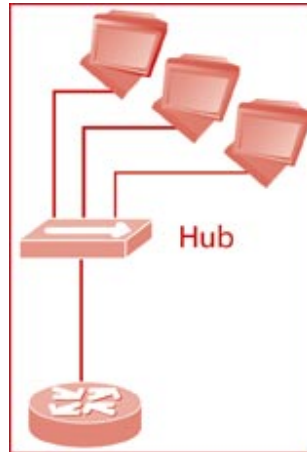


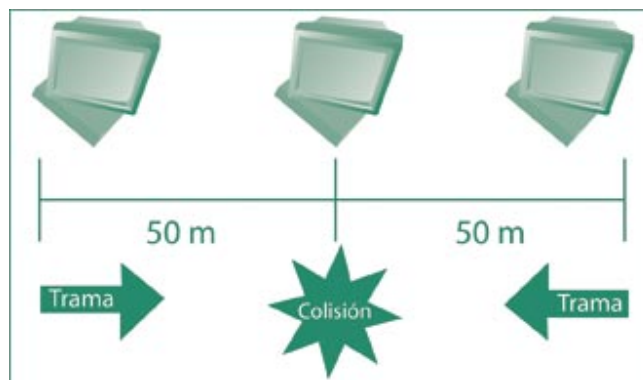
VLANs

La característica principal de una red de área local es que los dispositivos que la conforman comparten los recursos del medio físico, es decir, el ancho de banda proporcionado por el mismo. Cuando utilizamos un concentrador o hub dentro de una red, ésta se puede ver como una red de distribución hidráulica, donde las estaciones de trabajo conectadas a la misma toman cierta cantidad de agua, y mientras más máquinas existan en esa LAN, menor será la cantidad de líquido que podrán utilizar. A este segmento de “tubería” se le puede llamar también “dominio de colisiones”.



El empleo de un switch mejora el rendimiento de la red debido a que este dispositivo segmenta o divide los “dominios de colisiones”, es decir, el comportamiento que se tiene en una LAN al utilizar concentradores o hubs es el de compartir el medio o ancho de banda, por ello puede ocurrir que en algún momento el medio esté ocupado por la transmisión de información por parte de alguna de las computadoras, y si otro quiere enviar información en esa precisa hora, no lo podrá hacer hasta que el medio se encuentre disponible.

Por otro lado, si dos computadoras “escuchan” que el medio está vacío enviarán su información, pero debido a que éste es compartido puede suceder que los datos se encontrarán y “chocarán”, por lo que se hablará de una colisión y el material se destruirá; al perderse tendrá que volverse a enviar, lo que llevará a muchas retransmisiones de información.

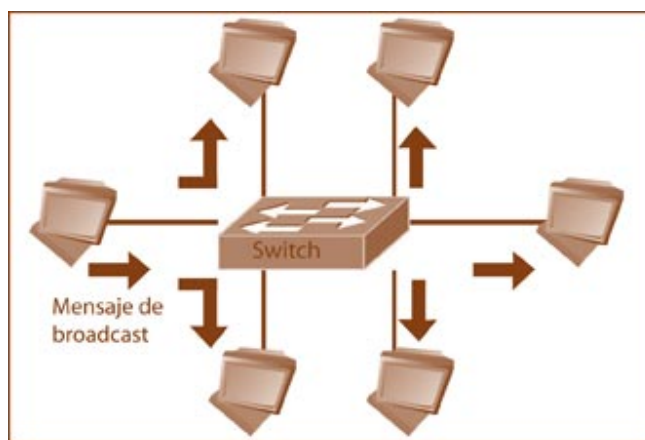


En una red LAN, cada uno de los puertos es una “tubería” dedicada a cada una de las casas (computadoras) dentro de la red, donde cada computadora dispone de toda la anchura de banda que la red proporciona, en este caso 10 o 100 Mbps, con objeto de evitar las colisiones que

pudieran existir en un medio compartido, por ello cada computadora tiene un tubo individual enlazado con el punto central de distribución que es el switch.

Algo que no puede mejorar ni el switch, ni el hub o concentrador, es el envío de mensajes de broadcast dentro de una red LAN, los que se asemejan a aquellos que escuchamos en una tienda departamental. Estos mensajes los escuchamos todos los que estamos en la tienda (la red LAN), ya sea que estén buscando a alguien o anunciando algún producto, y ninguna de las personas (computadoras) que estamos dentro de la tienda nos encontramos exentos de hacerlo.

En una LAN estos mensajes de broadcast son enviados a través de todos los puertos de un hub o de un switch. Si una computadora quiere comunicarse con otra y no sabe en dónde se encuentra, entonces la "vocea" dentro de la LAN, creando tráfico dentro de ésta, además todas las computadoras escucharán el mensaje pero sólo podrá contestarlo la que se está buscando, no importando si se encuentra o no conectada dentro del switch o concentrador.



Estos mensajes de broadcast son, en muchas ocasiones, tráfico innecesario como cuando estamos tratando de encontrar una computadora en específico, pero afectamos a todas las que estén dentro del "dominio de broadcast" o LAN.

Para solventar dicha situación se crea el concepto de Redes de Área Local Virtuales (VLANs), configuradas dentro de los switches, que dividen en diferentes "dominios de broadcast" a un switch, con la finalidad de no afectar a todos los puertos del switch dentro de un solo dominio de broadcast, sino crear dominios más pequeños y aislar los efectos que pudieran tener los mensajes de broadcast a solamente algunos puertos, y afectar a la menor cantidad de máquinas posibles.

Una Red de Área Local Virtual (VLAN) puede definirse como una serie de dispositivos conectados en red que a pesar de estar conectados en diferentes equipos de interconexión (hubs o switches), zonas geográficas distantes, diferentes pisos de un edificio e, incluso, distintos edificios, pertenecen a una misma Red de Área Local.

Con los switches, el rendimiento de la red mejora en los siguientes aspectos:

- Aísla los "dominios de colisión" por cada uno de los puertos.
- Dedicar el ancho de banda a cada uno de los puertos y, por lo tanto, a cada computadora.
- Aísla los "dominios de broadcast", en lugar de uno solo, se puede configurar el switch para que existan más "dominios".
- Proporciona seguridad, ya que si se quiere conectar a otro puerto del switch que no sea el suyo, no va a poder realizarlo, debido a que se configuraron cierta cantidad de puertos para cada VLAN.
- Controla más la administración de las direcciones IP. Por cada VLAN se recomienda asignar un bloque de IPs, independiente uno de otro, así ya no se podrá configurar por

parte del usuario cualquier dirección IP en su máquina y se evitará la repetición de direcciones IP en la LAN.

- No importa en donde nos encontremos conectados dentro del edificio de oficinas, si estamos configurados en una VLAN, nuestros compañeros de área, dirección, sistemas, administrativos, etc., estarán conectados dentro de la misma VLAN, y quienes se encuentren en otro edificio, podrán “vernors” como una Red de Área Local independiente a las demás.

El funcionamiento e implementación de las VLANs está definido por un organismo internacional llamado IEEE Computer Society y el documento en donde se detalla es el IEEE 802.1Q.

Hasta aquí ya hemos hablado de que se aísla el tráfico de colisiones y de broadcast, y que cada VLAN es independiente una de otra, pero todavía falta mencionar cómo es que se comunican entre sí, ya que muchas veces habrá que comunicarse entre computadoras pertenecientes a diferentes VLANs. Por ejemplo, los de sistemas con los de redes, o los de redes con finanzas, etcétera.

En el estándar 802.1Q se define que para llevar a cabo esta comunicación se requerirá de un dispositivo dentro de la LAN, capaz de entender los formatos de los paquetes con que están formadas las VLANs. Este dispositivo es un equipo de capa 3, mejor conocido como enrutador o router, que tendrá que ser capaz de entender los formatos de las VLANs para recibir y dirigir el tráfico hacia la VLAN correspondiente

CLASES DE VLAN

Como respuesta a los problemas generados en redes lan (colisiones, tráfico broadcast, movilidad, etc) se creo una red con agrupamientos lógicos independientes del nivel físico, con lo cual si un usuario se encontraba en el piso uno y debía moverse al piso dos ya no tenia que reconfigurar la maquina ni darle una nueva dirección IP (Internet Protocol; Protocolo de Internet) del piso dos, sino que ahora era una acción automática.

Las VLAN (Virtual Local Area Networks; Redes virtuales de área local) forman grupos lógicos para definir los dominios de broadcast. De esta forma existe el dominio de los rojos, donde el broadcast que genera el rojo solo le afectara a este color y el broadcast que genera el amarillo solamente afectara a esta parte de la red.

Aunque físicamente estén conectadas las maquinas al mismo equipo, lógicamente pertenecerán a una VLAN distinta dependiendo de sus aplicaciones con lo que se logra un esquema mas enfocado al negocio.

Anteriormente existía la red plana, donde el broadcast se repetía en los puertos y esto provocaba una situación critica. Ahora con las VLAN existe una segmentación lógica o virtual.

Existen dos clases de VLAN: implícitas y explícitas. Las implícitas no necesitan cambios en el frame, pues de la misma forma que reciben información la procesan, ejemplo de ello son las VLAN basadas en puertos. En esta clase de VLAN el usuario no modifica ni manipula el frame, ya que solo posee una marca y por lo tanto el sistema se vuelve propietario.

Las VLAN explícitas si requieren modificaciones, adiciones y cambios (MAC) al frame, por lo que sacaron los estándares 802.1p y 802.1q, en donde se colocan ciertas etiquetas o banderas en el frame para manipularlo.

Las VLAN deben ser rápidas, basadas en switches para que sean interoperables totalmente – porque los routers no dan la velocidad requerida- , su información deberá viajar a través del backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.

GENERACIONES DE VLAN

1. Basadas en puertos y direcciones MAC
2. Internet Working; se apoya en protocolo y dirección capa tres.
3. De aplicación y servicios: aquí se encuentran los grupos multicast y las VLAN definidas por el usuario.
4. Servicios avanzados: ya se cumple con los tres criterios antes de realizar alguna asignación a la VLAN; se puede efectuar por medio de DHCP (Dynamic Host Configuration Protocol ; Protocolo de configuración dinámica) o por AVLAN (Authenticate Virtual Local Area Networks; Redes virtuales autenticadas de área local).

VLAN por Puerto

Este tipo es el más sencillo ya que un grupo de puertos forma una VLAN -un puerto solo puede pertenecer a una VLAN -, el problema se presenta cuando se quieren hacer VLAN por MAC ya que la tarea es compleja. Aquí el puerto del switch pertenece a una VLAN , por tanto, si alguien posee un servidor conectado a un puerto y este pertenece a la VLAN amarilla , el servidor estará en la VLAN amarilla.

VLAN por MAC

Se basa en MAC Address, por lo que se realiza un mapeo para que el usuario pertenezca a una determinada VLAN. Obviamente dependerá de la política de creación.

Este tipo de VLAN ofrece mayores ventajas, pero es complejo porque hay que meterse con las direcciones MAC y si no se cuenta con un software que las administre, será muy laborioso configurar cada una de ellas.

VLAN por Protocolo

Lo que pertenezca a IP se enrutará a la VLAN de IP e IPX se dirigirá a la VLAN de IPX , es decir, se tendrá una VLAN por protocolo. Las ventajas que se obtienen con este tipo de VLAN radican en que dependiendo del protocolo que use cada usuario, este se conectará automáticamente a la VLAN correspondiente.

VLAN por subredes de IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de este para que el usuario aunque este conectado a la VLAN del protocolo IP sea asignado en otra VLAN subred que pertenecerá al grupo 10 o 20 dentro del protocolo.

VLAN definidas por el usuario

En esta política de VLAN se puede generar un patrón de bits, para cuando llegue el frame. Si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario protocolo, dirección MAC y puerto.

Si el usuario manifiesta otro patrón de bits, entonces se trasladará a la VLAN que le corresponda; aquí el usuario define las VLAN.

VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignará una VLAN correspondiente.

También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

VLAN por DHCP

Aquí ya no es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente. Esta política de VLAN es de las últimas generaciones.

VoIP

Descripción técnica detallada sobre Voz sobre IP (VOIP)

- Introducción
- El estandar VOIP - voz sobre IP
- Ventajas de la tecnología de voz sobre IP
- Todo sobre VOIP
- ¿Qué es H.323?
- Telefonía sobre IP: como cambiarle la cara a las telecomunicaciones

Introducción

El crecimiento y fuerte implantación de las redes IP, tanto en local como en remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, así como el estudio de nuevos estándares que permitan la calidad de servicio en redes IP, han creado un entorno donde es posible transmitir telefonía sobre IP lo que no significará en modo alguno la desaparición de las redes telefónicas modo circuito, sino que habrá, al menos temporalmente, una fase de coexistencia entre ambas, y por supuesto la necesaria interconexión mediante pasarelas (gateways), denominadas genéricamente pasarelas VoIP. Este aspecto ha sido abordado tanto por ITU como por el IETF.

Si a todo lo anterior, se le suma el fenómeno Internet, junto con el potencial ahorro económico que este tipo de tecnologías puede llevar acarreado, la conclusión es clara: VoIP (Protocolo de Voz Sobre Internet - Voice Over Internet Protocol) es un tema "caliente" y estratégico para las empresas.

El concepto original es relativamente simple: se trata de transformar la voz en "paquetes de información" manejables por una red IP (con protocolo Internet, materia que también incluye a las intranets y extranets).

Gracias a otros protocolos de comunicación, como el RSVP, es posible reservar cierto ancho de banda dentro de la red que garantice la calidad de la comunicación.

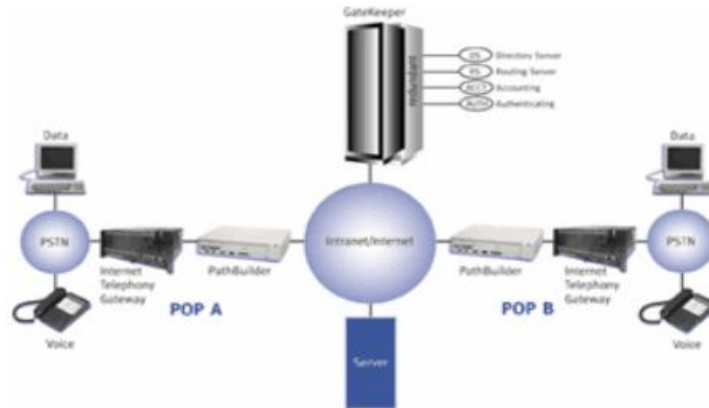
La voz puede ser obtenida desde un teléfono común: existen gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos. De hecho, el sistema telefónico podría desviar sus llamadas a Internet para que, una vez alcanzado el servidor más próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmitida hacia un teléfono común por la red telefónica tradicional. Vale decir que, se pueden mantener conversaciones teléfono a teléfono.

"Los carriers son conscientes de que el tráfico de voz hasta el año 2002 crecía apenas el 3%, mientras que el de datos estará en el orden del 30%, y las reglas del mercado indican que, cuando uno se resiste a vender un servicio, lo vende la competencia. Esto es bien sabido por los carriers." (Sergio Cusato, Marketing Manager de Nortel en el área de redes de datos para empresas)

COMO FUNCIONA LA VOZ SOBRE IP

La voz sobre IP convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales. La evolución de la transmisión conmutada por circuitos a la transmisión basada en paquetes toma el tráfico de la red pública telefónica y lo coloca en redes IP bien aprovisionadas. Las señales de voz se encapsulan en paquetes IP que pueden transportarse como IP nativo o como IP por Ethernet, Frame Relay, ATM o SONET.

Hoy, las arquitecturas interoperables de voz sobre IP se basan en la especificación H.323 v2. La especificación H.323 define gateways (interfaces de telefonía con la red) y gatekeepers (componentes de conmutación interoficina) y sugiere la manera de establecer, enrutar y terminar llamadas telefónicas a través de Internet. En la actualidad, se están proponiendo otras especificaciones en los consorcios industriales tales como SIP, SGCP e IPDC, las cuales ofrecen ampliaciones en lo que respecta al control de llamadas y señalización dentro de arquitecturas de voz sobre IP.



El estándar VoIP - Voz sobre IP

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

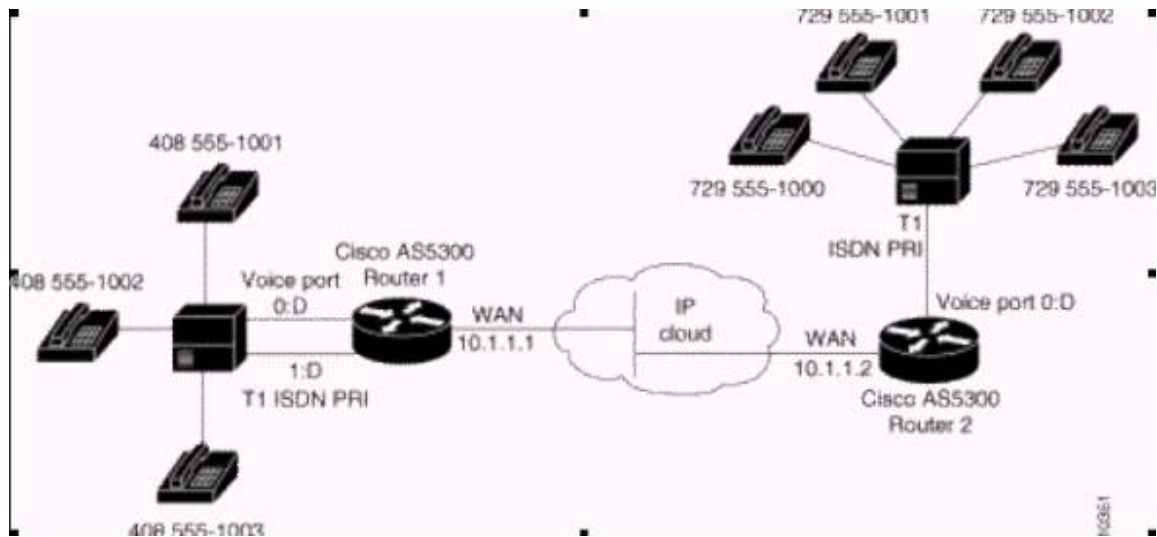


Fig. 1 Ejemplo de red con conexión de centralitas a routers CISCO que disponen de soporte VoIP.

Es innegable la implantación definitiva del protocolo IP desde los ámbitos empresariales a los domésticos y la aparición de un estándar, el VoIP, no podía hacerse esperar. La aparición del VoIP junto con el abaratamiento de los DSP's (Procesador Digital de Señal), los cuales son claves en la

compresión y descompresión de la voz, son los elementos que han hecho posible el despegue de estas tecnologías.

Para este auge existen otros factores, tales como la aparición de nuevas aplicaciones o la apuesta definitiva por VoIP de fabricantes como CISCO Systems, NORTEL-Bay Networks, ALCATEL, HUAWEI, ERICSSON, SIEMENS, NOKIA, NEC, etc. Por otro lado los operadores de telefonía están ofreciendo o piensan ofrecer en un futuro cercano, servicios IP de calidad a las empresas.

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

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

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

El VoIP/H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación:

- Direccionamiento:
 1. RAS (Registration, Admission and Status). Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través de el Gatekeeper.
 2. DNS (Domain Name Service). Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.
- Señalización:
 1. Q.931 Señalización inicial de llamada.
 2. H.225 Control de llamada: señalización, registro y admisión, y paquetización / sincronización del stream (flujo) de voz.
 3. H.245 Protocolo de control para especificar mensajes de apertura y cierre de canales para streams de voz.
- Compresión de Voz:
 1. Requeridos: G.711 y G.723.
 2. Opcionales: G.728, G.729 y G.722.
- Transmisión de Voz:
 1. UDP. La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
 2. RTP (Real Time Protocol). Maneja los aspectos relativos a la temporización, marcando los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción.

Control de la Transmisión:

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

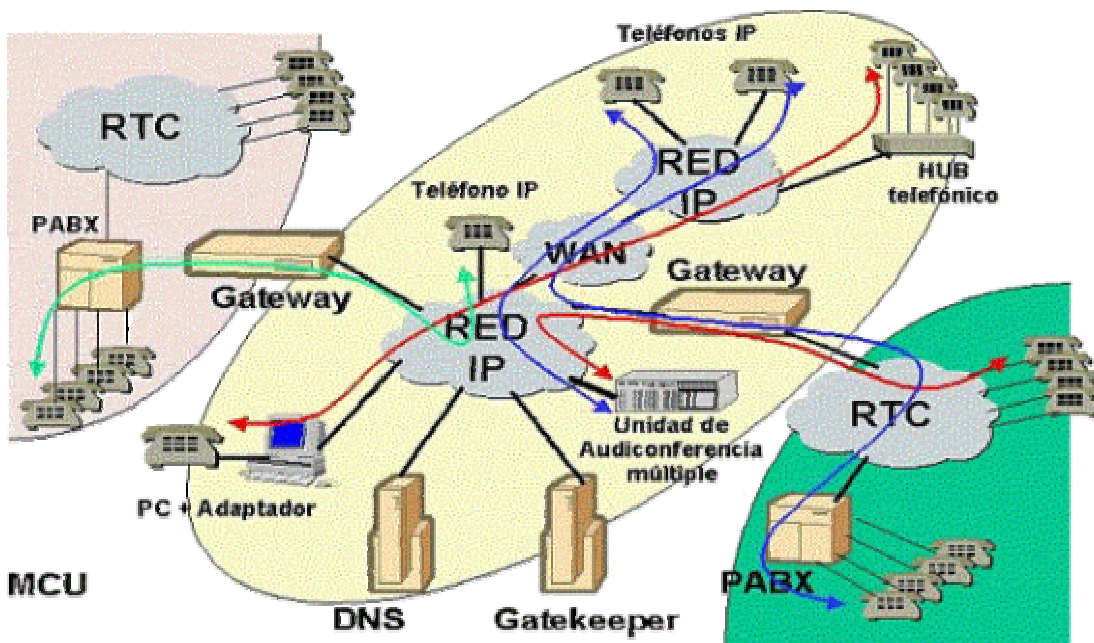
Establecimiento de llamada y Control					
Presentación					
Direccionamiento		Compresión de audio G.711 ó G.723		DTMF	
RAS(H.225)	DNS	RTP/RTCP		H.245	Q.931 (H.225)
Transporte UDP			Transporte TCP		
Red (IP)					
Enlace					
Físico					

Tabla 1. Pila de protocolos en VoIP

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

- Teléfonos IP.
- Adaptadores para PC.
- Hubs Telefónicos.
- Gateways (pasarelas RTC / IP).
- Gatekeeper.
- Unidades de audioconferencia múltiple (MCU Voz).
- Servicios de Directorio.

Fig. 2 Elementos de una red VoIP



Las funciones de los distintos elementos son fácilmente entendibles a la vista de la figura 2, si bien merece la pena recalcar algunas ideas.

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

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

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

Los distintos elementos pueden residir en plataformas físicas separada, o nos podemos encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos Gatekeeper y Gateway. También podemos ver en la figura 1 cómo Cisco ha implementado las funciones de Gateway en el router.

Gateway de Voz sobre IP

El término pasarela de VoIP en ocasiones también se suele utilizar para hacer referencia a otros elementos funcionales, en tal caso se le suelen llamar pasarelas de VoIP especiales, en tanto que se posicionan entre redes IP para desarrollar determinadas funciones de mapping, por ejemplo en la capa IP. Entidades específicas como proxies VoIP, transcodificadores VoIP, traductores de direcciones de red VoIP, etc., caen en esta categoría de pasarelas de VoIP.

Las pasarelas de interconexión en este contexto son básicamente dispositivos lógicos, aunque también pueden ser, y de hecho son, dispositivos físicos, como se verá posteriormente. Tienen una serie de atributos que caracterizan el volumen y tipos de servicios que pueden proveer, por ejemplo:

- Capacidad, expresa el volumen de servicio que puede brindar la pasarela, estando relacionado directamente con el número de puertos que tiene (igual al número máximo de llamadas simultáneas) y la velocidad del enlace de acceso.
- Protocolos de señalización soportados, tanto relativos a redes de VoIP como relativos a redes SCN.
- Codecs de voz utilizados.
- Algoritmos de encriptado que soporta.
- Rango de direccionado, que es el rango o abanico de números telefónicos que a su través se tiene acceso en la GSTN desde la red IP. En relación con la tarificación, este rango de direccionado puede o no estar fraccionado. En general, las pasarelas de interconexión tienen que proporcionar los siguientes “mecanismos” o funciones:
 - Adaptación de señalización, básicamente tiene que ver con las funciones de establecimiento y terminación de las llamadas,
 - Control de los medios, se relaciona con la identificación, procesamiento e interpretación de eventos relacionados con el servicio generados por usuarios o terminales,
 - Adaptación de medios, según requerimientos de las redes.

La pasarela o gateway de interconexión también desarrolla la función control de medios, que se ocupa de “manejar” toda la información de control generada por el terminal. Para el caso de comunicaciones de voz, la información de control del nivel de usuario más a destacar son los tonos multifrecuencia (DTMF) que produce un teclado telefónico convencional (por ejemplo, para interactuar con un servidor de voz). Ahora bien, dadas las características de estas señales, en el sentido que están en el rango audible pero no son señales de voz, sino tonos, es necesario prestar particular atención para su trasvase por la conexión híbrida que representa la pasarela de

interconexión. Las técnicas de compresión de voz de baja velocidad introducen considerable distorsión en los tonos DTMF, provocando la recepción y correspondiente decodificación incorrecta en los receptores. Entonces, esto requiere que las señales de audio y los tonos DTMF sean separados en la pasarela (si no lo ha sido ya en el emisor) y conducidas de forma independiente al receptor.

- Hay dos posibles soluciones para el transporte de los tonos DTMF:
Transporte “dentro de banda”: consiste en transportar estos tonos, digitalizados y paquetizados, con los protocolos RTP/UDP, mediante un formato de carga útil dedicado.
- Transporte “fuera de banda”: conlleva a utilizar un canal de control de medios seguro (no UDP, sino TCP) para el transporte de las señales TDMF.

El transporte de los tonos DTMF “dentro de banda” se ve afectado por la falta de garantía en la entrega de paquetes que el protocolo UDP ofrece, con nefastas consecuencias para el funcionamiento del servicio en caso de pérdida de un paquete asociado a un tono TDMF. Tiene la ventaja de que los tonos permanecen sincronizados en el tiempo con respecto a la voz.

En cambio, el transporte “fuera de banda” si bien gana en seguridad respecto a la entrega segura de los paquetes, pierden las señales su referencia exacta en el tiempo en relación con el stream de voz. Esta es precisamente la solución adoptada en la Recomendación H.323, mediante el canal H.245.

Ventajas de la tecnología de voz sobre IP

- Integración sobre su Intranet de la voz como un servicio más de su red, tal como otros servicios informáticos.
- Las redes IP son la red estándar universal para la Internet, Intranets y extranets.
- Estándares efectivos (H.323).
- Interoperabilidad de diversos proveedores.
- Uso de las redes de datos existentes.
- Independencia de tecnologías de transporte (capa 2), asegurando la inversión.
- Menores costos que tecnologías alternativas (voz sobre TDM, ATM, Frame Relay).

Todo sobre VoIP

Las redes de voz y datos son esencialmente diferentes. Las redes de voz y fax, que emplean conmutación de circuitos, se caracterizan por:

- Para iniciar la conexión es preciso realizar el establecimiento de llamada.
- Se reservan recursos de la red durante todo el tiempo que dura la conexión.
- Se utiliza un ancho de banda fijo (típicamente 64 Kbps por canal de voz) que puede ser consumido o no en función del tráfico.
- Los precios generalmente se basan en el tiempo de uso.
- Los proveedores están sujetos a las normas del sector y regulados y controlados por las autoridades pertinentes (en nuestro caso, el Ministerio de Fomento y la Comisión del Mercado de las Telecomunicaciones).
- El servicio debe ser universal para todo el ámbito estatal.
- Por el contrario, las redes de datos, basadas en la conmutación de paquetes, se identifican por las siguientes características:
- Para asegurar la entrega de los datos se requiere el direccionamiento por paquetes, sin que sea necesario el establecimiento de llamada .
- El consumo de los recursos de red se realiza en función de las necesidades, sin que, por lo general, sean reservados siguiendo un criterio de extremo a extremo.
- Los precios se forman exclusivamente en función de la tensión competitiva de la oferta y la demanda.

- Los servicios se prestan de acuerdo a los criterios impuestos por la demanda, variando ampliamente en cuanto a cobertura geográfica, velocidad de la tecnología aplicada y condiciones de prestación.
- Implementar una red convergente supone estudiar las diferencias existentes entre las características de las redes de voz y de datos, comprendiendo los problemas técnicos que implican dichas diferencias sin perder de vista en ningún momento la perspectiva del usuario final.

2. Las diferencias entre la operación de las redes de voz y datos requieren distintos enfoques de gestión.

Tradicionalmente, la industria de la telefonía trabaja con unas altas exigencias de fiabilidad, conocidas como los "cinco nueves": 99,999 por ciento. Esto se traduce en unos objetivos de diseño de centrales públicas de conmutación que garantizan niveles de caída del servicio de sólo dos horas cada cuarenta años de operación. Cuarenta años suponen aproximadamente 350.400 horas; y dos horas sin servicio representaría sólo un 0,0000057 de todo ese tiempo. O lo que es lo mismo, una disponibilidad del 99,9994 por ciento.

3. Factores de Calidad de Servicio (QoS). La entrega de señales de voz, vídeo y fax desde un punto a otro no se puede considerar realizada con un éxito total a menos que la calidad de las señales transmitidas satisfaga al receptor. Entre los factores que afectan a la calidad se encuentran los siguientes:

- Requerimientos de ancho de banda: la velocidad de transmisión de la infraestructura de red y su topología física.
- Funciones de control: incluye la reserva de recursos, provisión y monitorización requeridos para establecer y mantener la conexión multimedia.
- Latencia o retardo: de la fuente al destino de la señal a través de la red.
- Jitter: variación en los tiempos de llegada entre los paquetes. Para minimizar este factor los paquetes entrantes han de ser introducidos en un buffer y, desde allí, enviados a intervalos estándar.
- Pérdida de paquetes: cuando un paquete de vídeo o de voz se pierde en la red es preciso disponer de algún tipo de compensación de la señal en el extremo receptor.

Requerimientos de una red para soportar VoIP

A continuación se mencionan aspectos importantes que se deben tener en la red IP para implantar este servicio en tiempo real

- Manejar peticiones RSVP que es un protocolo de reservación de recursos.
- El costo de servicio debe estar basado en el enrutamiento para las redes IP.
- Donde se conecta con la red pública conmutada un interruptor de telefonía IP debe soportar el protocolo del Sistema de Señalización 7 (SS7). SS7 se usa eficazmente para fijar llamadas inalámbricas y con línea en la PSTN y para acceder a los servidores de bases de datos de la PSTN. El apoyo de SS7 en interruptores de telefonía IP representa un paso importante en la integración de las PSTN y las redes de datos IP.
- Se debe trabajar con un comprensivo grupo de estándares de telefonía (SS7, Recomendación H.323, SIP) para que los ambientes de telefonía IP y PBX/PSTN/ATM vídeo y Gateway telefónica puedan operar en conjunto en todas sus características

Calidad de Servicio QoS

Esta función tiene primordial importancia en relación con la QoS experimentada por el usuario final.

En esto influyen dos factores fundamentales:

- La calidad de la voz extremo a extremo, determinada por los sucesivos procesos de codificación – decodificación, y las pérdidas de paquetes en la red.
- La demora extremo a extremo, debido a las sucesivos procesos de codificación – decodificación, paquetización y “encolados”. Afecta la interactividad en la conversación, y por tanto a la QoS.
- Las redes IP son redes del tipo best-effort y por tanto no ofrecen garantía de QoS, pero las aplicaciones de telefonía IP si necesitan algún tipo de garantía de QoS en términos de demora, jitter y pérdida de paquetes. En tal sentido existen dos mecanismos de señalización para QoS , esto es, IntServ y DiffServ. Ambos son “mecanismos” de cara a la red.

Por tanto, es necesario buscar QoS no solo en la red, sino también en los terminales, y en los procesos que en los mismos se desarrollan, de ahí que sea necesario también decir que la sensibilidad a la pérdida de paquetes, a las demoras y sus fluctuaciones, que experimentan los servicios de voz sobre IP, dependen en buena medida de los mecanismos implementados en los terminales

La preparación de los medios en los terminales para ser enviados y transferidos por la red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica demora de procesamiento y demora de empaquetado:

- Demora de procesamiento: demora producida por la ejecución del algoritmo de codificación, que entrega un stream de bytes listos para ser empaquetados.
- Demora de paquetización: es el tiempo que se requiere para formar un paquete de voz a partir de los bytes codificados.

Debe señalarse que el resultado de esta codificación – paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que posibilita de cara a la red poder manejar más conexiones simultáneas, pero se incrementa la demora y la distorsión de la señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

Otro aspecto a tener en cuenta es el compromiso entre la demora de paquetización y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor demora de paquetización para cierto estándar de codificación. Claro está, según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50 %, con un crecimiento de la demora en forma exponencial en el caso de los codecs de baja velocidad como el G.723.1. La demora de paquetización también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP.

A las demoras de procesamiento y empaquetado se suma también la demora que introduce el proceso de buffering en los terminales, y la demora de “encolado” en la red. Todo esto da una demora extremo a extremo que percibe el usuario final en mayor o menor medida. Demoras extremo a extremo por debajo de 400 milisegundos no comprometen la interactividad en la conversación, pero ya por encima de 150 milisegundos se requiere control del eco.

Las demoras antes comentadas son resultado lógico de las características y modo de operación de las redes IP, así como también de la naturaleza de las señales de voz.

¿Qué es H.323?

El H.323 es una familia de estándares definidos por el ITU para las comunicaciones multimedia sobre redes LAN. Está definido específicamente para tecnologías LAN que no garantizan una calidad de servicio (QoS). Algunos ejemplos son TCP/IP e IPX sobre Ethernet, Fast Ethernet o Token Ring. La tecnología de red más común en la que se están implementando H.323 es IP (Internet Protocol).

Este estándar define un amplio conjunto de características y funciones. Algunas son necesarias y otras opcionales. El H.323 define mucho más que los terminales. El estándar define los siguientes componentes más relevantes:

- Terminal.
- GateWay.
- Gatekeeper.
- Unidad de Control Multipunto.

El H.323 utiliza los mismos algoritmos de compresión para el vídeo y el audio que la norma H.320, aunque introduce algunos nuevos. Se utiliza T.120 para la colaboración de datos.

El H.323 en perspectiva histórica.

Anteriormente al H.323, el ITU se enfocó exclusivamente en la estandarización de las redes globales de telecomunicaciones. Por ejemplo, en 1985 se comenzó el trabajo en la especificación que define el envío de imagen y voz sobre redes de circuitos conmutados, tales como RDSI. La ratificación de la norma (H.320) tuvo lugar 5 años después (fue aprobada por el CCITT en Diciembre de 1990). Sólo 3 años después se dispuso de equipos que cumplieran con la norma y que permitieran la inter-operabilidad entre sí.

En Enero de 1996, un grupo de fabricantes de soluciones de redes y de ordenadores propuso la creación de un nuevo estándar ITU-T para incorporar videoconferencia en la LAN. Inicialmente, las investigaciones se centraron en las redes de área local, pues éstas son más fáciles de controlar. Sin embargo, con la expansión de Internet, el grupo hubo de contemplar todas las redes IP dentro de una única recomendación, lo cual marcó el inicio del H.323.

El H.323 soporta vídeo en tiempo real, audio y datos sobre redes de área local, metropolitana, regional o de área extensa. Soporta así mismo Internet e intranets. En Mayo de 1997, el Grupo 15 del ITU redefinió el H.323 como la recomendación para "los sistemas multimedia de comunicaciones en aquellas situaciones en las que el medio de transporte sea una red de conmutación de paquetes que no pueda proporcionar una calidad de servicio garantizada.

Nótese que H.323 también soporta videoconferencia sobre conexiones punto a punto, telefónicas y RDSI. En estos casos, se debe disponer un protocolo de transporte de paquetes tal como PPP.

H.323: Una extensión del H.320

El H.323 se fundamenta en las especificaciones del H.320. Muchos de los componentes del H.320 se incluyen en el H.323. A este respecto, el H.323 se puede ver como una extensión del H.320. El nuevo estándar fue diseñado específicamente con las siguientes ideas en mente:

- Basarse en los estándares existentes, incluyendo H.320, RTP y Q.931.
- Incorporar algunas de las ventajas que las redes de conmutación de paquetes ofrecen para transportar datos en tiempo real.
- Solucionar la problemática que plantea el envío de datos en tiempo real sobre redes de conmutación de paquetes.

Tabla: Ventajas de la tecnología H.323

Reducción de los costes de operación.

H.323	H.320
Se pueden utilizar los cableados de campus, las conexiones WAN basadas en routers IP y los servicios WAN para enviar vídeo. Esto es una fuente potencial de importantes ahorros de explotación. Los costes de soporte de las infraestructuras (por ejemplo SNMP) pueden combinarse.	La tecnología H.320 requiere típicamente redes separadas para el vídeo y los datos. Esto supone un doble cableado e infraestructuras de red. Este modelo incrementa el coste de implantación por sistema.

Más amplia difusión y mayor portabilidad.

H.323	H.320
Con H.323, cada puerto con soporte IP puede potencialmente soportar vídeo. Esto hace la tecnología accesible a una más amplia variedad de usuarios. Además, es más fácil mover un equipo en nuestro entorno, lo que hará que un mismo equipo pueda ser usado para más aplicaciones.	Con H.320, se debe dedicar una línea por cada localización. La mayor parte de las salas o de los ordenadores personales no podrán fácilmente soportar vídeo, lo cual limita también la accesibilidad y portabilidad de los sistemas.

Un diseño Cliente / Servidor rico en prestaciones.

H.323	H.320
El diseño del H.323 descansa fuertemente en los componentes de la red. Sus capacidades están distribuidas a través de la red. Un ejemplo es el gatekeeper. Un gatekeeper puede residir en un servidor, en un gateway o en una MCU. Se encarga de registrar los usuarios o clientes (sistemas de videoconferencia) y puede potencialmente ofrecerles un conjunto de funciones de comunicación.	Como norma, un equipo H.320 no se conecta a un servidor. Las características del sistema residen en la plataforma de videoconferencia misma. Este enfoque de comunicación orientado al terminal no soporta servicios suplementarios tales como enrutado de llamadas, transferencia o retención. Son servicios a los que estamos acostumbrados por la tecnología de la centralitas telefónicas.

¿Por qué es importante H.323?

El H.323 es la primera especificación completa bajo la cual, los productos desarrollados se pueden usar con el protocolo de transmisión más ampliamente difundido (IP). Existe tanto interés y expectación entorno al H.323 porque aparece en el momento más adecuado. Los administradores de redes tienen amplias redes ya instaladas y se sienten confortables con las aplicaciones basadas en IP, tales como el acceso a la web. Además, los ordenadores personales son cada vez más potentes y, por lo tanto, capaces de manejar datos en tiempo real tales como voz y vídeo.

Componentes H.323

Entidad

La especificación H.323 define el término genérico entidad como cualquier componente que cumpla con el estándar.

Extremo

Un extremo H.323 es un componente de la red que puede enviar y recibir llamadas. Puede generar y/o recibir secuencias de información.

Terminal

Un terminal H.323 es un extremo de la red que proporciona comunicaciones bidireccionales en tiempo real con otro terminal H.323, gateway o unidad de control multipunto (MCU). Esta comunicación consta de señales de control, indicaciones, audio, imagen en color en movimiento y /o datos entre los dos terminales. Conforme a la especificación, un terminal H.323 puede proporcionar sólo voz, voz y datos, voz y vídeo, o voz, datos y vídeo.

Gatekeeper

El gatekeeper (GK) es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de los terminales H.323, gateways y MCUs. El GK puede también ofrecer otros servicios a los terminales, gateways y MCUs, tales como gestión del ancho de banda y localización de los gateways o pasarelas.

El Gatekeeper realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de los terminales de la LAN a las correspondientes IP o IPX, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la LAN y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la LAN. El Gatekeeper proporciona todas las funciones anteriores para los terminales, Gateways y MCUs, que están registrados dentro de la denominada Zona de control H.323.

Gateway

Un gateway H.323 (GW) es un extremo que proporciona comunicaciones bidireccionales en tiempo real entre terminales H.323 en la red IP y otros terminales o gateways en una red conmutada. En general, el propósito del gateway es reflejar transparentemente las características de un extremo en la red IP a otro en una red conmutada y viceversa.

MCU (Multipoint Control Units)

La Unidad de Control Multipunto está diseñada para soportar la conferencia entre tres o más puntos, bajo el estándar H.323, llevando la negociación entre terminales para determinar las capacidades comunes para el proceso de audio y vídeo y controlar la multidifusión.

La comunicación bajo H.323 contempla las señales de audio y vídeo. La señal de audio se digitaliza y se comprime bajo uno de los algoritmos soportados, tales como el G.711 o G.723, y la señal de vídeo (opcional) se trata con la norma H.261 o H.263. Los datos (opcional) se manejan bajo el estándar T.120 que permite la compartición de aplicaciones en conferencias punto a punto y multipunto.

Bibliografía

1. BLACK, U. (1999). Voice over IP. New Jersey: Prentice Hall PTR.
2. CUERVO, F., GREENE, N., HUITEMA, C., RAYHAN, A., ROSEN, B. y SEGERS, J. (2000). Megaco Protocol versión 0.8. RFC 2885, Agosto 2000.
3. DOUSKALIS, B. (2000). IP telephony: the integration of robust VoIP services. New Jersey: Prentice Hall PTR
4. GREENE, N., RAMALHO, M. y ROSEN, B. (2000). Media Gateways Control Protocol Architecture and Requirements. RFC 2805, Abril 2000.
5. HAMDJ, M., VERSCHEURE, O., HUBAUX, J-P., DALGIC, I. y WANG, P. (Mayo, 1999).Voice Service Interworking for PSTN and IP Networks. IEEE Communication Magazine, Mayo 1999, pags. 104-111.
6. HERSENT,O., GURLE, D. y PETIT, J.P. (2000). IP telephony: packet – based multimedia communication systems. Great Britain: Addison – Wesley.
7. ITU-T Study Group 16 (1998). Recommendation H.246. Enero 1998.
8. ITU-T Study Group 16 (2000). Recommendation H.323v4 (draft). Noviembre 2000.

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

10. www.voip-forum.com/

Breve glosario de acrónimos y términos VoIP

Acrónimos

ATM Asynchronous Transfer Mode (Modo de Transferencia Asíncrona)

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

CPE Customer Premises Equipment (Equipo en Instalaciones de Cliente)

CTI Computer Telephony Integration (Integración Ordenador- Telefonía)

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

DNS Domain Name System (Sistema de Nombres de Dominio)

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

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

FDM Frequency Division Multiplexing (Multiplexado por División de Frecuencia)

FoIP Fax over IP (Fax sobre IP)

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

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

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

IN Intelligent Network (Red Inteligente)

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

IP Internet Protocol (Protocolo Internet)

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

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

IPSec IP Security (Protocolo de Seguridad IP)

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

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

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

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

LDP Label Distribution Protocol (Protocolo de Distribución de Etiquetas)

LSR Label Switching Router (Encaminador de Conmutación de Etiquetas)

MBONE Multicast Backbone (Red Troncal de Multifusión)

MCU Multipoint Control Unit (Unidad de Control Multipunto)

MEGACO Media Gateway Control (Control de Pasarela de Medios)

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

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

MPLS Multiprotocol Label Switching (Conmutación de Etiquetas Multiprotocolo)

OLR Overall Loudness Rating (Índice de Sonoridad Global)

PBX Private Branch Exchange (Centralita Telefónica Privada)

PHB Per Hop Behaviour (Comportamiento por Salto)

PoP Point of Presence (Punto de Presencia)

POTS Plain Old Telephone Service (Servicio Telefónico Tradicional)

PPP Point to Point Protocol (Protocolo Punto a Punto)

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

QoS Quality of Service (Calidad de Servicio)

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

RSVP Reservation Protocol (Protocolo de Reserva)

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

RTP Real Time Protocol (Protocolo de Tiempo Real)

SAP Session Annunciation Protocol (Protocolo de Anuncio de Sesión)

SCN Switched Circuit Network (Red de Circuitos Conmutados)

SDP Session Description Protocol (Protocolo de Descripción de Sesión)

SIP Session Initiation Protocol (Protocolo de Inicio de Sesión)

SLA Service Level Agreement (Acuerdo de Nivel de Servicio)

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

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

TCP Transmission Control Protocol (Protocolo de Control de Transmisión)

TDM Time Division Multiplexing (Multiplexado por División de Tiempo)

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

UDP User Datagram Protocol (Protocolo de Datagramas de Usuario)

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

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

VPN Virtual Private Network (Red Privada Virtual)

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

Términos

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

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

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

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

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

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

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

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

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

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

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

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