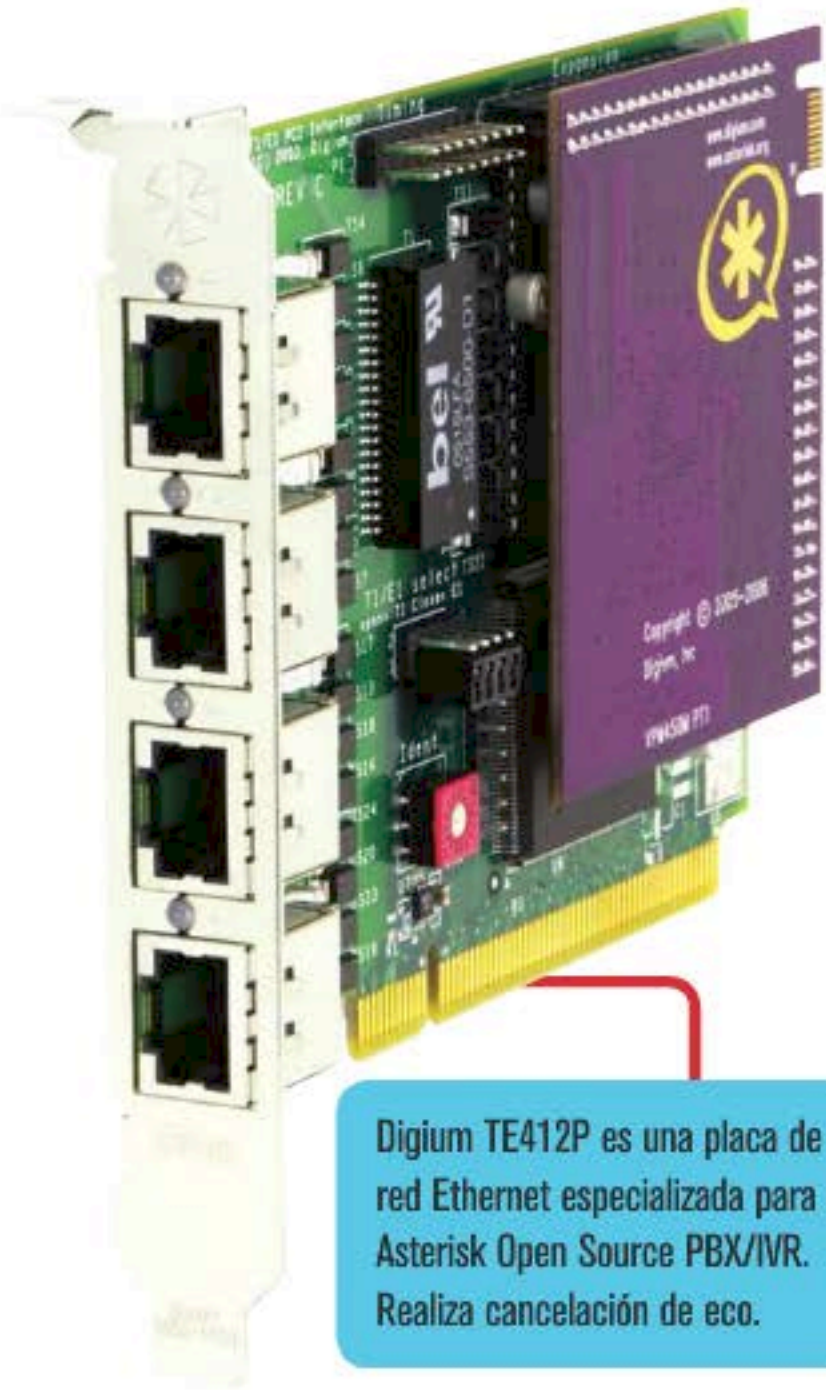
Para esto, se requerirá una conexión a Internet con un ancho de banda aceptable, sobre todo de subida (upstream). Requerirá además de una computadora con placa Ethernet, que no necesita ser de última generación, ya que el software es poco demandante. Es necesario descargar y grabar en CD o USB una versión booteable de Asterisk que instala el sistema operativo y la aplicación en un solo paso. Luego será necesario adquirir teléfonos IP (existen numerosos fabricantes) o adaptadores para teléfonos analógicos. Para empezar, lo más simple y económico es utilizar softphones corriendo sobre una computadora de la red. Los softphones pueden ejecutarse en equipos Windows o GNU/Linux, y no es necesario que todos los equipos sean GNU/Linux, solo el servidor debe serlo. También es posible administrar la central desde un equipo Windows utilizando una interfaz web.

SIP *(SESSION INITIATION PROTOCOL)* ES EL ESTÁNDAR CON MAYOR PENETRACIÓN UTILIZADO PARA VOIP SOBRE INTERNET.

Para comunicarse internamente dentro de la empresa utilizando los internos, no se necesita nada más, pero para comunicarse con líneas de telefonía tradicionales es necesario obtener un servicio pago para tal fin. Cuando se requieren seis o más líneas, puede contratarse como líneas E1/T1, que son líneas ya digitales. Debemos tener en cuenta que estas líneas tienen una interconexión específica que requiere de una placa especial.

Alternativas

También existen proveedores VoIP en el mercado que nos brindan un número telefónico e interconexión hacia la red pública, cuyos costos son más económicos que los de las líneas tradicionales.



Digium TE412P es una placa de red Ethernet especializada para Asterisk Open Source PBX/IVR. Realiza cancelación de eco.

En los casos donde no es posible una solución open source o no contamos con el tiempo suficiente o el conocimiento para implementarla, se puede adquirir una central telefónica IP por hardware con todas las funcionalidades definidas.
Algunas de las funcionalidades básicas que pueden requerirse son las que mencionamos a continuación:

▶ **Soporte VoIP**: incluye el soporte para teléfonos IP así como también soporte para líneas IP (trunks E1/T1). SIP es el protocolo estándar más extendido por lo que, sin duda, una PBX IP debe soportarlo.

▶ **Mensajes de voz**: en las centrales tradicionales antiguas solía ser un agregado. Consideremos que, en una central moderna, es algo de serie que debería estar incluido.

▶ **Movilidad**: cada vez más, los usuarios y empleados de las empresas necesitan ser productivos mientras se trasladan, se mueven entre salas de reunión o distintas oficinas. La central debe tener la capacidad de reenviar llamados de un interno a otro o, incluso, a líneas externas o móviles. De esta forma, si nos encargamos de asegurar que la movilidad sea una característica ofrecida por la central telefónica, ofrecemos un mejor servicio a los usuarios.

▶ **Conferencias**: permiten ahorrar mucho tiempo y dinero por la reducción de los traslados a causa de las reuniones. Una central telefónica completa debe proveer una solución para realizar conferencias entre más de tres internos.

▶ **Reportes**: para poder conocer y controlar los gastos de las llamadas telefónicas, es necesario contar con, al menos, un reporte de las llamadas realizadas en forma histórica.

Los sistemas VoIP utilizan protocolos de control de sesión para controlar el establecimiento de las llamadas, como así también códecs de audio para codificar la voz permitiendo la transmisión de audio sobre una red IP digital. Los códecs son el corazón de cualquier implementación VoIP. Algunas implementaciones utilizan códecs para banda estrecha mientas que otras soportan códecs de alta fidelidad en estéreo. Debemos tener en cuenta que los algoritmos de compresión utilizados en los diferentes códecs se encargan de analizar un bloque de muestras PCM, las cuales han sido entregadas por el codificador de voz. Cada uno de estos bloques posee una longitud variable que depende de la acción del codificador, por ejemplo el tamaño básico de un bloque del algoritmo G.729 es de 10 ms, mientras que el tamaño básico de un bloque del algoritmo utilizado por el códec G.723.1 es de 30 ms. De esta forma, encontramos que la cadena de voz análoga es completamente digitalizada en muestras PCM, y así mismo son entregadas al algoritmo de compresión correspondiente, en intervalos de 10 ms o 30 ms, según el códec que se esté utilizando. ■

VoIP sobre ATM/DSL

Para el caso de las conexiones VoIP sobre redes ATM, debemos tener en cuenta que poseen un overhead de casi 10% (el doble del introducido por Ethernet). Este impuesto incide en cada módem DSL, ya sea que tome o no ventaja de múltiples circuitos virtuales, aunque debemos considerar que pocos pueden hacer uso de esta ventaja. En estos casos la latencia es mayor en vínculos lentos, ya que disminuye al incrementar la velocidad del vínculo. Un frame Ethernet completo (1500 bytes) toma 94 ms para transmitir a 128 kbits/s, pero solo 8 ms a 1.5 Mbit/s. Si este último es el vínculo cuello de botella, esta latencia es quizás lo suficientemente pequeña como para asegurar una buena performance VoIP sin reducir el MTU.

Plataforma FreeSWITCH

La plataforma hermana de Asterisk provee numerosas funcionalidades de VoIP. Su modularidad facilita la integración de múltiples complementos.

Se trata de una plataforma open source de telefonía escalable diseñada para rutear e interconectar protocolos de comunicación. **FreeSWITCH** brinda soporte de audio, video, texto y otros formatos multimedia. Fue creada en 2006, según sus creadores, para llenar el espacio vacío dejado por las soluciones comerciales propietarias. Es posible integrar otros desarrollos dentro de la solución. Está desarrollada en C desde cero y licenciada bajo **MPL 1.1**.

Appliance Barracuda Communication Server integra la tecnología FreeSWITCH, sin necesidad de instalaciones.

Desarrollo

En su desarrollo, se han integrado variadas librerías para evitar realizar un trabajo de desarrollo desde cero. Posee una arquitectura modular y extensible, que cuenta solo con la funcionalidad básica. Pueden integrarse gran cantidad de módulos para personalizar las necesidades de los usuarios. Fue diseñado e implementado originalmente por **Anthony Minessale** con la ayuda de Brian West y Michael Jerris. Los tres provienen de las filas de Asterisk, donde también desarrollaban esta **PBX** (*Private Branch eXchange*) open source.

El proyecto fue iniciado con foco en soporte multiplataforma, modularidad, escalabilidad y estabilidad. Hoy en día, esta plataforma es soportada por una comunidad de desarrolladores y usuarios que contribuyen con el proyecto en forma diaria. Algunos de los competidores más famosos son Asterisk, Avaya Application Server, MS Lync, IBM Sametime y Cisco Unified Communications, entre otros. FreeSWITCH es capaz de soportar varias tecnologías de comunicación, como por ejemplo Skype, SIP (*Session Initiation Protocol*), H.323 y GoogleTalk facilitando, de esta forma, la integración con otros sistemas PBX open source, como por ejemplo sipXecs, Bayonne, YATE o también Asterisk.

CudaTel integra FreeSWITCH

Barracuda integra voz y video en cuatro modelos de Appliance **(270, 370, 470 y 670). Incluye servicios VoIP** (Voice over IP)**, como conferencias, preatendedor, servicio follow-me (suena en otros internos o celulares), voz a e-mail, todo administrado desde su interfaz web. Es compatible con cualquier dispositivo SIP y puede utilizar líneas analógicas y digitales. Puede realizar actualizaciones de firmware de los teléfonos en forma centralizada y se integra con** Active Directory **y con** Novell eDirectory.

Funciones

FreeSWITCH soporta funcionalidades SIP avanzadas, como las que mencionamos a continuación:

- **Presence**: una persona que llama a un interno puede visualizar rápidamente la disponibilidad de la otra persona. Por ejemplo, si la otra persona está en una llamada o una conferencia. De esta forma, el teléfono IP informa el estatus a la central, y la central puede informarlo al resto de los dispositivos a través de la lista de contactos global.
- **BLF** (*Busy Lamp Field*): este LED se muestra para cada uno de los integrantes de la libreta de contactos y permite ver, con rapidez, si el interno está ocupado o libre.
- **SLA** (*Shared Line Appearance*): también conocida como **SCA** (*Shared Call Appearance*). Es un LED que muestra el estado de una línea compartida. Este indicador muestra si una línea común esta en uso y poder unirse a una conversación existente. También es posible holdear una llamada en un equipo y retomarla en otro.
- **TCP TLS** (*Transport Layer Security*): es un protocolo criptográfico que provee seguridad (confidencialidad e integridad). Permite encriptar las llamadas realizadas a través de la red interna o sobre Internet.
- **sRTP** (*Secure Real-time Transport Protocol*): es un protocolo desarrollado por Cisco y Ericsson, que permite comunicaciones seguras en tiempo real. Provee autenticación e integridad además de protección contra reproducción de mensajes.
- **SBC** (*Session Border Controller*): puede ser utilizado como un proxy transparente. Por ejemplo, soporta la transmisión de faxes sobre IP (ITU T.38) así como otros protocolos que operan de punta a punta.

Admite los códecs de banda ancha y estrecha y es una solución ideal para mantener dispositivos legacy que conviven con una solución IP. Los canales de voz y el módulo de puente de conferencia pueden operar a 8, 12, 16, 24, 32 o 48 KHz y pueden puentear los canales de las diferentes velocidades. El códec G.729 para compresión de audio también está disponible bajo una licencia comercial.

FSclient es un cliente SIP que corre sobre Windows. Se integra con FreeSWITCH. Soporta libreta de contactos interna y externa.

Funcionamiento

FreeSWITCH se compila nativamente y corre sobre varios sistemas operativos, como Windows, Max OS X, Linux, BSD y Solaris tanto en plataformas de 32 como de 64 bits. Usa librerías de software disponibles libremente para realizar las funcionalidades requeridas. Algunas de las dependencias son:

- **APR** y **APR-Util**, se trata de *Apache Portable Runtime*.
- **SQLite**, una implementación liviana de un motor de bases de datos SQL.
- **PCRE**, mas conocido como *Perl Compatible Regular Expressions*.
- **Sofia-SIP**, una librería SIP open source para clientes de usuarios finales.
- **libspeex**, *Speex DSP library*.
- **mod_spandsp**, para proxy de fax T.38.
- **libSRTP**, se trata de una implementación open source del protocolo denominado *Secure Real-time Transport*.

Debemos tener en cuenta que estas dependencias son necesarias para compilar el core de FreeSWITCH, pero hay otras dependencias para los módulos, como por ejemplo, códecs particulares para audio y video. Esta es una aplicación modular, y los módulos pueden utilizarse para extender la funcionalidad base, pero la capa de abstracción previene la dependencia entre módulos. El objetivo es asegurar que un módulo no requiera a otro para poder cargarse. El core (libfreeswitch) puede ser embebido en casi cualquier aplicación que pueda usar un módulo .so o una dll. Las aplicaciones pueden escribirse en C, Lua, Java, .NET, Javascript/ECMAScript, Python, Perl y más.

Usos

La implementación por defecto está pensada para una PBX o un softswitch, pero puede adaptarse a múltiples usos, como los siguientes:

- Ruteo y cobro de llamados (por ejemplo: *calling cards*).
- **Transcoding B2BUA** (*back-to-back user agent*): opera entre los extremos y permite cobro del llamado, desconexión automática, transferencia de llamados y más.
- **IVR** (*Interactive Voice Response*): preatendedor que cuenta con múltiples opciones de derivación.
- Conferencias entre múltiples líneas internas y externas.
- Casillas de mensajes para los usuarios.
- **SBC** (*Session Border Controller*): permite realizar la conexión entre distintos puntos sobre la red de datos.
- Oculta la topología interna a los controladores externos.
- Soporta los terminales DAHDI, Khomp, PIKA, Rhino, Sangoma y Xorcom.
- Servidor de fax.
- Enrutador T.38 (Fax sobre IP).
- Uso de protocolos ITU T.30 a T.38. ■

Aplicación de telefonía Cisco UCM

En estas páginas, veremos el funcionamiento y la evolución de una de las aplicaciones de Cisco más utilizadas en telefonía IP; también, revisaremos sus capacidades de administración y configuración.

Se trata del corazón de la suite de servicios de colaboración de Cisco; **UCM** (*Unified Communications Manager*) permite el control de sesión y llamadas de video, voz, mensajería, movilidad, mensajería instantánea y presencia. Está disponible en una serie de modalidades: instalación tradicional, public cloud, private cloud, remoto o híbrido. Esta solución de productividad integrada permite a los usuarios comunicarse desde cualquier ubicación, utilizando casi cualquier dispositivo. La solución cuenta con más de 120.000 implementaciones alrededor del mundo, más de 50 millones de teléfonos IP y otros 10 millones de clientes soft deployados.

Funciones

La solución Cisco UCM extiende las funciones de telefonía empresarial desde teléfonos IP hasta dispositivos multimedia, gateways VoIP y aplicaciones multimedia. Los servicios adicionales de datos, voz y video, como por ejemplo la mensajería, las conferencias y los sistemas de respuesta multimedia, interactúan a través de la API de Cisco UCM. Provee servicios de señales y control de llamada a las aplicaciones integradas de telefonía como así también a aplicaciones de terceros. Realiza las siguientes funciones:

- Procesamiento de llamadas.
- Señalamiento y control de dispositivos.
- Administración de plan tarifario.
- Administración de las funcionalidades de los teléfonos.
- Servicios de directorio.
- Operación, administración, gerenciamiento y provisión (**OAM&P**, por sus siglas en inglés).
- Interfaz de programación hacia aplicaciones externas de procesamiento de voz, como por ejemplo Cisco IP Communicator, Cisco Unified IP Interactive Voice Response (IP IVR) y Cisco Unified Communications Manager Attendant Console.

El licenciamiento de la suite se basa principalmente en la cantidad de usuarios que se encuentren activos. Su administración se efectúa en forma centralizada utilizando Enterprise License Manager. Permite generar reportes de cumplimiento y brinda período de gracia para que seamos capaces de probar las funciones ofrecidas por esta aplicación.

Terminales IP de la solución Cisco UCM. Se conectan a la red Ethernet.

Implementación y ventajas

Algunos de los beneficios de la suite consisten en incluir una serie de aplicaciones de voz integrada que sirven para realizar conferencias, y ofrecer funciones de atención de llamadas manuales. Además, posee servicios complementarios, como poner en hold, realizar transfer, reenviar, generar conferencia, generar varias líneas, ruteo automático de llamadas, discado rápido por medio de memorias, rediscado del último número, y otras tantas funciones sobre los teléfonos IP. Como Cisco UCM es una aplicación de software, las actualizaciones y las mejoras pueden realizarse con facilidad actualizando el software del servidor, para evitar actualizaciones de hardware o la instalación de plaquetas adicionales como requieren las PBX tradicionales.

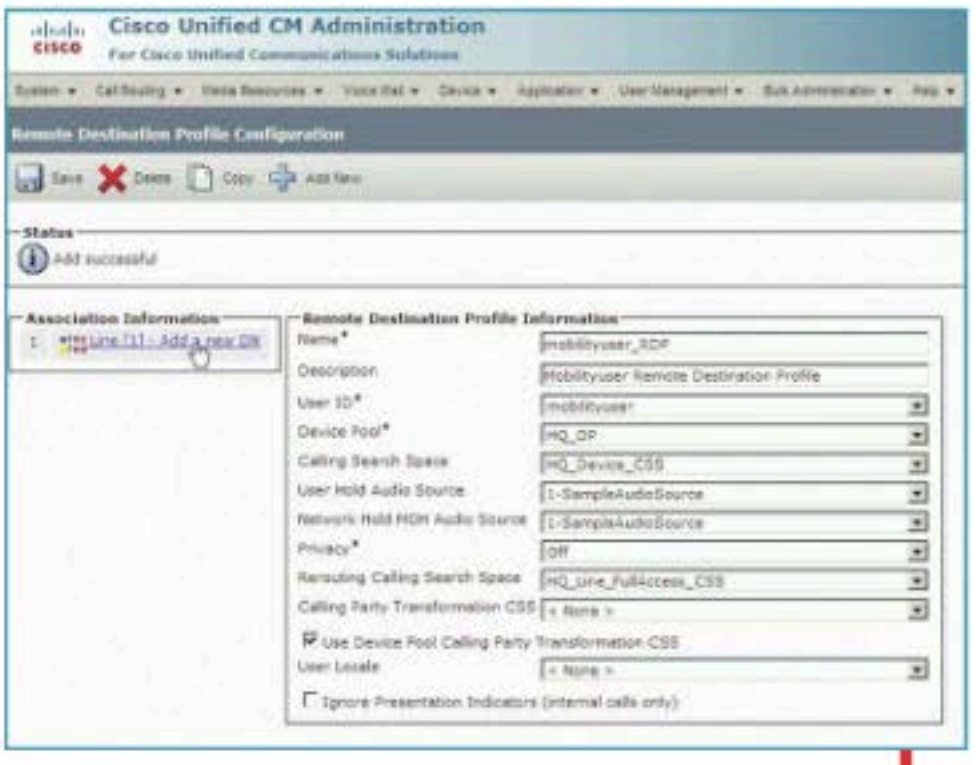
CISCO UCM PROVEE UNA SUITE COMPLETA Y ADAPTABLE A LAS NECESIDADES DE LAS EMPRESAS.

La implementación de Cisco UCM y los componentes **Cisco Unified IP Phones**, gateways y las aplicaciones sobre una red IP proveen una red virtual y distribuida que mejora la disponibilidad y escalabilidad de la solución. El control de admisión de llamadas asegura que la calidad del servicio (QoS) se mantiene incluso con vínculos WAN de poca capacidad, ya que tiene la posibilidad de prevenir situaciones de saturación del ancho de banda, derivando llamados a través de la red de telefonía tradicional (**PSTN**).
La administración de los dispositivos y sistemas se realiza desde una interfaz web que permite que los usuarios y administradores puedan acceder a las funciones y ayuda en línea.
Las comunicaciones unificadas demuestran un gran crecimiento, gracias a las funcionalidades que ofrecen a los usuarios y su bajo costo final operativo. Para las pequeñas y medianas empresas, es posible implementar la solución Cisco UCM Express, que provee una funcionalidad completa, a través de los routers **Cisco Integrated Services**.También, es posible deployar la solución utilizando máquinas virtuales en lugar de equipos de hardware dedicados.
El servicio web **PAWS** (*Platform Administrative Web Service*) permite monitorear los sistemas Cisco UCM, y realizar actualizaciones remotas y upgrades, reduciendo la complejidad y facilitando la administración en implementaciones de gran escala.
La solución posee gran cantidad de funcionalidades, y mejoras sobre los protocolos y las soluciones estándares, como los que mencionamos a continuación:

- Permite hacer uso unificado de capacidades de voz y video.
- Es posible realizar llamadas a usuarios de la solución proveyendo la dirección de e-mail gracias a las capacidades de directorio.
- Posee mejoras sobre el protocolo SIP que permiten mayor interoperabilidad entre los dispositivos de video.
- Se encarga de implementar diversas mejoras sobre RTCP (*Real-Time Transport Control Protocol*).
- Provee mejoras en la experiencia móvil con llamados de video.
- Ofrece la capacidad de recibir video o participar en conferencias de video usando Wi-Fi o redes de celulares, permitiendo sesiones de video entre celulares y teléfonos de escritorio.
- Los clientes y terminales tienen la capacidad de descubrir servicios (como voicemail, mensajería instantánea y aplicaciones de conferencia) en forma automática, y recibir notificaciones de estos.
- Es posible agregar atributos customizados (*Flex atributes*) y que sean sincronizados con las terminales.
- La extensión conocida como Secure Cross-Cluster permite realizar llamadas encriptadas utilizando para ello, la funcionalidad EMCC (*Extension Mobility Cross Cluster*).
- Es posible guardar seteos para llamadas rápidas, como pausas y dígitos, para realizar llamadas ágiles.
- Es posible reproducir música mientras los usuarios esperan ser atendidos mediante MoH (*Music on Hold*), podemos definir el tiempo de espera en la cola, y ofrece estadísticas básicas de las llamadas.
- Desde el teléfono, pueden grabarse conversaciones definidas. ■

La seguridad

La segregación de permisos en roles y usuarios provee múltiples niveles de seguridad a la administración de Cisco UCM y de otras aplicaciones relacionadas. El sistema agrupa los recursos y privilegios en roles, y cada aplicación posee roles predefinidos. Por otra parte, cada aplicación posee sus propios privilegios administrativos, aunque es posible definir nuevos roles para una aplicación determinada. Para cada recurso, el administrador define el nivel de privilegio.



Interfaz web para administración de **Cisco UCM**. Concentra todas las configuraciones de la solución.

Seguridad en VoIP

Veremos los conceptos sobre seguridad en telefonía IP; susceptibilidad de VoIP al sniffing, y métodos de ataque y protección contra amenazas.

Las organizaciones son las que han adoptado en mayor medida las **soluciones telefónicas IP** y las han integrado con los sistemas de telefonía tradicional. Esto se debe, en especial, a la reducción de costos que significa y por las funcionalidades adicionales que posee. Sin embargo, la implementación de esta tecnología sin un entendimiento acabado en la materia supone un riesgo de seguridad. Básicamente, una solución VoIP provee la misma funcionalidad que la solución tradicional, pero la arquitectura subyacente es completamente diferente. Estas diferencias afectan la forma en que se debe asegurar un sistema de telefonía.

Interfaz web de un teléfono IP Snom, que permite realizar llamadas en forma remota, así como también visualizar la libreta de contactos.

Telefonía IP

Los sistemas de **telefonía IP** (IPT) poseen funcionalidades que no están presentes en las soluciones tradicionales, por lo que estos agregan nuevos riesgos. Algunos ejemplos son: servicios HTTP, SNMP, telnet, teléfonos conectados a redes cableadas o wireless, acceso a Internet desde las centrales telefónicas y hacia ellas, funcionalidades de administración remota y teléfonos-software. Todos estos proveen vectores

Confidencialidad de teléfonos IP

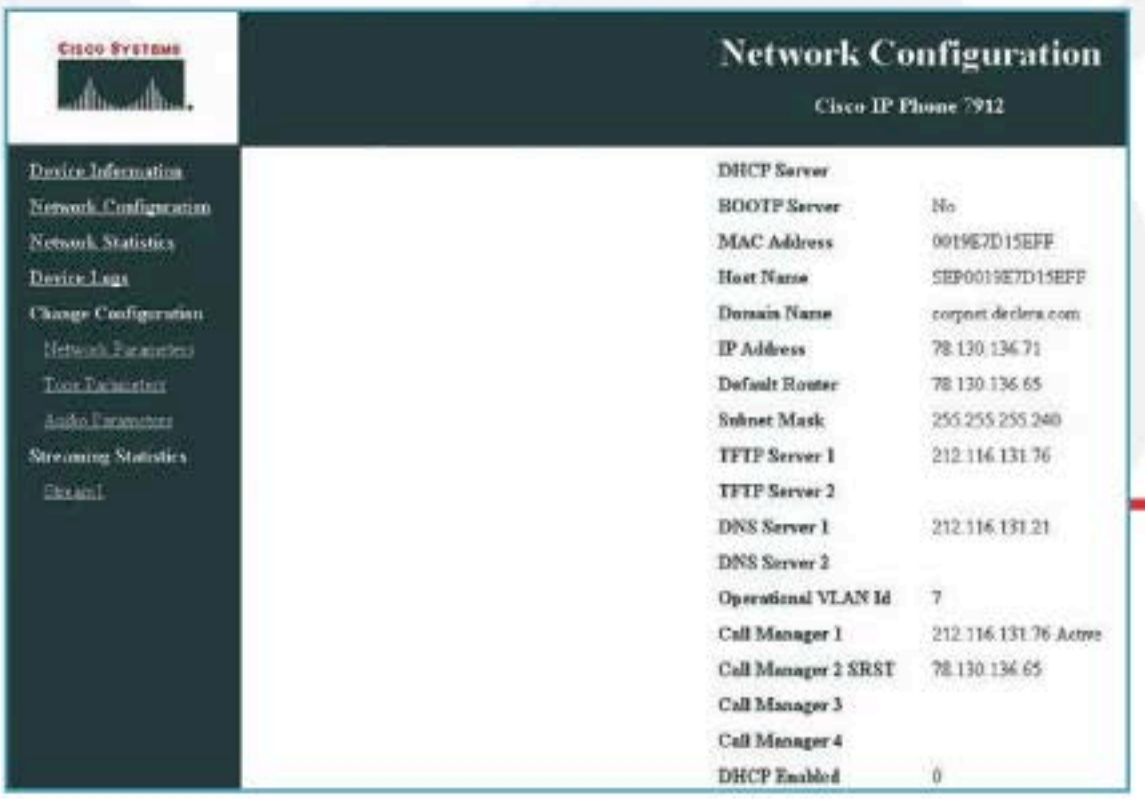
Los teléfonos contienen por lo menos un micrófono en el tubo, y el altavoz posee micrófonos adicionales. Teniendo en cuenta que los teléfonos son controlados por software y, por lo tanto, los micrófonos también, una vulnerabilidad puede permitir, a un atacante, controlar el teléfono y sus micrófonos. Algunas medidas preventivas para áreas críticas consisten en desconectar los micrófonos cuando no son requeridos.

de exploración y ataque. El software que utilizan estos componentes también es vulnerable y posee fallas de seguridad que deben ser consideradas como en cualquier otro sistema de comunicación.
Las soluciones de telefonía IP no se limitan a software o protocolos propietarios como en el caso de las soluciones tradicionales. Los protocolos utilizados son públicamente conocidos y, por lo tanto, un atacante puede estudiarlo en busca de fallas de seguridad. Las **soluciones IP** se basan principalmente en estándares abiertos, como por ejemplo **SIP** (*Session Initiation Protocol*) y **H.323**. Las centrales se basan normalmente en arquitecturas y sistemas operativos estándares de los cuales no es necesario aclarar que se conocen numerosas vulnerabilidades y que es preciso realizar actualizaciones en forma permanente. Las soluciones tradicionales utilizan software y hardware propietario, mucho más difícil de obtener y estudiar en busca de vulnerabilidades. Esto afecta tanto a las centrales como a los teléfonos.

DIVIDIR LA RED EN MÚLTIPLES VLAN NO PROVEE BENEFICIOS DE SEGURIDAD SI EL TRÁFICO ENTRE ELLAS NO ES RESTRINGIDO.

Información

La información transportada por las soluciones IP es mucho más accesible para los atacantes si no se toman ciertas precauciones. Las soluciones tradicionales poseen un cableado dedicado entre el teléfono y la central, en cambio, las soluciones IP comparten el cableado y la red con otros dispositivos de datos. En las redes IP, por defecto cualquier dispositivo es accesible desde otro dispositivo en la misma red. La manipulación de los datos de la red puede permitir a un usuario acceder a la información que circula entre los dispositivos.



Detalles de la configuración de un teléfono IP Cisco 7912. Desde la interfaz web, es posible visualizarla y realizar modificaciones.

Es común encontrar que las centrales IP estén conectadas a Internet aunque no es obligatorio. Esto se da cuando se habilita la central para realizar llamadas o para permitir la administración remota sobre redes IP. Las soluciones tradicionales no se conectan a redes IP, y las llamadas entrantes y salientes solo circulan por la red de las compañías telefónicas. Normalmente, las centrales telefónicas son conectadas en una red de datos existente, lo que implica beneficios para la implementación y administración. Sin embargo, el agregado de telefonía IP incrementa de manera significativa el número de dispositivos, y la red debe adaptarse para cumplir con los requerimientos de la telefonía.

Dispositivos

Para implementar telefonía IP, múltiples dispositivos deben ser conectados a la red tales como servidores, teléfonos IP y gateways. Cada dispositivo debe ser configurado para reducir las posibilidades de ser comprometido, por eso, el diseño de la red y la ubicación de los distintos dispositivos en ella deben ser analizados con cuidado. Entonces tenemos dos capas de protección, la primera la dan los dispositivos, con su configuración y versión de software, y la segunda consiste en el diseño y la configuración de la red. La infraestructura de la red debe estar preparada, y la red perimetral (firewalls y gateways) asegurada antes de que los dispositivos sean deployados.
Por último, los teléfonos IP se disponen y se les permite a los usuarios utilizarlos. De esta manera, se asegura que no existen dispositivos desprotegidos durante la implementación, y que los usuarios tienen funcionalidad completa y calidad de llamados en la implementación.
Las mitigaciones que pueden aplicarse a cada uno de los riesgos presentes en la red dependen de cuán seguro es el entorno actual, de las políticas y procedimientos de seguridad y de la sensibilidad de la información que circula por la red.
La convergencia de la red de datos y voz requiere que la red sea modificada para considerar las amenazas relacionadas con la telefonía IP. La infraestructura de red alcanzada incluye a los dispositivos que procesan los datos, como los switches, routers y firewalls.

Seguridad

La telefonía IP hace a la infraestructura de teléfonos y servidores más accesible a los atacantes. Los ataques contra la red de telefonía se realizan utilizando las mismas herramientas que en la red de datos, pero también se suman herramientas especializadas.

En caso de separarse la red de telefonía de la red de datos, se dificulta su penetración. La implementación de medidas de seguridad sobre la red dificulta el espionaje, pero no permite eliminar el riesgo completamente. La confiabilidad y performance de la red es muy importante en aplicaciones de tiempo real, como lo es la telefonía, por lo que los controles de seguridad que se implementen deben considerar esta variable.

LA IMPLEMENTACIÓN DE SOFTPHONES SUPONE RETOS CUANDO LAS REDES UTILIZAN DISTINTAS VLAN PARA TELÉFONOS Y PCS.

Dividir la red en múltiples VLAN no provee ningún beneficio de seguridad si el tráfico entre las VLAN no se restringe. El tráfico de telefonía IP debe ser controlado por routers que filtren paquetes o switches de capa tres. Las ACLs (*Access Control Lists*) deben configurarse en estos dispositivos solo para permitir que los teléfonos IP se conecten contra los servidores de telefonía IP, y viceversa. En muchos casos, solo el tráfico de señales debe permitirse entre teléfonos y servidores de telefonía IP. El **filtrado** debe realizarse basado en direcciones IP, número de puertos y flags TCP/IP, y no solamente en número de puertos. La red de telefonía IP debería estar separada en VLAN gerenciadas por switches capa 3 y 4 stateful, que bloqueen los protocolos que no sean requeridos por la red de telefonía IP. Una solución aún más robusta es utilizar un firewall de capa 4 para separar las VLAN de telefonía de las VLAN de datos. El firewall de capa 4 y las DMZ asociadas funcionan como un punto de control para el tráfico que circula entre la red de telefonía y la de datos. No debería permitirse ningún tráfico entre la red de datos y la de telefonía que no estuviera expresamente autorizado y monitoreado. En los casos que sea posible, se deben eliminar las necesidades de tráfico entre las redes de datos y telefonía. Por ejemplo, deshabilitar la interfaz web de los teléfonos IP y permitir solamente la conexión desde el servidor central que actualice los teléfonos. Algunos dispositivos, como el servidor de mensajería unificada, cumple un rol en ambas redes y, por lo tanto, debe acceder a las dos. Este tipo de dispositivos debe colocarse en redes DMZ administradas por firewalls de capa 4.

El **espionaje en comunicaciones de voz** no encriptadas es más común sobre redes IP de uso general. Los paquetes multimedia pueden ser reconstruidos una vez capturados por el atacante, aunque pueden ser implementadas diversas protecciones de seguridad para dificultar el espionaje.

Una red switcheada implica que no está difundiendo hacia todos los dispositivos conectados, pero debemos tener en cuenta que es posible modificar un switch para lograrlo. La seguridad física de los switches es una de las primeras medidas por contemplar para reducir este riesgo. Otro método para lograrlo, consiste en inundar (*flood*) el switch con tráfico, lo cual desborda la tabla de MAC Address causando que el tráfico se envíe en forma broadcast (difusión) hacia todos los puertos. Otro método es realizar un ataque del tipo Man-in-the-middle. En este caso, un atacante pretende ser el dispositivo de destino imitando su MAC address.

Los ataques denegación de servicio (DoS) pueden tomar numerosas formas y son difíciles de prevenir. Pueden utilizar vulnerabilidades de software para deshabilitar dispositivos, consumir recursos de un dispositivo o utilizar gran cantidad del ancho de banda. Los dos primeros pueden ser controlados manteniendo el software actualizado, mientras que el excesivo consumo del ancho de banda puede ser controlado al nivel de la red. Las mitigaciones para los ataques DoS pueden generarse limitando el tráfico hacia los servidores de telefonía IP desde el exterior.

Si se detecta a tiempo un atacante de la red de telefonía IP, puede reducirse significativamente el daño que este puede causar. Seleccionar el IDS o IPS adecuado puede tener un gran impacto tanto para la red de datos como para la de telefonía IP. Detectar una intrusión y detenerla implica que el avance no se propaga hacia otras redes internas, por lo que el diseño de la red debe contemplar todas las aplicaciones.

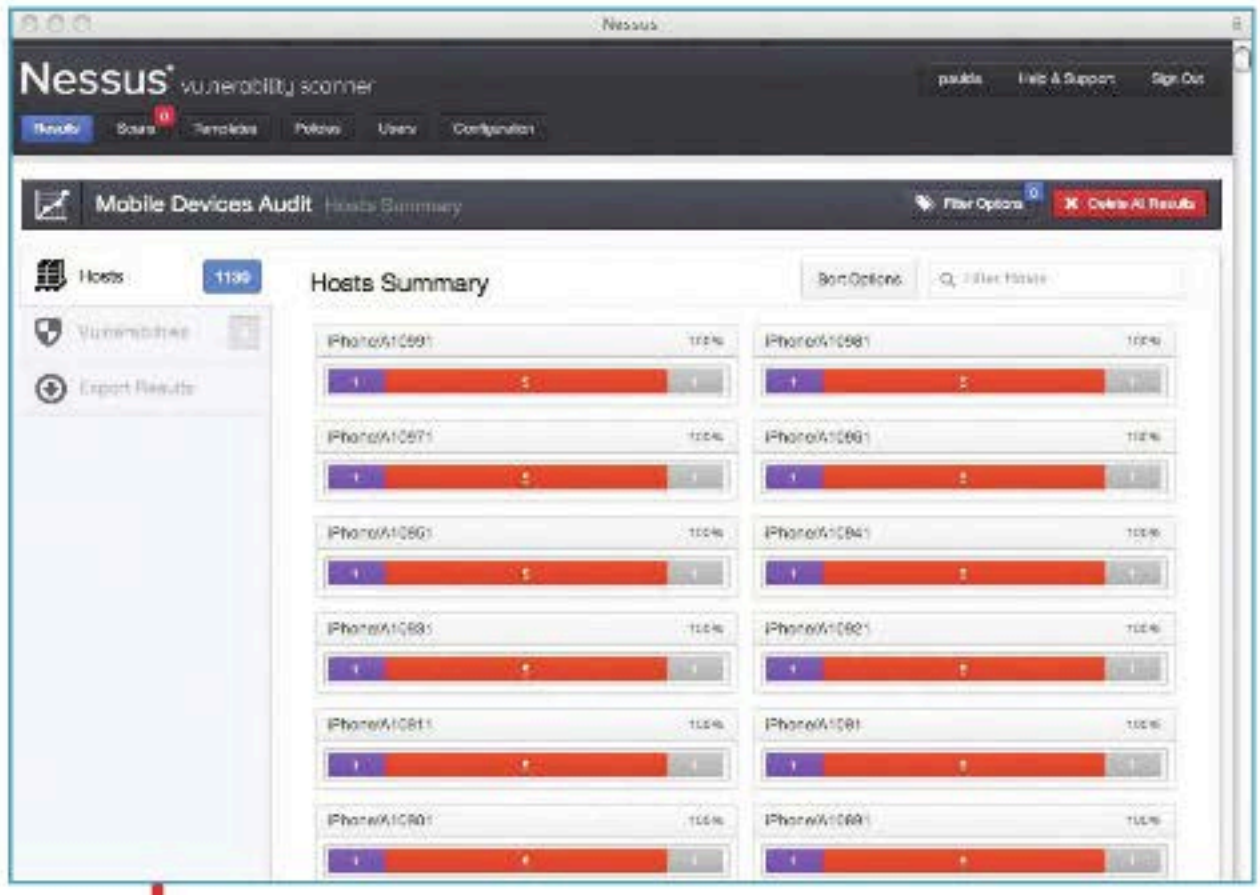
Los servidores de telefonía IP son utilizados para administrar los teléfonos IP. Varios aspectos de estos requieren consideraciones de seguridad para proteger de ataques a los sistemas.

Firewall Cisco ASA 5520. Permite el filtrado de capa 4 entre los distintos segmentos de la red.

El software instalado en los servidores, como el sistema operativo, la base de datos y las aplicaciones VoIP, requieren configuraciones seguras. Debemos tener en cuenta que muchos servidores poseen capacidades de administración remota que los hacen más vulnerables.

Funciones

Los **servidores VoIP** realizan funciones críticas, como autenticación y autorización de teléfonos y usuarios. Los servidores suelen ser servidores de propósito general que ejecutan sistemas operativos como Windows, Unix o Linux. Los datos se almacenan en bases de datos, como Oracle o MS-SQL, y las aplicaciones ejecutan otros servicios requeridos para el normal funcionamiento. Por lo general, todos los sistemas operativos, las bases de datos y las aplicaciones se instalan con configuraciones de seguridad débiles, como passwords por defecto, auditoría desactivada, vulnerabilidades conocidas y más. Todas estas problemáticas deben ser abordadas en forma sistemática no solo para este servicio, sino para todos los que se implementan en el entorno. Los teléfonos IP incluyen una variedad de soluciones de conectividad, como Ethernet, IrDA, Bluetooth y Wi-Fi (802.11a/b/g). Algunos ofrecen todas estas opciones de conectividad y actúan como puntos de acceso, lo que los convierte en potenciales puertas de entrada para intrusos. Mientras que algún tipo de conectividad es requerida, dejar todas las opciones habilitadas supone un riesgo. Cada funcionalidad adicional agrega mayor complejidad y suma una posible vulnerabilidad por aprovechar. La forma más común de conectividad es a través de la red Ethernet. Muchos teléfonos funcionan a su vez como switches permitiendo conectar una PC a él de manera de dejar que un único cable alimente el teléfono y la PC. Esta arquitectura simplifica el despliegue, pero supone que un atacante que gane acceso a la PC pueda acceder directamente al teléfono, y viceversa. Un atacante puede utilizar este acceso para interceptar llamadas o ejecutar un ataque de denegación de servicio. Este riesgo puede reducirse implementando VLAN separadas para teléfonos y PC, pero no todos los teléfonos poseen soporte para VLAN en los switches integrados.



Escaneo de seguridad realizado con Nessus, que detecta vulnerabilidades de red en los equipos VoIP.

Softphones

La implementación de **softphones** supone varios retos cuando, por ejemplo, las redes están separadas y utilizan distintas VLAN para los teléfonos y las PCs. En este caso, una PC debería acceder a la red de datos y de telefonía derivando el modelo de seguridad. Reemplazar teléfonos fijos con softphones genera un único punto de falla, ya que se complejiza la administración, y los usuarios finales pueden cargar softphones no autorizados. Si estos deben ser utilizados, debe generarse otra VLAN para las PCs con softphones. En caso de ser deployados en forma masiva, no es práctico tener dos redes separadas, y debe utilizarse una única VLAN; en este caso, deben contemplarse teléfonos físicos a modo de backup por sectores. ■

Llaves privadas

Algunos servidores almacenan llaves para encriptación y autenticación. Un atacante que gane acceso al servidor podría extraer la llave del servidor y utilizarla para desencriptar las comunicaciones o suplantar identidad. Dependiendo del tipo de llave, pueden implementarse distintas protecciones. Las llaves utilizadas para firmar digitalmente configuraciones, firmware, aplicaciones o certificados deben poseer una contraseña compleja asociada. También es posible utilizar sistemas para gestión de claves, como lo son los tokens.

Ataque de vishing

En estas páginas, analizaremos este tipo de ataque, para conocer su funcionamiento y las medidas de protección necesarias.

En los últimos años, hemos escuchado de la prominente guerra del phishing, el smishing y el vishing en el ámbito de la seguridad informática. Hoy en día, muchos argumentan una posible estafa en sus cuentas bancarias o el probable uso de su identidad para fines de lucro. Debemos saber que existen probabilidades de ataque tanto a los usuarios como a las empresas. Por lo que se aconseja que tengamos disponibles una serie de medidas preventivas que destruyan la posibilidad de que seamos las futuras víctimas de este grupo de prácticas ilícitas.

Origen

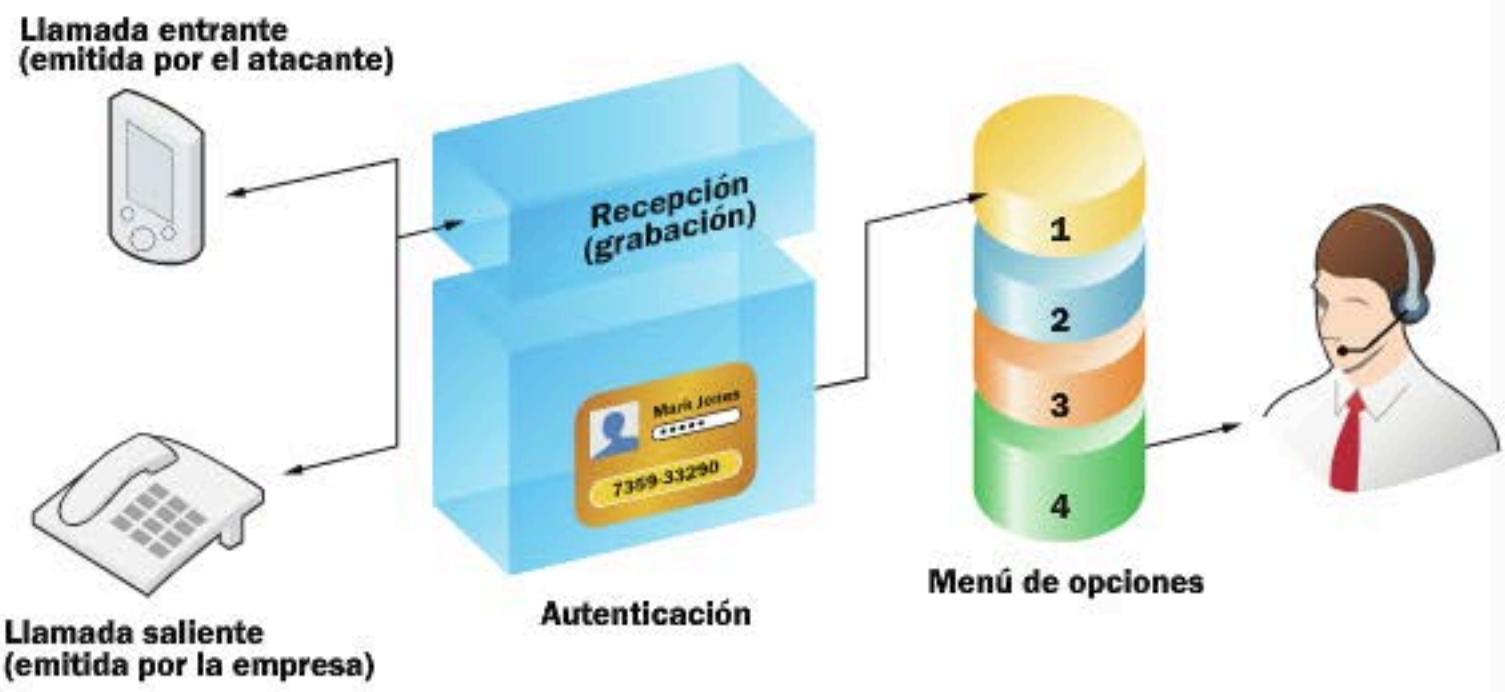
Antes de comenzar de lleno, es necesario aclarar algunos conceptos que nos permitirán comprender la esencia de la palabra **vishing**. Para ello, comencemos armando la definición sobre la base de los siguientes términos: *VoIP* y *phishing*.

VoIP se define propiamente como un conjunto de recursos que hacen posible que la señal de voz viaje a través de Internet (gracias a la intervención del protocolo IP). Mientras que phishing se define como una práctica que consiste en intentar adquirir información, ya sea de una empresa o de un usuario, de forma fraudulenta a través del envío de correo electrónico, a menudo concebido como una modalidad de ataque en el ámbito de la seguridad informática. Vishing hace referencia a una no tan reciente modalidad de fraude mediante intervenciones telefónicas (voz), la cual tiene como finalidad la recopilación de información financiera personal (por lo general de cuentahabientes) para la obtención de beneficios económicos. El vishing es conocido a menudo como phishing telefónico.

EN EL AÑO 2011, LOS USUARIOS DE SKYPE FUERON OBJETO DE VISHING MEDIANTE LA PRESENCIA DE UN SUPUESTO VIRUS.

Funcionamiento

La forma en la que se lleva a cabo este ataque es mediante una llamada telefónica a la víctima. Esta intervención se hace con el propósito de informar que, por cuestiones de seguridad, deben ser verificados un conjunto de datos relacionados con su tarjeta de crédito o información de acceso a sus cuentas bancarias. Por lo general, esta actividad



Los **sistemas IVR** son una alternativa interesante para reducir ataques de phishing con VoIP.

se realiza de manera aleatoria a través de lo que se conoce como **war dialing** (marcado automático de números telefónicos). El *war dialing* es una técnica que originalmente estaba orientada al rastreo de líneas telefónicas, tras una serie de intentos de marcación. Su objetivo es violar los accesos restringidos a las redes locales valiéndose de las vulnerabilidades de los módems. Es evidente que, aunque esto es cosa del pasado, en la actualidad representa la base de muchos de los métodos de intrusión modernos.

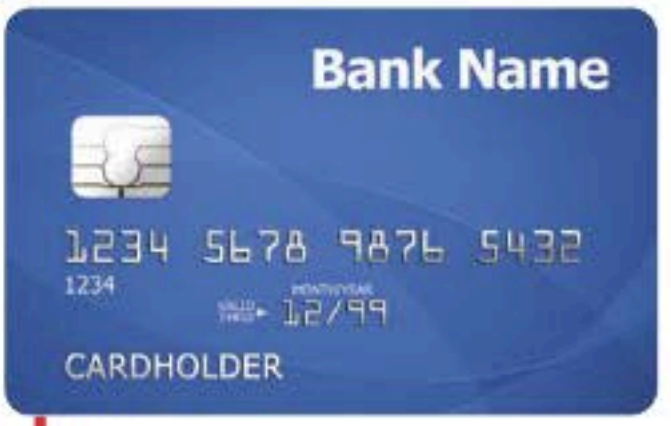
Las llamadas realizadas por el **visher** o atacante a sus víctimas, por lo regular, emiten falsos mensajes pregrabados (en ocasiones en vivo) que informan sobre supuestas promociones, ajustes de información financiera o advertencias. Estas últimas son emitidas aparentemente para notificar que la tarjeta del cuentahabiente está siendo utilizada de forma fraudulenta, por lo que se le solicita que se comunique con cierto número telefónico, donde se obtienen sus datos. La información extraída se trata, por lo general, del número de tarjeta bancaria (la cual tiene dieciséis dígitos), el nombre del titular de la cuenta, fechas de expiración y, en ocasiones, el propio PIN. Datos que luego sirven para estafar al usuario e, incluso, robar su identidad.

La infraestructura VoIP representa hoy en día un recurso muy vulnerable, a tal grado que muchos criminales cibernéticos pueden ser capaces de alterar el identificador de llamadas para lograr que el número del remitente aparezca como si viniera desde el banco. Por lo que resulta más sencilla la manipulación del número de llamadas con VoIP en comparación con el uso de una infraestructura diferente.

Medidas de prevención

Este método de fraude se encuentra hoy de moda, y atenta contra la integridad de la persona física y moral involucrada en menesteres financieros. En primera instancia, si por alguna razón estamos considerando la implementación de IP en nuestro negocio o empresa, no olvidemos estar preparados para enfrentar cualquier problema. Por esta razón, vamos a citar una serie de medidas a las que podemos recurrir para evitar ser estafados:

- Prescindamos de emitir información personal o confidencial a cualquier dependencia u organización que no sea nuestro propio banco.
- Después de atendida la llamada telefónica que advierte sobre un supuesto fraude financiero, colguemos el teléfono sin brindar ningún dato y dirijámonos a la sucursal bancaria de nuestra elección para hacer las preguntas pertinentes.
- Ante cualquier aclaración, cambio de información financiera personal, validación de números de cuenta, cancelación de tarjetas, etc., comuniquémonos en forma directa con el banco. De preferencia, consigamos ser atendidos en forma personal por un asesor.
- Evitemos realizar transacciones bancarias mediante números telefónicos que recibamos, así hayan sido enviados al móvil o celular, o bien a través de mensajes de texto o también a través de correos electrónicos.
- En la medida de lo posible, se recomienda el uso de un sistema IVR para el monitoreo de las llamadas telefónicas (este sistema se describe más adelante) o mediante la aplicación de sistemas de biometría de voz.



Las tarjetas de crédito son el blanco perfecto para la estafa por phishing con VoIP.

Solución

Aunque se sabe que no existe una solución tecnológica contra este tipo de ataques, se han desarrollado propuestas bastante interesantes para ayudar a reducir problemas por vishing, tales como: los sistemas de reconocimiento de voz (biométricos) y los sistemas **IVR** (*Interactive Voice Response*, respuesta interactiva de voz). Estas opciones figuran hoy en día como una buena opción para monitorear llamadas telefónicas entrantes y protegernos ante cualquier fraude. Es aceptado por muchas compañías para garantizar la seguridad de sus usuarios al realizar operaciones. ■

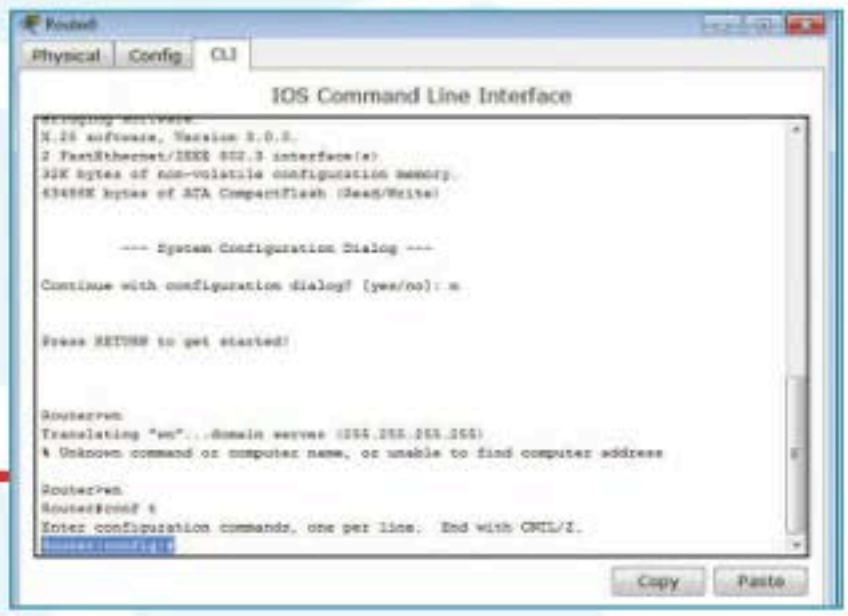
Internet Background Noise (IBN)

En esta sección, analizaremos el ruido de fondo de Internet, su origen y otros conceptos relacionados.

Poco se conoce sobre el llamado ruido de fondo de Internet (**IBN** *Internet Background Noise*), referido por otros autores como radiación de fondo de Internet. En este apartado, daremos a conocer algunos datos interesantes sobre este fenómeno que puede atentar contra la seguridad en las redes. El IBN consiste en una serie de paquetes de datos que viajan a través de Internet, los cuales pueden ser capaces de dirigirse en forma directa a una dirección IP o cargarse en un puerto (sin uso) de cualquiera de los dispositivos de una red. Estos paquetes, por lo general, se hallan estructurados de mensajes de control de red y tráfico, y figuran como el resultado del escaneo de puertos TCP y ciertas actividades maliciosas por lo general originadas por un gusano en particular, conocido como **Conficker**.

Origen de IBN

El ruido de fondo de Internet es, a menudo, generado por algún virus (malware) en busca de nuevas víctimas, hardware mal configurado (terminales de telefonía IP), fugas de datos en redes privadas y tráfico en la red (debido al número de módems que operan con una dirección IP no modificable). La vulnerabilidad del protocolo de Internet en su versión cuatro (IPv4) también ha hecho posible la infiltración del prominente ruido de fondo. Actualmente, el nuevo diseño del protocolo IPv6, en comparación con la versión cuatro, cuenta con un arreglo de direcciones mucho más grande, por lo que hará que sea más difícil que los virus o el malware sean capaces de escanear los puertos. Con esta implementación, también conseguiremos reducir problemas por configuración inadecuada del hardware o terminales presentes en las redes de datos.



El hardware mal configurado: una de las causas principales del IBN.

El gusano de la red

Los paquetes que conforman el fenómeno IBN, muchas veces, son el principal hangar de este temido intruso también conocido como el gusano de la red, el cual es el responsable de más del cincuenta por ciento del ruido de fondo en Internet. Una particularidad de este intruso es su rápida reproducción por todo el sistema operativo de una PC conectada a una red informática. Hoy en día, muchas son las soluciones que pueden auxiliarnos para combatir este tipo de amenazas. Un conjunto de medidas de prevención, como ya sabemos, suele ser contar con un buen antivirus, un firewall bien configurado y, desde luego, un sistema operativo debidamente actualizado.

El tráfico en Internet

En años anteriores, se estimaba que, cada segundo, se generaba un promedio de 5 GB de ruido de fondo en Internet, y a menudo se pensaba que un usuario podía perder cerca de 20 bits cada segundo por tráfico no solicitado. Durante la década pasada, la cantidad de ruido de fondo de una sección del bloque de direcciones IPv4 se ha incrementado de 1 a 50 Mbps. IPv6 puede ser la alternativa para evitar problemas por ruido blanco.

Retrodispersión

La **retrodispersión** es un término empleado para describir el ruido de fondo de Internet como resultado de un ataque. Sabemos que la causa principal de la existencia del IBN son los virus (conocidos como malware), los cuales se convierten en los protagonistas del IBN. Retrodispersión, también conocido como devoluciones de mensajes de spam, es una actividad que consiste en la dispersión de mensajes de red enviados en forma masiva a través de Internet. ■

CONVIÉRTETE EN UN EXPERTO CON LA COLECCIÓN:

SALIDA LABORAL

TÉCNICO en ELECTRÓNICA

CONCEPTOS FUNDAMENTALES Y PRÁCTICA PROFESIONAL

CON ESTA COLECCIÓN PODREMOS:

- ENTENDER LOS CONCEPTOS CLAVES DE ELECTRICIDAD Y ELECTRÓNICA.
- UTILIZAR LOS INSTRUMENTOS DE MEDICIÓN DE LABORATORIO.
- SIMULAR, CONSTRUIR Y MEDIR CIRCUITOS.
- CONTROLAR DISPOSITIVOS DE MANERA INALÁMBRICA.
- APROVECHAR AL MÁXIMO SENSORES Y TRANSDUCTORES.
- UTILIZAR LA PLATAFORMA ARDUINO.

ESTA OBRA INCLUYE:

24 fascículos + **4** libros + **3** eBooks + **1** coleccionador

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00023
9 789871 857784

CONTENIDO DE LA OBRA