TEMA 9
INSTALACIÓN
Y
ADMINISTRACIÓN
DE
OTROS SERVICIOS
DE RED E INTERNET

Servicio horario NTP

Protocolo NTP

Servicio de sindicación

Protocolos RSS y Atom
Clientes o Agregadores de sindicación

Servicio de terminal remoto

Telnet, Rlogin, SSH
X-Terminal
Escritorio remoto VNC
Terminal Server
Acceso remoto mediante interface web

Servicio de tecnología de voz IP “VoIP”

Telefonía tradicional
Funcionamiento de VoIP
Protocolos VoIP
Elementos VoIP

Servicio horario NTP.

Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable.

Protocolo NTP.

Network Time Protocol (NTP) es un protocolo de Internet para sincronizar los relojes de los sistemas informáticos a través del ruteo de paquetes en redes con latencia variable. NTP utiliza UDP como su capa de transporte, usando el puerto 123. Está diseñado para resistir los efectos de la latencia variable. NTP utiliza el Algoritmo de Marzullo con la escala de tiempo UTC, incluyendo soporte para características como segundos intercalares. NTPv4 puede mantenerse sincronizado con una diferencia máxima de 10 milisegundos (1/100 segundos) a través de Internet, y puede llegar a acercarse hasta 200 microsegundos (1/5000 segundos) o más en redes de área local sobre condiciones ideales.

El demonio NTP de Unix es un proceso de nivel de usuario que se ejecuta continuamente en la máquina que soporta NTP, y la mayor parte del protocolo está implementado en este proceso de usuario. Para obtener el mejor rendimiento de NTP, es importante tener un reloj NTP estándar con lazo de seguimiento de fase implementado en el kernel del Sistema operativo, en vez de sólo usar la intervención de un demonio NTP externo: todas las versiones actuales de GNU/Linux y Solaris soportan esta característica. NTP utiliza un sistema de jerarquía de *estratos de reloj*, en donde los sistemas de estrato 1 están sincronizados con un reloj externo tal como un reloj GPS ó algún reloj atómico. Los sistemas de estrato 2 de NTP derivan su tiempo de uno ó más de los sistemas de estrato 1, y así consecutivamente (cabe mencionar que esto es diferente de los estratos de relojes utilizados en los sistemas de telecomunicaciones).

Las estampas de tiempo utilizadas por NTP consisten en un segundo de 32-bit y una parte fraccional de 32-bit, dando con esto una escala de 232 segundos (136 años), con una resolución teórica de 2−32 segundos (0.233 nanosegundos). Aunque las escalas de tiempo NTP se redondean cada 232 segundos, las implementaciones deberían desambiguar el tiempo NTP utilizando el tiempo aproximado de otras fuentes. Esto no es un problema en la utilización general ya que esto solamente requiere un tiempo cercano a unas cuantas décadas.

Servicio de sindicación.

La Sindicación de Contenidos es una forma que tienen algunos sitios web de distribuir contenidos a los que los usuarios acceden frecuentemente. El contenido se distribuye a través de unos Canales y los usuarios pueden leer esos canales con un software denominado programa Agregador (también llamado Lector de Canales o Lector de Noticias, en inglés: Newsreader o Feed Reader). Un ejemplo fácil de entender sería la sindicación de los titulares de noticias de última hora de un periódico. Los usuarios pueden recibir dichos titulares y, si están interesados en ver más información, hacer un clic para llegar a la página web original. Además de titulares de noticias, los Canales de Sindicación pueden contener otros tipos de información, como mensajes de un foro, avisos importantes, nuevos contenidos añadidos en un web, etc.

Protocolos RSS y Atom.

RSS son las siglas de **Really Simple Syndication**, un formato XML para sindicar o compartir contenido en la web. Se utiliza para difundir información actualizada frecuentemente a usuarios que se han suscrito a la fuente de contenidos. El formato permite distribuir contenidos sin necesidad de un navegador, utilizando un software diseñado para leer estos contenidos RSS (agregador). A pesar de eso, es posible utilizar el mismo navegador para ver los contenidos RSS. Las últimas versiones de los principales navegadores permiten leer los RSS sin necesidad de software adicional. RSS es parte de la familia de los formatos XML desarrollado específicamente para todo tipo de sitios que se actualicen con frecuencia y por medio del cual se puede compartir la información y usarla en otros sitios web o programas. A esto se le conoce como redifusión web o *sindicación web* (una traducción incorrecta, pero de uso muy común).

ATOM hace referencia a dos estándares relacionados.

- El *Formato de Redifusión Atom* es un fichero en formato XML usado para Redifusión web.
- mientras que el *Protocolo de Publicación Atom* (resumido en Inglés *AtomPub* o *APP*) es un protocolo simple basado en HTTP para crear o actualizar recursos en Web.

Las fuentes web permiten que los programas busquen actualizaciones del contenido publicado en un sitio Web. Para crear uno el propietario de un sitio Web puede usar software especializado, como un Sistema de gestión de contenido que publica una lista (o fuente web) de artículos recientes en un formato estándar, legible por máquinas. La fuente web puede ser descargada por sitios web que redifunden el contenido usando la fuente web, o por un agregador que permiten que los lectores en Internet se suscriban y vean los contenidos de la fuente web.
Una fuente web puede contener entradas, que pueden ser encabezados, artículos completos, resúmenes y/o enlaces al contenido de un sitio web.
El formato Atom fue desarrollado como una alternativa a RSS. Ben Trott fue uno de los defensores del nuevo formato que llegó a llamarse Atom. Él notó la incompatibilidad entre algunas versiones del protocolo RSS, ya que pensaba que los protocolos de publicación basados en XML-RPC no eran lo suficientemente interoperables.

Clientes o Agregadores de sindicación.

Los agregadores o *lectores de fuentes web* (programas o sitios que permiten leer fuentes web) se pueden obtener resúmenes de todos los sitios que se desee desde el escritorio del sistema operativo, programas de correo electrónico o por medio de aplicaciones web que funcionan como agregadores.

No es necesario abrir el navegador y visitar decenas de páginas.

FeedReader: Agregador RSS, intuitivo y moderno.

Feeddemon: Software RSS. Uno de los más potentes y utilizados. Interfaz fácil de usar

Rssowl: Lector de feeds. Múltiples características. Código libre.

Rss Feed Creator: Crea y edita fácilmente tus propios RSS.

Jitbit Rss Feed Creator: Edita tu propio canal RSS sin ningún conocimiento de XML.

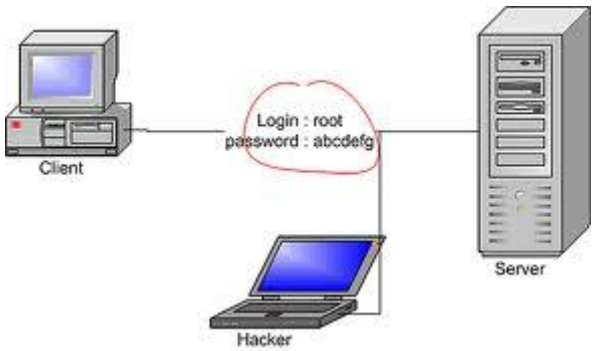
Mini-Rssl: Crear miniRss para tu página en un santiamén.

Servicio de terminal remoto:

Se trata de un servicio desde un equipo acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.

Telnet, Rlogin, SSH.

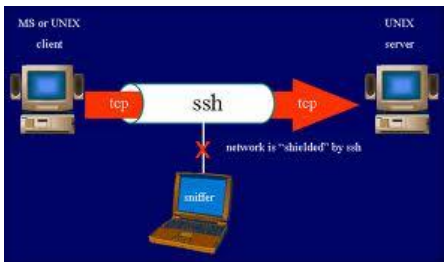
Telnet: Telnet (**TELecommunication NETwork**) es el nombre de un protocolo de red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. También es el nombre del programa informático que implementa el cliente. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.
Telnet sólo sirve para acceder en modo terminal, es decir, sin gráficos, pero fue una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente en el mismo sitio que la máquina que los tenía. También se usaba para consultar datos a distancia, como datos personales en máquinas accesibles por red, información bibliográfica, etc.
Aparte de estos usos, en general **telnet** se ha utilizado (y aún hoy se puede utilizar en su variante SSH) para abrir una sesión con una máquina UNIX, de modo que múltiples usuarios con cuenta en la máquina, se conectan, abren sesión y pueden trabajar utilizando esa máquina. Es una forma muy usual de trabajar con sistemas UNIX.



Rlogin: Rlogin (Remote Login) es una aplicación TCP/IP que comienza una sesión de terminal remoto sobre el anfitrión especificado como host. El anfitrión remoto debe hacer funcionar un servicio de Rlogind (o demonio) para que el Rlogin conecte con el anfitrión. Utiliza un mecanismo estándar de autorización de los Rhosts. Cuando no se especifica ningún nombre de usuario ni con la opción -l ni con la opción username@, Rlogin conecta como el usuario actualmente logueado.
El Rlogin envía realmente dos nombres de usuario al servicio del Rlogind (o al demonio): remuser y locuser.
- **El remuser** es el nombre con el que se registra al usuario en la máquina cliente (e incluye su dominio o nombre de la máquina). Es llamado remuser por el servidor (o demonio) porque desde el punto de vista del servidor(o demonio), la máquina del cliente es remota. El remuser es el nombre que debe aparecer en el archivo global de hosts. El remuser no se puede fijar por el usuario.

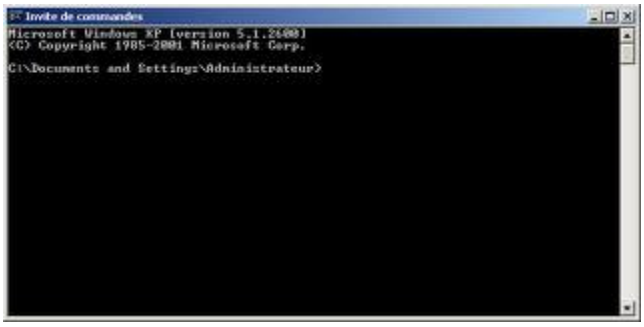
El locuser es el nombre del usuario que el servidor (o demonio) utiliza para ejecutar el comando en el servidor. Desde el punto de vista del servidor (o demonio), el servidor es la máquina local. Éste es el nombre del usuario con el que estás actualmente conectado o el nombre del usuario incorporado explícitamente en la línea de comando del rlogin.

SSH (**S**ecure **SH**ell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.
Además de la conexión a otros dispositivos, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a los dispositivos y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.
SSH trabaja de forma similar a como se hace con telnet. La diferencia principal es que SSH usa técnicas de cifrado que hacen que la información que viaja por el medio de comunicación vaya de manera no legible y ninguna tercera persona pueda descubrir el usuario y contraseña de la conexión ni lo que se escribe durante toda la sesión; aunque es posible atacar este tipo de sistemas por medio de ataques de REPLAY y manipular así la información entre destinos.



X-Terminal

Es un terminal de pantalla/entrada para las aplicaciones cliente del X Windows System. Los terminales X disfrutaron de un período de popularidad a principio de los años 1990 cuando ofrecieron un costo total de propiedad más bajo alternativo a una completa estación de trabajo UNIX. Un terminal X corre con un servidor X. (En el X, el uso de los términos "cliente" y "servidor" se hace desde el punto de vista de los programas: el servidor X suministra una pantalla, un teclado, un ratón y una pantalla táctil a las aplicaciones cliente).
Esto hace una conexión con un X Display Manager (introducido en el X11R3) corriendo en una máquina central, usando el X Display Manager Control Protocol (XDMCP), introducido en el X11R4). Los clientes livianos han suplantado algo a los terminales X puesto que los "engordan" agregando memoria flash que contiene software que duplica mucho a los varios sistemas operativos de Microsoft, así adquiriendo la capacidad de "hablar" en una gama de protocolos de escritorios remotos.



Escritorio remoto VNC

Un **escritorio remoto** es una tecnología que permite a un usuario trabajar en una computadora a través de su escritorio gráfico desde otro terminal ubicado en otro lugar.
La tecnología de escritorio remoto permite la centralización de aquellas aplicaciones que generalmente se ejecutan en entorno de usuario (por ejemplo, procesador de textos o navegador). De esta manera, dicho entorno de usuario se transforma en meros terminales de entrada/salida.
Los eventos de pulsación de teclas y movimientos de ratón se transmiten a un servidor central donde la aplicación los procesa como si se tratase de eventos locales. La imagen en pantalla de dicha aplicación es retornada al terminal cliente cada cierto tiempo.

Elementos básicos:
-. Protocolo de comunicaciones
El elemento característico en cualquier implementación de escritorio remoto es su protocolo de comunicaciones, que varía dependiendo del programa que se use:
*Independent Computing Architecture (**ICA**), utilizado por MetaFrame.*

- *Remote Desktop Protocol (**RDP**), utilizado por Terminal Services.*
- *Adaptive Internet Protocol (**AIP**), utilizado por Secure Global Desktop.*
- *Virtual Network Computing, (**VNC**), utilizado por el producto del mismo nombre.*
- ***X11**, utilizado por X-Windows.*

VNC son las siglas en inglés de Virtual Network Computing (**Computación Virtual en Red**). **VNC** es un programa de software libre basado en una estructura cliente-servidor el cual nos permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente.
También llamado software de escritorio remoto. VNC no impone restricciones en el sistema operativo del ordenador servidor con respecto al del cliente: es posible compartir la pantalla de una máquina con cualquier sistema operativo que soporte VNC conectándose desde otro ordenador o dispositivo que disponga de un cliente VNC portado. La versión original del **VNC** se desarrolló en Reino Unido, concretamente en los laboratorios AT&T Olivetti Research Laboratory, en Cambridge, Reino Unido.
El programa era de código abierto por lo que cualquiera podía modificarlo y existen hoy en día varios programas para el mismo uso. Muchos derivados modernos de él son software libre bajo licencia GNU General Public License.

Terminal Server

Los **Servicios de Escritorio Remoto** (del inglés **Remote Desktop Services**), antiguamente conocido como **Servicios de Terminal** (o **Terminal Services**) son un componente de los sistemas operativos Windows que permite a un usuario acceder a las aplicaciones y datos almacenados en otro ordenador mediante un acceso por red. Basado en el protocolo de escritorio remoto (Remote Desktop Protocol (RDP)) aparece por primera vez en Windows NT 4.0 (Terminal Server Edition). Los productos Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows Server 2003 y Windows Server 2008 han introducido algunas mejoras y funcionalidades nuevas. Microsoft proporciona el software cliente para todas las versiones de Windows 32 bits y para Mac OS X de Apple. El uso de los servicios de terminal requiere de tres componentes:
1) Servidor de Terminal Server.
2) Cliente de Terminal Server.
3) Protocolo de escritorio remoto.
La instalación de dicho componente no supone mayor problema ya que se incorpora en los sistemas operativos, aunque sí que es algo diferente en Windows 2000 y 2003. Podemos distinguir dos tipos de instalación:
1) **Modo Administración remota:** proporciona acceso remoto a los servidores por parte de los administradores. Soporta, además de la sesión de consola, dos sesiones más, sin tener que pagar ninguna licencia extra

2) **Modo Servidor de Aplicaciones:** permite el acceso simultáneo por parte de varios clientes remotos. En este caso sí será necesario adquirir licencias de terminal.

Acceso remoto mediante interface web.

El acceso remoto mediante el navegador es uno de los más utilizados a la hora de manipular otras máquinas. Esto se debe a que la mayoría de equipos informáticos que necesitan tener acceso a contenido web (ya sea local o en red) y para esto es necesario un navegador Web. Teniendo en cuenta este dado, los fabricantes de dispositivo electrónicos han guiado sus esfuerzos a la manipulación de sus dispositivos mediante el navegador. Buen ejemplo de estos pueden ser los router o las videocámaras Ip. También se han realizado grandes progresos a la hora del acceso y manipulación remota de equipo al equipo a nivel de Sistema Operativo, esto consiste en realizar algunos cambios de permisos en el Sistema de la máquina a la que se quiere acceder para que la otra máquina mediante el navegador pueda acceder a la máquina como manipularla.

Servicio de tecnología de voz IP "VoIP."

Voz sobre Protocolo de Internet, también llamado **Voz sobre IP**, **Voz IP**, **VozIP**, **VoIP** (por sus siglas en inglés, Voice over IP), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet). Esto significa que se envía la señal de voz en forma digital, en paquetes de datos, en lugar de enviarla en forma analógica a través de circuitos utilizables sólo por telefonía convencional como las redes PSTN.
Los Protocolos que se usan para enviar las señales de voz sobre la red IP se conocen como protocolos de Voz sobre IP o protocolos IP. Estos pueden verse como aplicaciones comerciales de la "Red experimental de Protocolo de Voz" (1973), inventada por ARPANET. El tráfico de Voz sobre IP puede circular por cualquier red IP, incluyendo aquellas conectadas a Internet, como por ejemplo las redes de área local (LAN). Es muy importante diferenciar entre Voz sobre IP (VoIP) y Telefonía sobre IP.

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

- Telefonía sobre IP es el servicio telefónico disponible al público, por tanto con numeración E.164, realizado con tecnología de VoIP.

Telefonía tradicional.

El **teléfono** es un dispositivo de telecomunicación diseñado para transmitir señales acústicas por medio de señales eléctricas a distancia.
Los sistemas de telefonía tradicional están guiados por un sistema muy simple pero ineficiente denominado conmutación de circuitos. La conmutación de circuitos ha sido usada por las operadoras tradicionales por más de 100 años.
En este sistema cuando una llamada es realizada la conexión es mantenida durante todo el tiempo que dure la comunicación. Este tipo de comunicaciones es denominada "circuito" porque la conexión esta realizada entre 2 puntos hacia ambas direcciones.
Estos son los fundamentos del sistema de telefonía convencional.

Así es como funciona una llamada típica en un sistema de telefonía convencional:

1. Se levanta el teléfono y se escucha el tono de marcado. Esto deja saber que existe una conexión con el operador local de telefonía.
2. Se marca el número de teléfono al que se desea llamar.
3. La llamada es transmitida a trabes del conmutador (switch) de su operador apuntando hacia el teléfono marcado.
4. Una conexión es creada entre tu teléfono y la persona que se está llamando, entremedio de este proceso el operador de telefonía utiliza varios conmutadores para lograr la comunicación entre las 2 líneas.
5. El teléfono suena a la persona que estamos llamando y alguien contesta la llamada.
6. La conexión abre el circuito.
7. Uno habla por un tiempo determinado y luego cuelga el teléfono.
8. Cuando se cuelga el teléfono el circuito automáticamente es cerrado, de esta manera liberando la línea y todas las líneas que intervinieron en la comunicación.

Funcionamiento de VoIP.

Funcionamiento de forma básica:
1. La voz es digitalizada y transformada en el origen de la llamada en un conjunto de paquetes de información, que son transmitidos a través de la red.

2. Para alcanzar el destino, cada paquete puede seguir un camino distinto, dependiendo de las condiciones de la red, y compartiendo el medio con otros paquetes de datos.

3. Finalmente, en el destino estos paquetes de datos son ordenados y transformados de nuevo en voz.

Funcionamiento de forma extendida:
1. Se levanta el teléfono, lo que envía una señal al conversor analógico-digital llamado ATA.

2. El ATA recibe la señal y envía un tono de llamado, esto deja saber que ya se tiene conexión a internet.

3. Se marca el numero de teléfono de la persona que se desea llamar, los números son convertidos a digital por el ATA y guardados temporalmente.

4. Los datos del número telefónico son enviados a tu proveedor e VoIP. Las computadoras de tu proveedor VoIP revisan este numero para asegurarse que esta en un formato valido.

5. El proveedor determina a quien corresponde este número y lo transforma en una dirección IP.

6. El proveedor conecta los dos dispositivos que intervienen en la llamada. En la otra punta, una señal es enviada al ATA de la persona que recibe la llamada para que este haga sonar el teléfono de la otra persona.

7. Una vez que la otra persona levanta el teléfono, una comunicación es establecida entre tu computadora y la computadora de la otra persona. Esto significa que cada sistema está esperando recibir paquetes del otro sistema. En el medio, la infraestructura de internet maneja los paquetes de voz la comunicación de la misma forma que haría con un email o con una página web. Cada sistema debe estar funcionando en el mismo protocolo para poder comunicarse. Los sistemas implementan dos canales, uno en cada dirección.

8. Se habla por un periodo de tiempo. Durante la conversación, tu sistema y el sistema de la persona que se está llamando transmiten y reciben paquetes entre sí.

9. Cuando se termina la llamada, se cuelga el teléfono. En este momento el circuito es cerrado.

10. El ATA envía una señal al proveedor de Telefonía IP informando que la llamada a sido concluida.

Protocolos VoIP.

El objetivo del **protocolo de VoIP** es dividir en paquetes los flujos de audio para transportarlos sobre redes basadas en IP. Los protocolos de las redes IP originalmente no fueron diseñados para el fluido el tiempo real de audio o cualquier otro tipo de medio de comunicación. La PSTN está diseñada para la transmisión de voz, sin embargo tiene sus limitaciones tecnológicas.
Es por lo anterior que se crean los protocolos para voip, cuyo mecanismo de conexión abarca una serie de transacciones de señalización entre terminales que cargan dos flujos de audio para cada dirección de la conversación.
A algunos de los protocolos voip más importantes:

SIP (Session Initiation Protocol) es un protocolo de señalización para conferencia, telefonía, presencia, notificación de eventos y mensajería instantánea a través de

Internet. Fue desarrollado inicialmente en el grupo de trabajo IETF MMUSIC (Multiparty Multimedia Session Control) y, a partir de Septiembre de 1999, pasó al grupo de trabajo IETF SIP.

• Acrónimo de “Session Initiation Protocol”.

• Este protocolo considera a cada conexión como un par y se encarga de negociar las capacidades entre ellos.

• Tiene una sintaxis simple, similar a HTTP o SMTP.

• Posee un sistema de autenticación de pregunta/respuesta.

• Tiene métodos para minimizar los efectos de DoS (Denial of Service o Denegación de Servicio), que consiste en saturar la red con solicitudes de invitación.

• Utiliza un mecanismo seguro de transporte mediante TLS.

• No tiene un adecuado direccionamiento de información para el funcionamiento con NAT.

IAX

• Acrónimo de “Inter Asterisk eXchange”.

• IAX es un protocolo abierto, es decir que se puede descargar y desarrollar libremente.

• Aún no es un estándar.

• Es un protocolo de transporte, que utiliza el puerto UDP 4569 tanto para señalización de canal como para RTP (Protocolo de Transporte en tiempo Real).

• Puede truncar o empaquetar múltiples sesiones dentro de un flujo de datos, así requiere de menos ancho de banda y permite mayor número de canales entre terminales.

• En seguridad, permite la autenticación, pero no hay cifrado entre terminales.

• Según la documentación (Asterisk 1.4) el IAX puede usar cifrado (aes128), siempre sobre canales con autentificación MD5.

H.323

• Originalmente fue diseñado para el transporte de vídeo conferencia.

• Su especificación es compleja.

• H.323 es un protocolo relativamente seguro, ya que utiliza RTP.

• Tiene dificultades con NAT, por ejemplo para recibir llamadas se necesita direccionar el puerto TCP 1720 al cliente, además de direccionar los puertos UDP para la media de RTP y los flujos de control de RTCP.

• Para más clientes detrás de un dispositivo NAT se necesita gatekeeper en modo proxy.

MGCP

• Acrónimo de “Media Gateway Control Protocol”.

• Inicialmente diseñado para simplificar en lo posible la comunicación con terminales como los teléfonos.

• MGCP utiliza un modelo centralizado (arquitectura cliente * servidor), de tal forma que un teléfono necesita conectarse a un controlador antes de conectarse con otro teléfono, así la comunicación no es directa.

• Tiene tres componentes un MGC (Media Gateway Controller), uno o varios MG (Media Gateway) y uno o varios SG (Signaling Gateway), el primero también denominado dispositivo maestro controla al segundo también denominado esclavo.
• No es un protocolo estándar.

SCCP
• Acrónimo de "Skinny Client Control Protocol".
• Es un protocolo propietario de Cisco.
• Es el protocolo por defecto para terminales con el servidor Cisco Call Manager PBX que es el similar a Asterisk PBX.
• El cliente Skinny usa TCP/IP para transmitir y recibir llamadas.
• Para el audio utiliza RTP, UDP e IP.
• Los mensajes Skinny son transmitidos sobre TCP y usa el puerto 2000.

Elementos VoIP.

La complejidad de una infraestructura VoIP para la empresa puede variar sustancialmente según las necesidades de ésta. De este modo, se puede plantear una sencilla solución basada en instalar algún software especializado en los ordenadores de la empresa a los que va a dotar de la capacidad de establecer llamadas mediante esta tecnología.
En cambio, también es posible realizar implantaciones más avanzadas que permitan a la empresa disponer de un completo centro de comunicaciones con diversos terminales, centralita telefónica, etc. En el caso de estas implantaciones más avanzadas se hace necesaria la intervención de una empresa especializada.

Entre los distintos elementos que pueden formar parte de la infraestructura se pueden encontrar los siguientes:
-. Terminales: Para poner en funcionamiento un sistema VoIP hacen falta los instrumentos necesarios para realizar la transformación de la voz en datos y viceversa. Estos instrumentos pueden ser terminales IP o terminales no IP.
• Entre los terminales no IP se encuentran los teléfonos y faxes convencionales, por ejemplo.

• Entre los terminales IP podemos incluir el teléfono IP y el fax IP (terminales hardware), y los ordenadores (terminales software).

De cara al usuario, tanto la apariencia como la funcionalidad de los teléfonos IP es igual a los teléfonos actuales, lo que permite eliminar la desconfianza inicial que puede

producir el cambio. Por otro lado, los terminales software ejecutándose en un ordenador personal puede producir un mayor rechazo inicial en el usuario, pero las capacidades y posibilidades que ofrecen son superiores: disponer de una agenda integrada, posibilidad de envío simultáneo de ficheros, etc. La diferencia fundamental entre ambos es que los primeros son capaces de entregar a su salida la conversación telefónica en formato IP, mientas que los segundos no, por lo que necesitan de un dispositivo intermedio que haga esta conversión.

-. Gateway: Se denomina Gateway al dispositivo intermedio que permite reutilizar terminales no IP (como los teléfonos convencionales) para su uso con VoIP. Por una parte se conecta a la red telefónica convencional (RTB) y por el otro a una red informática (por ejemplo Internet), haciendo de puente entre ambas. De este modo, se pueden utilizar teléfonos convencionales dentro del sistema VoIP.

Gatekeeper: Aunque no es imprescindible disponer de este elemento en el sistema, sí que es conveniente, ya que lo dota de mayores capacidades. Su función es el control de las llamadas y la gestión de su direccionamiento, todo terminal antes de realizar una llamada, debe consultar con el gatekeeper si ésta es posible. Una vez obtenido permiso, el gatekeeper es quien realiza la traducción entre el identificador de usuario destino y la dirección a la que dirigir la llamada, a modo de agenda telefónica.

-. Otros elementos: Existen otros elementos que van a permitir dotar de mayor funcionalidad a los sistemas VoIP implantados en la empresa. Este es el caso de una central telefónica o PBX, que puede ser implementada de manera sencilla mediante software, lo que reduce de una manera muy importante la inversión necesaria para disponer de dichos servicios.