UNIVERSIDAD AUSTRAL DE CHILE
FACULTAD DE CIENCIAS DE LA INGENIERÍA
ESCUELA DE ELECTRICIDAD Y ELECTRÓNICA

ANALISIS Y EVALUACIÓN DE PARAMETROS PARA UNA ÓPTIMA CALIDAD DE SERVICIO EN TELEFONÍA IP

Trabajo de Titulación para optar al
Titulo de Ingeniero en Electrónica

PROFESOR PATROCINANTE:
Sr. Néstor Fierro Monreud

CRISTIAN EDUARDO DELGADO PEREIRA

VALDIVIA 2006

COMISIÓN REVISORA

Profesor Patrocinante:

SR. NÉSTOR FIERRO M. _____

Profesores Informantes:

SR. PEDRO REY C. _____

SR. RAÚL URRA R. _____

FECHA DE EXAMEN DE GRADO:

Dedicada a toda mi familia.
En particular a mis padres adorados.
Y para todos aquellos que creyeron en mí.

AGRADECIMIENTOS

En primer lugar debo dar las gracias a Dios por darme la salud y la vida, para poder lograr finiquitar orgullosamente una etapa más de mi vida.

También quisiera expresar mi más sincera gratitud a mi familia, en especial a mis adorados Padres: Raúl y Margoth, por sus valiosos consejos, invalorable esfuerzo, apoyo, comprensión y cariño, instruyéndome en el camino del bien y superación profesional.

Gracias a todo el Cuerpo Docente, por ampliar mis conocimientos y por la experiencia adquirida, siendo fundamentales en mi desarrollo como profesional. Y en particular a los profesores que son miembros de esta comisión de titulación por las valiosas sugerencias y correcciones realizadas.

Quiero agradecer también a todos mis compañeros y amigos que me brindaron su apoyo incondicional durante la carrera y a aquellos que colaboraron con migo en este trabajo realizado.

ÍNDICE

RESUMEN

El fuerte crecimiento e implantación de la red IP, tanto en lo local como en lo remoto, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real y nuevos estándares, han creado un entorno donde es posible transmitir Telefonía sobre IP.

Como se necesita algún tipo de garantía de la calidad del servicio en Telefonía IP, el presente trabajo de titulación está basado en el análisis y evaluación de cada uno de los factores que influyen en la degradación de la voz, de manera tal de evidenciar las soluciones que permiten optimizar y evitar y/o responder de manera adecuada, para así proveer niveles óptimos de calidad de extremo a extremo en redes IP.

Para comenzar a interiorizar este tema es necesario tener en cuenta cuales son los requerimientos de Telefonía IP. Para ello se describen y analizan los protocolos, como estándares que sustentan a la red IP, que hacen posible el tráfico de voz. Con esta información como antecedente, se estudia en detalle los elementos que proporcionan la base sólida del funcionamiento, de acuerdo a las diversas necesidades y situaciones que se puedan presentar.

De igual forma, como parte de esta investigación, se detallan los Servicios que es capaz de desarrollar una red de Telefonía IP además de la simple conectividad entre usuarios, de manera tal de proporcionar las limitaciones, tendencias y ventajas económicas que se puedan obtener, en comparación a otras alternativas, como lo es la red de telefonía pública tradicional.

Por último y no menos importante, se hace necesario considerar las implicaciones regulatorias de la Telefonía IP, asunto considerado de gran relevancia e impacto de cara al desarrollo del sector de las comunicaciones, siendo abordando este tema de manera global.

SUMMARY

The strong development and implantation of the network IP, as much in the premises as in the remote thing, the development of advanced techniques of voice digitalization, control mechanisms and prioritization of traffic, protocols of transmission in real time and new standards, they have created an surroundings where it is possible to transmit Telephony on IP.

As it needs any type of guarantee in the quality of service in Telephony IP, the present work of degree is based on the analysis and evaluation of each one of factors which they influence in the degradation of the voice, so it demonstrates solutions that allow to optimize and to avoid and/or to respond of adapted way, thus to provide optimal levels with quality of end to end in networks IP.

In order to begin to internalize this subject it is necessary to consider what are the requirements of Telephony IP. For it the protocols are described and analyzed like standards that they sustain to network IP, which they make possible the traffic of voice. With this information like antecedent, one studies in detail the elements that an solid base of the operation, according to the diverse necessities and situations that can be presented.

Similarly like part of this investigation, the service that is able to develop a network of telephony IP in additions to the simple connectivity between users, so it provides the limitations, tendencies and economic advantages that can be obtained, in comparison to other alternatives are detailed, as it is it the network of traditional public telephony.

Finally and not less important it is necessary to consider the regulatory implications of Telephony IP, considered subject of great relevance and impact facing the development of the sector of the communications, approaching this subject of global way.

1. CAPITULO I. INTRODUCCIÓN.

Desde hace algún tiempo la expansión de Internet, y la diseminación de las redes IP en todo el mundo, los esquemas de etiquetado IP y las prestaciones hardware de conmutadores y routers han demostrado efectividad para transportar 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, siendo 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: "la telefonía IP" empieza a ver su hora más gloriosa, siendo el fruto más legitimo de la convergencia tecnológica. Siendo un tema 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 voz.

La voz puede ser obtenida desde un micrófono conectado a la placa de sonido del PC, o bien 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 mas próximo al destino, esa llamada vuelva a ser traducida como información analógica y sea transmita hacia un teléfono común por la red telefónica tradicional. Vale decir, se pueden mantener conversaciones teléfono a teléfono.

Ciertamente, existen objeciones de importancia, que tienen que ver con la calidad del sistema y con el uptime (tiempo entre fallas) de las redes de datos en comparación con las de telefonía. Sin embargo, la versatibilidad y los costos del nuevo sistema hacen que los operadores de telecomunicaciones estén considerando la posibilidad de dar servicios sobre IP y, de hecho (aunque todavía aun el marco regulatorio no lo permite en forma masiva, y a pesar que difícilmente lo admitan), algunos ya están insertos en el mercado con esta tecnología.

Todo el mundo ya conoce las ventajas potenciales que brinda la telefonía IP, pero como adoptar y desplegar esta nueva alternativa sigue siendo una incógnita para muchos usuarios. A continuación se mencionaran algunas cuestiones a tener en cuenta si desea adentrarse en el mundo de las redes convergentes.

El argumento inicial a favor de este nuevo modelo de redes se basa en la gran presencia actual de las infraestructuras IP en los entornos corporativos de datos, así como en la suposición de que parte de la capacidad de estas redes esta siendo desaprovechada. Dando por sentado éste último extremo, parece que nada hay mejor que emplear el ancho de banda inutilizado para soportar el tráfico de voz y fax. De esta manera no solo aumentaría la eficiencia global de la red, sino también las sinergias entre su diseño, despliegue y gestión.

Este primer acercamiento al tema viene avalado por las conclusiones de diferentes investigaciones de mercado que coinciden en destacar el enorme potencial de crecimiento de la Telefonía sobre IP. De hecho, hacia el 2010 se estima que un 35 por ciento de las llamadas telefónicas en todo el mundo será efectuado sobre redes basadas en IP. Independiente de esta previsión tan optimista debemos estudiar y analizar esta tecnología para conocer sus ventajas e inconvenientes:

a. **La convergencia plantea un serio reto:** 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 país, la Subtel)
    - El servicio debe ser universal para todo el ámbito estatal.

Por el contrario, las redes de datos basadas en la conmutaron 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 la 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 condición 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.

b. **Factores de Calidad de Servicio (QoS).** La entrega de señales de voz, video 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 (bandwidth): 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 (delay): de la fuente al destino de la señal a través de la red.
    - Jitter: variación en los tiempos de llegada entre los paquetes.
    - Perdidas de paquetes: cuando un paquete de video o de voz se pierde en la red es preciso disponer de algún tipo de compensación de la señal en el extremo receptor.

c. **Implementación de nuevos estándares.** Los estándares vienen a ser el anteproyecto necesario para diseñar, implementar y gestionar las comunicaciones de voz y datos. En su desarrollo trabajan diferentes entidades reconocidas como organizaciones de estándares internacionales, entre los que se encuentran ANSI (American National Standards Institute), IEEE (Institute of Electrical and Electronics Engineers), ISO (Internacional Organization for Standardization), ITU (International Telecommunication Union) e IETF (Internet Engineering Task Force).

d. **Interoperatividad multifabricante.** Volviendo al pasado, se recuerda cuando era corriente que una tarjeta Ethernet de un fabricante no comunicara con otra similar de un fabricante distinto. En la actualidad este problema ya no existe, pero conviene no olvidarlo porque la

redes convergentes suponen un nuevo concepto que solo acaba de arrancar. Afortunadamente, la industria, dirigida por el International Multimedia Teleconferencing Consortium (IMTC), ha avanzando mucho en esta área crítica. Inicialmente se adoptó H.323, como norma para asegurar la interoperatividad entre los equipos, sin embargo, en la actualidad el candidato ideal para el desarrollo de los servicios convergentes, es SIP, el cual aporta un marco estable para la construcción de interoperatividad entre dispositivos, aplicaciones y otros elementos del mundo de la telefonía IP.

En muy poco tiempo, el interés por la telefonía IP esta yendo mas allá de la simples llamadas gratuitas de voz y fax por Internet para extender su influencia a cómo las comunicaciones de empresa darán servicio a los usuarios finales en el próximo milenio, y a las potenciales economías de escala que promete.

Como muestra se puede ver que compañías como Cisco, la han incorporado a su catalogo de productos, los teléfonos IP ya están disponibles y los principales operadores mundiales, están promoviendo activamente el servicio IP a las empresas, ofreciendo calidad de voz a través del mismo. Por otro lado tenemos ya estándares que nos garantizan interoperabilidad entre los distintos fabricantes. Conllevando a despertar el interés en la sociedad.

El presente trabajo está orientado, al análisis de esta tecnología respecto a la Calidad de Servicio (QoS) ofrecida, como así también, conocer los Servicios a los que se puede acceder desde una PC especialmente equipada, un equipo telefónico común, y/o un teléfono IP.

Durante el desarrollo de está investigación se verán muchos conceptos relacionados para hablar del tema de voz transmitida sobre redes de conmutación de paquetes, por lo que es preciso definir de una forma simple y clara la situación actual para que a partir de este momento se puedan identificar claramente tanto los términos como los elementos que de alguna u otra forma intervienen en los distintos niveles del desarrollo de la convergencia de redes. Términos que posiblemente identifican el camino hacia los servicios de VoIP:

- **Telefonía:** servicios de telecomunicación prestados sobre la Red Telefónica Conmutada (RTC) o PSTN (Public Switched Telephone Network), comprendiendo tres tipos de redes: Red Telefónica Básica (RTB), la Red Digital de Servicios Integrados (RDSI) y la red GSM (Global System for Mobile communications).

- **Voz en Internet:** servicios de telefonía prestados sobre la red pública global formada por la interconexión de redes de conmutación de paquetes basadas en IP.
- **Voz sobre IP (VoIP):** servicios de telefonía prestados sobre redes IP "privadas" sin interconexión a la RTC.
- **Telefonía IP (ToIP):** servicios de telefonía prestados sobre Redes IP "privadas" en interconexión con la RTC.
- **Voz sobre Frame Relay (VoFR):** servicios de telefonía prestados sobre redes soportadas por circuitos Frame Relay, orientados a la transmisión de datos.
- **Voz sobre ATM (VoATM):** servicios de telefonía prestados sobre redes ATM donde existe posibilidad de ofrecer una calidad de servicio (QoS).
- **Multimedia sobre IP (MoIP):** servicios multimedia (vídeo, audio, imagen, etc.) prestados sobre redes IP.
- **Fax sobre IP (FoIP):** servicios de transmisión de fax prestados sobre redes IP.

La Voz sobre IP es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos, como se la conoce en Internet con MSN Hotmail, MSN Yahoo y similares.

La "**Telefonía IP"** es una aplicación inmediata de esta tecnología, de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación: voz, fax, aplicaciones de mensajes de voz, etc., que son transportadas vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

Por lo tanto la conclusión es clara: la telefonía IP es mucho más que Voz sobre IP (VoIP, Voice over IP); es integrar servicios que tradicionalmente se ofrecían en PBX con la ubicuidad de Internet (o redes IP) y la cantidad de servicios posibles, convergentes y, en cierta manera, revolucionarios.

2. CAPITULO II. RED IP.

En este segundo capítulo, se realizó un estudio profundo de los protocolos básicos que permiten el funcionamiento globalizado de las redes IP.

Como esta tecnología, puede parecer un poco confusa y abrumadora, inicialmente se presentan los componentes de red subyacentes sobre los que está construida esta tecnología.

Posteriormente se hace referencia a la familia de protocolos TCP/IP, que es considerada como la piedra angular sobre la que se sustentan los servicios que actualmente podemos encontrar en Internet, y por tanto su estudio es parte fundamental para el resto del trabajo. Se introducirá el sistema de direccionamiento, el formato utilizado en sus cabeceras y el modo de funcionamiento de los protocolos más importantes de esta familia.

2.1. INTRODUCCIÓN.

La moderna tecnología digital permite que diferentes sectores, como por ejemplo: telecomunicaciones, datos, radio y televisión se fusionen en uno solo. Esta circunstancia, conocida comúnmente como convergencia, está ocurriendo a escala global y está cambiando drásticamente la forma en que se comunican tanto las personas como los dispositivos. En el centro de este proceso, formando la red troncal y haciendo posible la convergencia, están las redes IP.

La Red IP es una red estándar universal para la Internet, intranet y extranet, creada específicamente para soportar los Servicios IP. Ha sido desplegada por la TTD (Telefónica Transmisión de Datos) y entre otras cosas, permitiendo que las empresas puedan utilizar protocolos comunes para sus comunicaciones internas y externas con sus clientes y sus proveedores, sobre una red única.

Para posibilitar la comunicación entre este tipo de redes es necesario un conjunto de reglas formales para su interacción. A estas reglas se les denominan protocolos, donde el más destacado es TCP/IP.

TCP/IP es la base de la operación de Internet. Define las reglas por seguir de cada equipo conectado a la red de redes en materia de envío, transporte, presentación y empaquetado de los datos. Este estándar fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en el ARPANET una red de área extensa del departamento de defensa.

2.2. INTRODUCCIÓN A REDES.

2.2.1. Antecedentes.

Para poder definir una red, es conveniente fijar los términos correspondientes a ETD, ECD o ETCD. En general, se define ETD como un Equipo Terminal de Datos capaz generar y/o procesar información y transmitirla y/o recibirla a través de los circuitos de control que cumplen el rol de controlador de comunicaciones, pudiendo ser internos o externos en la unidad de procesamiento. ETCD consiste en un Equipo de Terminación de Circuito de Datos, cuya función es de actuar como interfaz entre el controlador de comunicaciones y el medio físico que actuara como enlace. En una terminología anterior, se le denominaba ECD, Equipo de Comunicación de Datos.

2.2.2. Definición de red.

Una red de telecomunicaciones es un conjunto de medios instalados, organizados, operados y administrados con la finalidad de brindar servicios de comunicación a distancia. En particular, se dice que una red de computadoras es una red de telecomunicaciones de datos que enlaza a dos o más ETD.

Para estudiar las redes, se pueden hacer distintos enfoques, según las características que se analizan, y cada una de estas da a lugar a una o varios tipos de red específicos.

2.2.3. Categorías.

Estas se evidenciarán deda la siguiente estructura:

- De acuerdo a su localización;
- En base a su relación funcional;
- Debido a su carácter;
- Según la topología de red;
- Disponibilidad;
- Tecnología de transmisión; y
- Al tipo de información

2.2.3.1. De acuerdo a su localización.

2.2.3.1.1. Redes LAN.

Una red de área local (Local Area Network, LAN) es una red de comunicaciones utilizada para la interconexión de computadores personales y estaciones de trabajo, en un entorno físicamente

reducido a unos pocos kilómetros. Permitiendo a los usuarios compartir información y recursos como: espacio en disco duro, impresoras, CD-ROM, etc.

Los estándares más comunes utilizados son el IEEE 802.3 (Ethernet) operando entre 10 y 100 Mbps y el IEEE 802.5 (ToKen Ring) que opera entre 4 y 16 Mbps. Con medios de transmisión tales como cable de par trenzado, cable coaxial (casi obsoleto), y fibra óptica.

Característicamente estas redes ofrecen una baja latencia y una baja tasa de errores, operando con velocidades de transmisión entre 10 y 100Mbps

2.2.3.1.2. Redes MAN.

El Área de red metropolitana, representa una evolución del concepto de red de área local a un ámbito más amplio, cubriendo áreas de una cobertura superior. Son redes de alta velocidad (banda ancha), que proporcionan capacidad de integración de múltiples servicios mediante la transmisión de datos, voz y video, sobre medios de transmisión tales como fibra óptica y par trenzado de cobre a velocidades que van desde los 2 Mbps hasta 155 Mbps.

La principal razón que distinguen a la MAN, para estar en una categoría especial es que se ha adoptado un estándar para ellas, ya está implementado y se llama DQDB (Distributed Queue Dual Bus, o bus dual de cola distribuida) definido por IEEE 802.6.

Prestan servicios de transporte para interconexión de redes, telefonía con PBX, etc. Pueden ser de conmutación de circuitos o de paquetes con servicios orientados o no a la conexión.

2.2.3.1.3. Redes WAN.

Cuando se llega a un cierto punto deja de ser un poco práctico seguir ampliando una LAN, dado por las limitaciones físicas. La red de área extensa (Wide Area Network, WAN) representa el conjunto de soluciones de comunicaciones que permiten, a nivel de alcance, abarcar geográficamente un país o continente.

Son redes punto a punto (subred), caracterizado por la unión de diferentes LANs utilizado routers, y líneas de comunicación que une a las redes. Estas subredes poseen dos componentes diferentes; las líneas de transmisión llamados circuitos, canales o troncales donde se mueve la información y los elementos de conmutación basados en computadores especializados que conectan dos o más líneas de transmisión, encargándose de decidir que camino, que línea de salida toma la información que llega por la línea de entrada.

Por lo general usan redes públicas y/o privadas, haciendo uso de diferentes tipos de topologías de transmisión.

2.2.3.1.4 Redes WLAN.

La red inalámbrica de área local (Wireless Local Area Network) es un sistema de comunicación de datos inalámbrico flexible muy utilizado como alternativa a la LAN cableada o como una extensión de ésta. Utiliza tecnología de radiofrecuencia que permite mayor movilidad a los usuarios.

Estas redes utilizan el estándar IEEE 802.11, el cual se basa en el mismo marco de estándares que Ethernet, garantizando interoperatividad y una implantación sencilla de las funciones y dispositivos de interconexión Ethernet/WLAN.

El atractivo fundamental de este tipo de redes es la facilidad de instalación y el ahorro que supone la supresión del medio de transmisión cableado. Aún así, debido a que sus prestaciones son menores en lo referente a la velocidad de transmisión que se sitúa entre los 2 y los 10 Mbps frente a los 10 y hasta los 100 Mbps ofrecidos por una red convencional, las redes inalámbricas son la alternativa ideal para hacer llegar una red tradicional a lugares donde el cableado no lo permite, y en general las WLAN se utilizarán como un complemento de las redes fijas.

Según los requerimientos del sistema, existen diversas configuraciones que se puedan implementar, la más básica es "ad-hoc" (ó peer to peer) que consiste en dos terminales móviles equipados con la correspondiente tarjeta adaptadora para comunicaciones inalámbricas. Cuando los requerimientos son aumentar el enlace de una red del tipo anterior, se implementa el "modo infraestructura", basado en la instalación de un punto de acceso, permitiendo así tener acceso a otros recursos (por ejemplo, conexión con otras redes). Y finalmente es la que incluye el uso de "antenas direccionales", cuyo objetivo es el de enlazar varias LAN o WMAN.

2.2.3.2. De acuerdo a la relación funcional.

2.2.3.2.1. Cliente-Servidor.

Esta arquitectura es una forma de dividir y especializar programas y equipos de cómputo a fin de que la tarea que cada uno de ellos realizada se efectúe con la mayor eficiencia, y permita simplificarlas.

En esta arquitectura la capacidad de proceso está repartida entre el servidor y los clientes, donde uno o más ordenadores actúan como servidores y el resto como clientes. Pueden estar conectados a una red LAN, WAN o a una red mundial como lo es Internet.

En la funcionalidad de un programa distribuido se pueden distinguir 3 capas o niveles: Manejador de Base de Datos (Nivel de almacenamiento), Procesador de aplicaciones o reglas del negocio (Nivel lógico) y Interface del usuario (Nivel de presentación)

2.2.3.2.2. Igual a Igual (P2P).

Se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan simultáneamente como clientes y como servidores de los demás nodos de la red. Este modelo de red contrasta con el modelo cliente-servidor la cual se rige de una arquitectura monolítica donde no hay distribución de tareas entre sí, solo una simple comunicación entre un usuario y una terminal en donde el cliente y el servidor no pueden cambiar de roles.

Dentro de esta arquitectura se diferencian tres tipos: las centralizadas (utilizan un único servidor), descentralizadas (no utiliza un servidor central) y semi-centralizadas o mixtas (el servidor no comparte archivos).

2.2.3.3. De acuerdo a su carácter.

2.2.3.3.1. Redes públicas.

Estas redes tienen carácter público cuando los requerimientos necesarios para ser usuario de la misma, no tienen otra restricción que la disponibilidad de los medios técnicos.

Las redes públicas pueden ser de conmutación de paquetes o de conmutación de circuitos, y los servicios son suministrados por compañías que se dedican a transportar señales, llamadas carriers, las que dan cobertura tanto local como larga distancia.

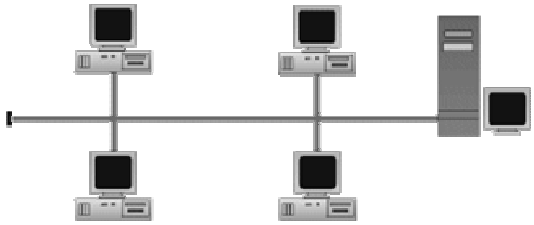
2.2.3.3.2. Redes privadas.

Estas redes, operan con un fin determinado y los usuarios pertenecen a una o varias corporaciones con intereses específicos en las mismas. En la práctica, una red privada puede ser una red con facilidades de una pública. En este caso, el cliente proporciona todo el equipamiento de conmutación y alquila enlaces entre distintos lugares. De este modo, el término privado se refiere al hecho de que la organización tiene el uso exclusivo de todo o una parte de ella, sin compartir los recursos de la red pública dentro de la cual funciona.

2.2.3.4. De acuerdo a la topología de red.

2.2.3.4.1. Red de bus.

En esta topología, las estaciones comparten una misma línea de comunicación (medio). Cuando una estación quiere transmitir, simplemente envía sus tramas al bus (medio de comunicación). Cuando una señal atraviesa el bus (normalmente un cable coaxial), todas y cada una de las estaciones escuchan la señal que lleva consigo una designación de dirección. Ambos extremos del cable troncal, deberán tener conectado un terminador, con el propósito de evitar que un paquete llegue a un extremo del troncal y rebote, manteniendo ocupada la red.



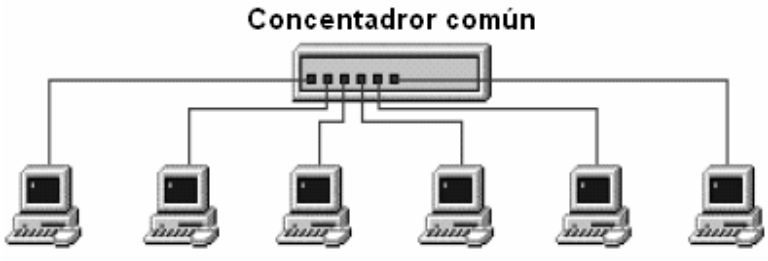
Los sistemas de bus, como Ethernet o la mayoría de los sistemas de banda ancha, emplean un cable bidireccional con trayectorias de avance y regreso sobre el mismo medio, o bien emplean un sistema de cable doble o dual para lograr la bidireccionalidad.

Es la topología más común en pequeñas LAN, con hub o switch final en uno de los extremos.

2.2.3.4.2. Red de estrella.

Normalmente, es una red donde todas las estaciones están conectadas a un concentrador común o nodo central con cable por computadora. Utilizando par trenzado, coaxial, o fibra óptica.

La fiabilidad del sistema se basa en que un nodo puede fallar sin que ello afecte a los demás nodos de la red. No obstante, su punto débil es que un fallo en el nodo central provoca irremediablemente la caída de toda la red.



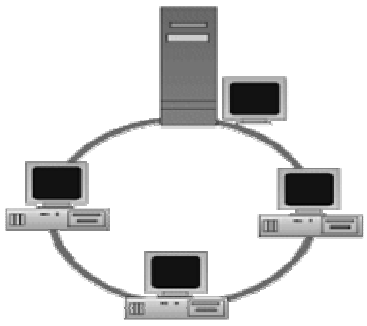
Esta arquitectura se utiliza en redes LAN, donde el nodo central es una Mau o una Cau que conecta en estrella estaciones de trabajo para redes Token Ring, o un hub o un switch para redes Ethernet. También esta topología se utiliza en redes WAN, donde habitualmente el nodo central es una computadora de gran tamaño, conocida como "mainframe", actuando como una ETD en conjunto con variadas interfaces para la conectividad de DCE.

Bajo una apreciación de costos, la implementación de esta arquitectura resulta ser muy elevada, dado que cada nodo está conectado al nodo principal por un cable independiente.

2.2.3.4.3. Red de anillo.

En una red de anillo los ETD se conectan uno tras otro formando un círculo cerrado. Esta topología mueve información sobre el cable en una dirección. Siendo considerada como una topología activa.

El acceso al medio de la red es otorgado a un ETD en particular en la red por un "token". El token circula alrededor del anillo y cuando una ETD desea enviar datos, espera al token y posiciona de él, y entonces envía los datos sobre el cable. El ETD de destino envía un mensaje (al origen) que de fueron recibidos correctamente. Creando un nuevo token el ETD que transito que transitó la información, empezando el ritual de paso de token o estafeta (token passing) nuevamente.

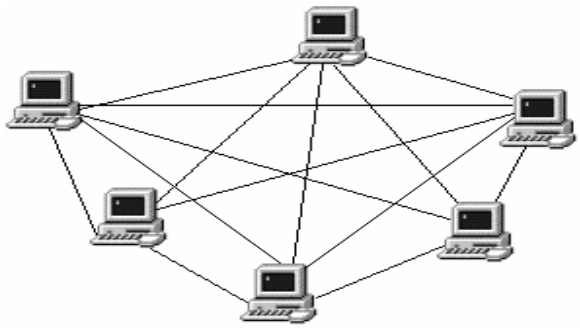


La falla de un enlace compromete la integridad y funcionalidad de toda la red. Una desventaja (por ejemplo, si se produce un corte del cable), afecta a todas las estaciones, por lo que se han desarrollado sistemas en anillo doble o combinando topologías de anillo y estrella para contrarrestar este efecto.

En aplicaciones prácticas, los anillos son lógicos. La red Ethernet cuando utiliza cable coaxial sigue una topología en bus lineal tanto físico como lógico. En cambio al instalar cable bifilar, la topología lógica sigue siendo en bus pero la topología física es en estrella o en estrella distribuida.

2.2.3.4.4. Red malla.

Una red con topología en malla ofrece una redundancia y fiabilidad superiores. Cada equipo está conectado a todos los demás equipos mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red, de modo que si falla un cable, otro se hará cargo del tráfico.



Aunque la facilidad de solución de problemas y el aumento de la fiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. En muchas ocasiones, la topología en malla se utiliza junto con otras topologías para formar una topología híbrida. Muy empleada en las redes de área amplia (WAN).

2.2.3.5. De acuerdo a la disponibilidad.

2.2.3.5.1. Enlaces dedicados.

Es un trayecto de comunicación estáticamente definido entre dos sistemas que se comunican ya sea por un enlace físico determinado, o por una traza lógicamente definida por completo dentro de un sistema de comunicaciones.

Normalmente estos circuitos pueden ser fijos cuando se arriendan líneas que mantienen una conexión permanente entre dos lugares fijos, nombre que se le da a redes punto a punto. Se utilizan por lo general en la construcción de redes privada.

Un circuito también puede ser del tipo lógico, como lo son redes X.25 o Frame Relay que son protocolos de transmisión de datos en redes de conmutación de paquetes. Estos circuitos no son punto

a punto, es un enlace que se establece en forma virtual preparando el camino para la transmisión, se le llama Circuito Virtual Permanente.

2.2.3.5.2. Redes Conmutadas.

Cuando las redes no requiere conexiones permanentes entre dos puntos y otros, se le dice que son redes conmutadas porque debe establecerse la ruta de datos –o trayecto- antes de comenzar la comunicación entre dos puntos. Son rutas temporales entre diversos puntos, una vez establecida podría incluso ser dinámicamente alterada sin que se altere la comunicación entre los ETD, dependiendo del tipo de red.

Independiente de las técnica de conmutación que se establezca, que pueden ser de circuito, de mensajes, o de paquetes. Las características principales de estas son:

La transmisión no puede ser preestablecida o preacondicionada, por cuanto los circuitos que se establecen y las rutas de los datos empleadas podrán cambiar de sesión en sesión.

Al cortarse la comunicación, se libera el enlace.

El costo es generalmente una función del tiempo de conexión o una función de la cantidad de datos transmitidos.

2.2.3.6. De acuerdo al tipo de información.

Se ha mencionado frecuentemente que la información que se transmite puede ser digital o analógica, lo cual define algunos aspectos del alcance de un servicio.

2.2.3.6.1. Redes digitales.

Son redes diseñadas y equipadas para el transporte de señales digitales, y aparecieron ante la necesidad de transmitir digitalmente mensajes codificados de forma digital. Ahora, es cada vez más común la digitalización de transmisión y conmutación en las redes, debido a la presencia de diseños cada vez más simples, minimización del ruido, como así también poseen la capacidad de transportar voz, imagen y texto, en tiempo real.

Los requerimientos de comunicación actuales, junto a las nuevas tecnologías, han hecho que sea posible la existencia de Redes Digitales de Servicios Integrados (RDSI) o integrated switched data network (ISDN).

2.2.3.6.2. Redes analógicas.

Son redes diseñadas y equipadas para el transporte de señales analógicas. Son el medio de transporte de señal más difundido, ya que en sus orígenes estas redes fueron ideadas para la transmisión de voz, y éste es un fenómeno que si bien es naturalmente analógico, en el momento de su mayor expansión no había tecnología para desarrollarlas en forma digital.

Actualmente, son las más usadas ya que trabajan sobre la base de las redes de telefonía públicas y se encuentran disponibles con una cobertura mundial y con grandes inversiones de capital. Son más económicas en comparación las redes digitales. Sus servicios están normalizados internacionalmente por el ITU-T que es el Comité de Telecomunicaciones de la Unión Internacional de Telefonía, y esta normalización hace que existan las interfaces estándares con equipos ETD

2.2.3.7. De acuerdo a la tecnología de transmisión.

2.2.3.7.1. Redes de broadcast.

Aquellas redes en las que la transmisión de datos se realiza por un sólo canal de comunicación, compartiendo todos los ETD de la red. Cualquier paquete de datos enviado por cualquier máquina es recibido por todas las de la red. Este mecanismo es muy útil cuando se desea llegar a muchos receptores y se cuenta con recursos escasos como procesamiento o ancho de banda. La desventaja es que los nodos que no tienen interés en la información enviada se ven interrumpidos con cada mensaje de broadcast, además que el broadcast no es enviado por los enrutadores de un segmento a otro. Como aplicación, se utiliza en redes satelitales, así también en redes LAN (red con topologías bus y anillo).

2.2.3.7.2. Redes point to point.

Las redes punto a punto son aquellas en las que se usa cada canal de datos para comunicar únicamente a 2 nodos, en contraposición a las redes multipunto, en las cuales cada canal de datos se puede usar para comunicarse con diversos nodos. La ventaja de este tipo de conexión se encuentra en la alta velocidad de transmisión que soporta y la seguridad que presenta al no existir conexión con otros usuarios. Un inconveniente es su costo.

2.2.3.8. De acuerdo al tipo de información.

2.2.3.8.1. Redes de transmisión simple.

En este tipo de redes, la transmisión de datos se produce en un solo sentido. Siempre existen un ETD emisor y un ETD receptor que no cambian sus funciones.

2.2.3.8.2. Redes Half-Duplex.

En estas redes la transmisión de los datos se produce en ambos sentidos pero alternativamente, estableciendo un solo sentido a la vez. Si se está recibiendo datos no se puede transmitir.

2.2.3.8.3. Redes Full-Duplex.

Las redes basadas en este modelo de transmisión de datos, se produce en ambos sentidos al mismo tiempo. Un extremo que esta recibiendo datos puede, al mismo tiempo, estar transmitiendo otros datos. Este procedimiento de carga, transporte y descarga "reduce" el trafico en la red.

2.3. PROTOCOLO TCP/IP.

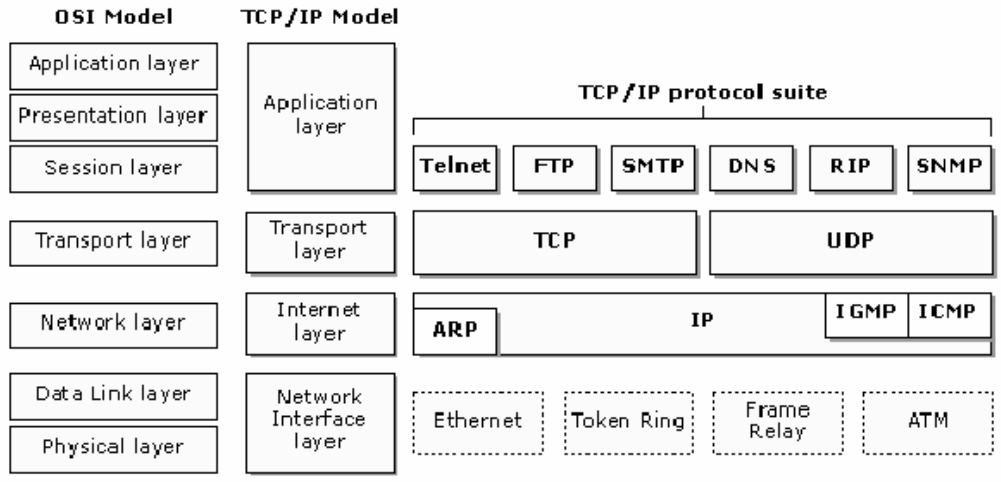
2.3.1 Modelo Arquitectónico.

La arquitectura TCP/IP se empezó a desarrollar como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU.) y con la expansión de la Internet, está hoy en día convertida en una de las arquitecturas de redes mas ampliamente difundida.

La pila TCP/IP se llama así por dos de sus protocolos más importantes: **TCP** (Transmission Control Protocol) de **IP** (Internet Protocol).

El protocolo Internet (IP) permite que se transmitan los datos a través y entre redes, de ahí su nombre, inter-net protocol (protocolo entre redes). Los datos viajan sobre una red basada en IP en forma de paquetes IP (unidad de datos). Cada paquete IP incorpora una cabecera y los datos del propio mensaje, y en la cabecera se especifican el origen, el destino y otra información acerca de los datos.

El Protocolo de Control del Transmisión (TCP) es el protocolo más común para asegurar que un paquete IP llega de forma correcta e intacto. TCP ofrece la transmisión fiable de datos para los niveles superiores de aplicaciones y servicios en un entorno IP. Proporcionando fiabilidad en la forma de un envío de paquetes de extremo a extremo orientado a conexión a través de una red interconectada.



La relación de esta arquitectura con respecto al modelo de referencia OSI (Open Systems Interconnection) de la ISO que posee siete niveles (o capas). Se basa en un modelo (TCP/IP) que está definido por cuatro capas en las que se agrupan los protocolos. Estas capas son:

La **Capa de Interfaz de red** que es la responsable de enviar los datos al medio físico (cables-adaptadores) de la red y recibir datos del mismo. Esta para acceder al medio corre por las interfaces conocidas, como: IEEE 802.2, Ethernet, CSMA/CD, X.25, Token Ring, etc.

La **Capa de Internet**, es el nivel de red del modelo OSI. Incluye al protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes, manejando así la comunicación de una maquina a otra. Es utilizado con esta finalidad por los protocolos del nivel de transporte.

La **Capa de Transporte**, coincide con el nivel de transporte del modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

Y finalmente tenemos la **Capa de Aplicación** que corresponde con los niveles OSI de aplicación, presentación y sesión. Aquí se incluyen protocolos destinados a proporcionar servicios, tales como: correo electrónico (SMTP), transferencia de ficheros (FTP), conexión remota (TELNET), aplicación para el control de la red (SNMP), y otros más recientes como el HTTP, TFPT, DNS, VoIP, etc.

2.3.2. Capa de Interfaz de red.

En la capa de acceso al medio se determina la forma en que los puestos de la red envían y reciben datos sobre el medio físico. Un organismo de normalización conocido como IEEE (Instituto de ingenieros eléctricos y electrónicos) ha definido los principales protocolos de la capa de acceso al medio conocidos en conjunto como estándares 802. Los más importantes son: Token Ring, Token Bus, CSMA/CD y FDDI, que se estudian a continuación.

2.3.2.1. CSMA/CD.

El estándar IEEE 802.3 especifica el método de control del medio (MAC), que regula el uso del canal compartido, evitando las colisiones. Denominado CSMA/CD, siglas que corresponden a **CSMA**, que significa Carrier Sense Media Access (Acceso al Medio por Detección de Portadora), basada en un algoritmo que sitúa las tramas en la señal física de la portadora y **CD**, por las siglas Collision Detection o Detección de Colisiones, permite detectar la colisión debido a una variación en la señal.

El algoritmo de acceso múltiple define las siguientes acciones o respuestas de una estación:

- **Postergar:** La estación no debe transmitir mientras haya una portadora presente o mientras no haya pasado el tiempo mínimo entre paquetes.
- **Transmitir:** La estación puede transmitir hasta que se termine el paquete o hasta que se detecte una colisión.
- **Interrumpir:** Si se detecta una colisión, la estación debe interrumpir la transmisión del paquete y transmitir una breve señal de interferencia (jamming) para asegurar que todas las estaciones participantes en la colisión la detecten.
- **Retransmitir:** La estación debe esperar un tiempo de retardo aleatorio y luego intentar la retransmisión del paquete.

Hoy en día, Ethernet es la implementación comercial de este protocolo. A continuación veremos qué define esta importante arquitectura a subnivel MAC y a nivel físico.

La capa MAC se ha especificado de un modo independiente a la velocidad, exceptuando el tramo entre paquetes, todos los parámetros de la capa MAC son definidos en bits respecto del tiempo. Ello permite la variación de la velocidad sin alterar los parámetros MAC, por lo que CSMA/CD funciona a 1 Mbps. (1Base5), 10 Mbps. (redes Ethernet actuales) y 100 Mbps. (Fast Ethernet o 100Base-T).

La segunda parte del protocolo Ethernet es la capa física (PHY o physical layer) que se ocupa de la comunicación entre la capa MAC y el cableado. Existiendo diferentes implementaciones de la capa física, dadas las diferentes posibilidades de cableado:

10 Base X, (donde la "X" puede ser):

- **2** Ethernet con coaxial fino
- **5** Ethernet con coaxial grueso
- **T** Ethernet con par trenzado de 4 hilos
- **F** Ethernet con fibra óptica
- **S** Ethernet con fibra óptica

100 Base X. (donde la "X" puede ser):

- **T** Ethernet con par trenzado ocho hilos.
- **F** Ethernet con Fibra Óptica.
- **S** Ethernet con Fibra Óptica.

1000 Base X, (donde la "X" puede ser):

- **F** Ethernet con Fibra Óptica.
- **S** Ethernet con Fibra Óptica.

2.3.2.2. Token Bus.

Está definido por IEEE 802.4, destinado a topologías lógicas en bus y con protocolo MAC de paso de testigo (Token Bus). Corresponde a un protocolo que realiza procesos de control de acceso al medio compartido, evitando así las denominadas colisiones.

El derecho de transmisión se va pasando de estación en estación de forma ordenada a través de un frame de control (token), bajo la organización de un anillo lógico, que permite conocer la dirección del predecesor como la del sucesor (c/estación).

Existen diferentes niveles físicos para esta norma y sus velocidades pueden ser de 1,5 a 10 Mbps.

2.3.2.3. Token Ring.

También llamado IEEE 802.5 fue ideado por IBM y algunos otros fabricantes, con topología lógica en anillo y técnica de acceso de paso de testigo. El acceso al medio es determinista por el paso (anti-horario) de testigo o token.

Las redes basadas en este estándar alcanzan una velocidad máxima de transmisión que oscila entre los 4 y los 16 Mbps., cuyo rango se elevó posteriormente a 100 Mbps por HSTR (High Speed Token Ring).

2.3.2.4. FFDI.

FDDI (Fiber Distributed Data Interface) es una evolución de Ethernet, token bus a protocolos de mayores prestaciones. Propuesto por ANSI (estándar X3T9.5), el cual es principalmente uilizado para la interconexión de dos o mas redes locales que con frecuencia distan grandes distancias.

Transmite datos en tiempos cortos y acotados, a altas velocidades, cuyo valor alcanza velocidades de transmisión de hasta 100Mbps y utiliza un método de acceso al medio basado en paso de testigo (token passing).

Soportando dos tipos de tráficos síncrono y asíncrono.

Es importante además, hacer notar que FDDI define una topología de red local en doble anillo (uno transmitiendo en el sentido de las agujas del reloj y el otro en dirección contraria) y con soporte físico de fibra óptica (FO). La transmisión se da en uno de los anillos pero si tiene lugar un error en la transmisión el sistema es capaz de utilizar una parte del segundo anillo para cerrar el anillo de transmisión.

Una red FDDI puede conectar un máximo de 500 estaciones con una distancia máxima entre estaciones de 2Km y 20Km dependiendo del tipo de FO. La longitud máxima del anillo de fibra es de 200Km ó 100Km si es doble.

Dentro de esta norma existe una clasificación de acuerdo a la cantidad de anillos a que sean conectados los dispositivos. Los dispositivos denominados A, encargados de la seguridad frente a la ruptura del anillo, debido a que se conectan a los dos anillos (primario-secundario). A diferencia de los dispositivos B, que se conectan únicamente a uno de los dos anillos (primario). La elección de una estación se basa en la seguridad y los costos asociados.

2.3.2.5. IEEE 802.11x.

Conocida también como Wi-Fi (Wireless Fidelity) o como WLAN.

La norma IEEE 802.11 fue diseñada para sustituir a la capa física y MAC de la norma 802.3 (Ethernet), donde los dispositivos acceden a la red de forma inalámbrica. Como mecanismo de acceso

al medio, se basa en el protocolo CSMA/CA, que es muy similar al utilizado en Ethernet (CSMA/CD), a través del cual se evitan a un máximo las colisiones producidas en el sistema

Existen varias subespecificaciones, como lo son IEEE 802.11b e IEEE 802.11g, que disfrutan de una aceptación internacional debido a que la banda de 2.4 GHz que está disponible casi universalmente, con velocidades de hasta 11 Mbps y 54 Mbps, respectivamente.

Debido a las demandas del sistema, se está desarrollando un nuevo estándar (802.11n) que trabaja a 2.4 GHz a una velocidad de 108 Mbps.

2.3.3. Capa de Internet.

2.3.3.1. Protocolo Internet (Internet Protocol - IP).

El Protocolo IP es el principal del modelo OSI, así como parte integral del TCP/IP. Las tareas principales del IP se basan en el direccionamiento de los datagramas de información y la administración del proceso de fragmentación de dichos datagramas.

El datagrama es la unidad de información enviada a través de la red, que provee las bases para la distribución de paquetes.

Las características más relevantes de este protocolo son:

- Transmisión en unidades llamadas datagramas.
- No orientado a conexión, de manera no fiable
- Sin control de congestión, ni corrección de errores.
- No hay garantización de la entrega en secuencia.

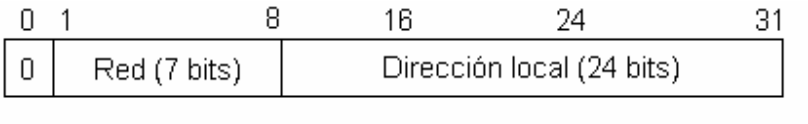
2.3.3.1.1 Direccionamiento IP.

El TCP/IP utiliza una dirección cuya longitud es de 32 bits para identificar una maquina (Host address) y la red a la cual está conectada (Network address). Siendo asignada por una autoridad central, el NIC (Network Information Center) o Centro de información de red.

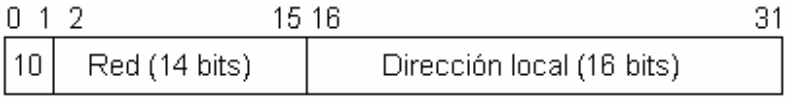
La dirección IP no individualiza a un ordenador, sino que identifica la conexión de dicho aparato a una red. Por eso cuando un ordenador se cambia de red se debe reasignar su identificación IP.

Existen cuatro formatos para la dirección IP, cada uno de los cuales se utiliza dependiendo del tamaño de la red. Los cuatro formatos, Clase A hasta Clase D (aunque últimamente se ha añadido la Clase E para un futuro).

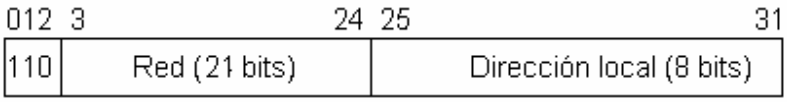
CLASE A: las direcciones de clase A, correspondes a redes grandes con muchas máquinas, con 7 bits para red y 24 bits para los dispositivos. El rango de direcciones varía desde el 0.0.0.0 hasta el 127.0.0.0. Esto permite tener 128 (2^{7}) redes, con 16777214 ($2^{24} - 2$) host en cada una.



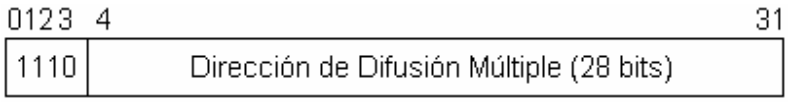
CLASE B: las direcciones clase B sirven para redes de tamaño intermedio, con 14 bits para red y 16 bits para los dispositivo. Las direcciones de esta clase están comprendidas entre 128.0.0.0 hasta el 191.255.255.255. Lo que permite tener 16384 (2^{14}) redes con 655534 ($2^{16} - 2$) host en cada una.



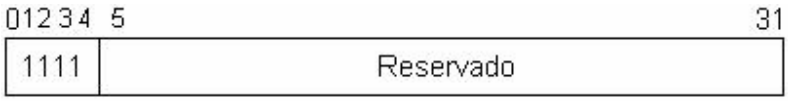
CLASE C: las direcciones clase C se asocia a redes pequeñas, tiene 21 bits para red y tiene solo 8 bits para la dirección local o anfitrión (host), localizándose el rango de direcciones entre 192.0.0.0 a la 223.255.255.255. Permitiendo un numero de redes igual a 2097152 (2^{21}), y un número de 254 ($2^{8} - 2$) host.



CLASE D: las direcciones de clase D se usan con fines de multidifusión 28 bits, cuando se quiere una difusión general a más de un dispositivo. El rango es desde 224.0.0.0 a la 238.255.255.255



CLASE E: las direcciones de clase E, serán de utilización futura, cuyo rango está comprendido desde 240.0.0.0 hasta el 247.255.255.255.



Por tanto, las direcciones IP son cuatro conjuntos de 8 bits, con un total de 32 bits. Por comodidad estos bits se representan como si estuviesen separados por un punto, por lo que el formato de dirección IP puede ser: red.host.host.host para clase A hasta red.red.red.host para clase C.

2.3.3.1.2. Formato del Datagrama IP.

La estructura de un datagrama IP está dividida en bloques de 32 bits (4 bytes). El datagrama IP se transmite enviando primero el bit 0, luego el bit 1, 2, 3... y así sucesivamente hasta finalizar el datagrama.

Esta estructura consta de los siguientes campos:

La **versión (**4 bits), sirve para identificar el número de versión del protocolo al que pertenece el datagrama, lo que permite la coexistencia de diferentes versiones del protocolo IP.

El **tamaño de la cabecera** (Header Length), son 4 bits que indican la longitud de la cabecera en palabras de 32 bits.

El **campo del tipo de servicio** (Type Of Service), se compone de 8 bits. Es una indicación de la calidad del servicio (Qos) solicitado para este datagrama IP

La **longitud del datagrama** (Total Length), es un número de 16 bits que indica la longitud total del datagrama, considerando tanto como la cabecera como los datos, especificada en bytes.

El **número de identificación del datagrama** (Identificartion Field), es un número de 16 bits que en caso de fragmentación de un datagrama nos indica su posición en el datagrama original. Lo que permite recomponer el datagrama original en la máquina de destino.

Las **banderas** (Flags) son 3 bits. El primer bit no se utiliza actualmente. El segundo es el bit de más fragmentos (**MF**) que indica si el datagrama recibido es un fragmento de un datagrama mayor. Y el tercero es el bit de no fragmentar (**DF**), que prohíbe la fragmentación del datagrama.
Cuando MF asume un valor "0", significa que se trata del último fragmento del datagrama y en caso contrario, si es "1", indica que hay mas fragmentos.
Y en el caso de DF, cuando es "0", permite la fragmentación, y si es "1", no la permite.

El **desplazamiento del fragmento** (Fragmentation Offset, FO) tiene un campo de 13 bits, indicando la posición en bytes que ocupan los datos en el datagrama original, medido en unidades de 8 bytes (64 bits). Como se proporcionan 13 bits, puede haber un máximo de 8912 (2^{13}) fragmentos por datagrama, y por lo tanto el tamaño máximo de un datagrama es de 65536 bytes, uno mas que el campo de longitud total.

El **tiempo de vida** (Time To Live, TTL), es un campo de 8 bits que indica el tiempo máximo que el datagrama será valido y podrá ser transmitido por la red. Consiste en un mecanismo que realiza la cuenta que es inicializada en el ordenador de origen (256), y se va decrementando en una unidad por cada salto de dispositivos de encaminamiento (router). Cuando llega a cero la cuenta, el paquete se descarta y se envía un datagrama (ICMP) de error al ordenador de origen para avisar la perdida.

El **tipo de protocolo** (8 bits), indica el número oficial del protocolo de alto nivel al que IP debería entregar los datos del datagrama. Algunos de estos valores son:

0 **Reservado**.
1 **ICMP** (Internet Control Message Protocol).
2 **IGMP** (Internet Group Management Protocol).
3 **GGP** (Gateway-to-Gateway Protocol).
4 **IP** (IP encapsulation).
5 **Flujo** (Stream).
6 **TCP** (Transmission Control).
7 **EGP** (Exterior Gateway Protocol).
8 **PIRP** (Private Interior Routing Protocol).
9 **UDP** (User Datagram).
10 **OSPF** (Open Shortest Path First).

El **checksum** (16 bits), actúa como un mecanismo de control de errores. Como algunos de los campos de la cabecera pueden cambiar en alguno de los dispositivitos de encaminamiento, este valor es verificado y recalculado en cada uno de estos. El algoritmo empleado consiste en sumar todas las medias palabras de 16 bits a medida que van llegando, usando la aritmética de complemento a 1, y luego obtener el complemento a 1 del resultado. Esta suma de comprobación de la cabecera es cero cuando llega el datagrama.

La **dirección IP de origen** (Source IP address), es la dirección IP de 32 bits del host emisor.

La **dirección IP de destino** (Destination IP address), es la dirección IP de 32 bits del host receptor.

Las **opciones IP** (Options IP) es un campo de longitud variable, que contiene las solicitudes enviadas por el usuario (que pueden ser: marca de tiempo, registro de ruta, seguridad, etc.)

Relleno: (variable), si las direcciones IP no ocupan un múltiplo de 32 bits, el campo de opciones se rellena para que su tamaño sea múltiplo de 32 bits (4 bytes).

Dato (Data): Contiene la información del nivel superior (TCP, UDP).

2.3.3.1.3. Encaminamiento IP.

Esta función proporciona los mecanismos necesarios para interconectar distintas redes físicas. La formación de la red virtual que conecta múltiples redes se consigue por medio de unos hosts especiales denominados "**routers**".

Un routers interconecta redes físicas diferentes a nivel de la capa de red y encamina paquetes entre ellas. Este debe comprender la estructura de direccionamiento asociada con los protocolos que soporta IP y debe elegir las mejores rutas de transmisión así como tamaños óptimos para los datagramas realizando fragmentación si lo considera oportuno.

El encaminamiento IP puede ser de "**entrega directa**", cuando la transmisión de un datagrama de realiza entre dos host (origen – destino) conectados directamente a la misma red física (por ejemplo, una sola red ethernet). Y se hace necesaria una **"entrega indirecta"**, cuando el host destino no está conectado directamente a la red del origen, lo que implica que el datagrama deberá atravesar varias redes físicas, y para ello es necesario atravesar routers (identificación del siguiente salto).

Para averiguar la siguiente máquina a la que se debe enviar un determinado datagrama por un router o un host, se utiliza el método de algoritmo de encaminamiento. Que consiste en tablas donde se almacena información sobre los posibles destinos y sobre cómo alcanzarlos. Estas suelen ser pares

del tipo <N, R>. Donde “N” es un número de red y “R” es la dirección IP del router en el siguiente salto para alcanzar dicha.

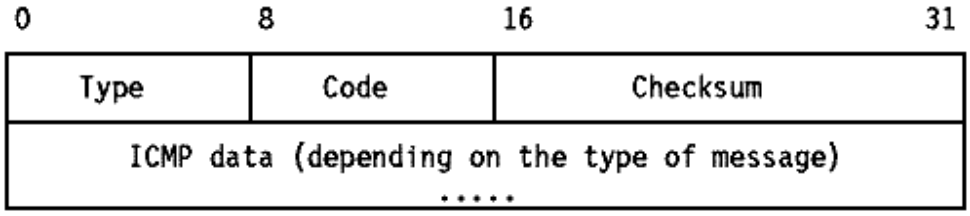
2.3.3.2. ICMP (Internet Control Message Protocol).

A nivel de red ningún sistema funciona correctamente bien todo el tiempo, presentándose fallas típicas (por ejemplo: procesadores, valor TTL, congestión en los routers, etc.) que deben ser controladas. Para ello se hace uso de un protocolo denominado ICMP (protocolo de control de mensajes de Internet).

ICMP es un protocolo de control, que proporciona el medio para el envió de mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Cuando un sistema detecta una condición de error en la red, usualmente emitirá un mensaje de error ICMP, para notificar sobre la condición de error al sistema remitente del paquete que la generó, el cual debe relacionar el error con un programa de aplicación individual o tomar otra acción para corregir el problema. Algunos de estos mensajes pueden ser generados por sistemas intermediarios (routers), mientras que otros pueden ser generados por sistemas finales (hosts).

Cada tipo de **mensaje ICMP** tiene su propio formato, aunque todos ellos comienzan con tres campos comunes. El resto de campos puede variar en función del tipo de mensaje. Los campos comunes son el campo tipo, el campo código y el campo checksum.



Datagrama ICMP

El **Tipo** (Type) indica el carácter del mensaje enviado (8 bits), ya que el protocolo permite especificar una gran variedad de errores o mensajes de control de flujo de las comunicaciones.

El campo de **Código** (Code), indica el código de error (8 bits), dentro del tipo de error indicado en el campo “tipo”.

El **Checksum** (de 16 bits), simplemente permite verificar la integridad del mensaje enviado, lo que permite detectar posibles errores en el envío, transporte o recepción del mensaje de control ICMP.

Además, los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.

La razón de regresar más que el encabezado del datagrama únicamente es para permitir que el receptor determine de manera más precisa que protocolo(s) y que programa de aplicación son responsables del datagrama.

El campo TYPE de ICMP define el significado del mensaje así como su formato. Los tipos incluyen:

tipo	mensaje ICMP
0	Echo Reply (respuesta de eco)
3	Destination Unreacheable (destino inaccesible)
4	Source Quench (disminución del tráfico desde el origen)
5	Redirect (redireccionar - cambio de ruta)
8	Echo (solicitud de eco)
11	Time Exceeded (tiempo excedido para un datagrama)
12	Parameter Problem (problema de parámetros
13	Timestamp (solicitud de marca de tiempo)
14	Timestamp Reply (respuesta de marca de tiempo)
15	Information Request (solicitud de información) - obsoleto-
16	Information Reply (respuesta de información) - obsoleto-
17	Addressmask (solicitud de máscara de dirección)
18	Addressmask Reply (respuesta de máscara de dirección)

Tipo 8 y 0: En la mayoría de los sistemas, el comando que llama al usuario para enviar solicitudes (petición / respuesta) de ECO se conoce como “ping”. Este es utilizado en redes para comprobar si otro host está operativo.

Tipo 3: Cuando un dispositivo de encaminamiento detecta que la red o el servidor de destino es inalcanzable, envía un mensaje de destino inalcanzable al emisor del datagrama. Este vendrá dado por el valor del campo "código", pudiendo presentar los siguientes valores:

código	suignificado
0	no se puede llegar a la red
1	no se puede llegar al host o aplicación de destino
2	el destino no dispone del protocolo solicitado
3	no se puede llegar al puerto destino o la aplicación destino no está libre
4	se necesita aplicar fragmentación, pero el flag correspondiente indica lo contrario
5	la ruta de origen no es correcta
6	no se conoce la red destino
7	no se conoce el host destino
8	el host origen está aislado
9	la comunicación con la red destino está prohibida por razones administrativas
10	la comunicación con el host destino está prohibida por razones administrativas
11	no se puede llegar a la red destino debido al Tipo de servicio
12	no se puede llegar al host destino debido al Tipo de servicio

Tipo 4: cuando los datagramas llegan demasiado deprisa para ser procesados, el servidor de destino o un dispositivo de encaminamiento intermedio envía un mensaje de petición al emisor para controlar el flujo.

Tipo 5: se suelen enviar cuando, existiendo dos o más routers diferentes en la misma red, el paquete se envía al router equivocado. En este caso, el router receptor devuelve el datagrama al host origen junto con un mensaje ICMP de redirección, lo que hará que éste actualice su tabla de enrutamiento y envíe el paquete al siguiente router.

Tipo 11: cuando un datagrama llega al fin de su vida, por haber excedido el número de saltos entre routers permitido, se envía un mensaje ICMP de este tipo al host de origen.

Tipo 12: cuando un paquete está mal construido en el origen, y un equipo de encaminamiento lo detecta este envía un mensaje ICMP de errores de parámetro y descarta el datagrama.

Tipo 13 y 14: son mensajes de petición y respuesta de marca de tiempo, respectivamente. Indican la hora de un sistema, y sirven para efectuar una apreciación de lo que tarda el sistema remoto en el procesamiento del buffer de memoria y del datagrama.

Tipo 15 y 16: obsoletos.

Tipo 17 y 18: son mensajes de petición y respuesta de máscara de dirección, respectivamente. Usados cuando un host se reinicia en una red y no conoce cuántos bits se han asignado a la máscara de subred.

2.3.3.3. IGMP (Internet Group Management Protocol).

El protocolo de administración de grupos de Internet (IGMP), funciona como una extensión del protocolo IP, se utiliza para intercambiar información acerca del estado de pertenencia entre enrutadores IP que admiten la multidifusión y miembros de grupos de multidifusión. Los hosts miembros individuales informan acerca de la pertenencia de hosts al grupo de multidifusión y los enrutadores de multidifusión sondean periódicamente el estado de la pertenencia, especificando el interés del host (activo/inactivo) en recibir tráfico de multidifusión de una lista de orígenes especificada.

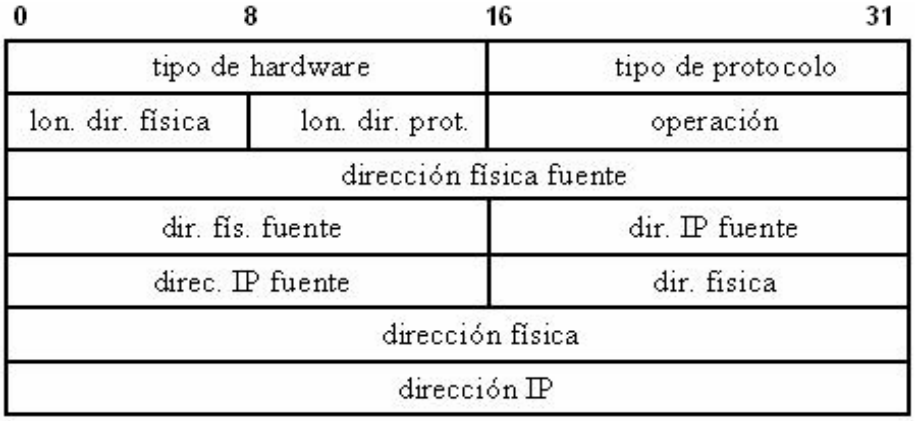
2.3.3.4. ARP (Address Resolution Protocol).

El protocolo de resolución de direcciones (ARP), es el encargado de convertir las direcciones IP en direcciones de la red física (Ethernet). Para ello utiliza una tabla de direcciones IP en correspondencia con las direcciones físicas (MAC).

Cuando se envía un mensaje a un host (ordenador) de destino, y la dirección buscada no está en la tabla, ARP envía un mensaje como broadcast a toda la red y cuando un host reconoce su dirección IP envía (al host origen) un mensaje de respuesta que contiene la dirección física, permitiendo la comunicación con la máquina destino, guardándose esta dirección física en la Tabla de direcciones ARP.

2.3.3.4.1. Formato ARP

El formato de mensaje de ARP no es fijo, lo que le permite ser usado por otros protocolos de alto nivel. Consiste en una larga secuencia de bits, distribuida como se muestra en la figura



El **campo Hardware** indica el tipo de interfaz de Hardware. Por ejemplo una red Ethernet tiene asignado el valor 1.

Value	Description
1	Ethernet.
2	Experimental Ethernet.
3	Amateur Radio AX.25.
4	Proteon ProNET Token Ring.
5	Chaos.
6	IEEE 802.
7	ARCNET.
8	Hyperchannel.
9	Lanstar.
10	Autonet Short Address.
11	LocalTalk.
12	LocalNet (IBM PCNet or SYTEK LocalNET).
13	Ultra link.
14	SMDS.

Números de Protocolo. El campo protocolo identifica el protocolo Ether usado. Por ejemplo el valor del interfaz Ethernet es 0800 hex.

Longitud de la dirección Hardware. El valor para Ethernet es 6, lo que proporciona 48 bits para una dirección Ethernet (12 semi-octetos).

Longitud del Protocolo. Este campo se usa para definir la longitud de la dilección de red. Para una red IP es 4.

Operación. Especifica el código de la operación. La solicitud ARP tiene valor 1, y la respuesta ARP tiene valor 2.

Dirección Hardware del Origen. Los campos dirección Hardware del Origen, dirección IP del Origen, y dirección IP del Destino los completa el emisor (si los conoce). El receptor añade la dirección Hardware del Destino y devuelve el mensaje al emisor con el código de operación 2. (El código de la Respuesta ARP).

La dirección Hardware de Origen (para Ethernet) esta formada por octetos que representan una dirección Ethernet de 48 bits, o un numero.

Dirección IP de Origen. Puede ser una dirección de clase A, B o C.

Dirección Hardware de Destino. Este campo está formado igual que el campo dirección Hardware de Origen.

Dirección IP de Destino. Este campo es igual que el campo Dirección IP de Origen

2.3.3.4.2. Mensaje RARP (Reverse Address Resolution Protocol).

El protocolo de resolución de direcciones inverso, es el encargado se asignar una dirección IP a una dirección física (Ethernet).

El formato del RARP es similar al del ARP. El valor del código de operación para una solicitud es 3, y el valor para una respuesta es 4.

2.3.4. Capa de Transporte.

Esta capa ofrece a la capa de aplicación dos servicios:

- un servicio orientado a conexión (TCP, Transmition Control Protocol);
- y un servicio no orientado a conexión (UDP, User Datagram Protocol).

El modulo **UDP**, no garantiza la entrega de los datagramas, proporcionando un servicio de baja fiabilidad. Los servicios que requieren un sistema de transporte fiable, deben emplear el protocolo **TCP**.

2.3.4.1. Protocolo TCP (Transmition Control Protocol).

El Protocolo de Control de Transmisión (TCP) nació principalmente por la necesidad de una comunicación "segura" entre el emisor y el destinatario del mensaje. Así, las aplicaciones pueden encargarse de su tarea sin preocuparse de la seguridad en la comunicación,

La interfaz entre los programas de aplicación y la entrega confiable (es decir, características de TCP) viene dada por los siguientes aspectos:

Servicio orientado a conexión. El servicio de entrega de flujo en la maquina de destino pasa al receptor exactamente la misma secuencia de bytes que le pasa el transmisor en al maquina de origen.

Conexión de circuito virtual. Durante la transferencia se establece un sondeo entre los dos equipos para verificar que los datos se reciban correctamente. Cuando se recibe un segmento

completo, el receptor envía una respuesta de confirmación (Acknowledge) al emisor confirmando el número de bytes correctos recibidos.

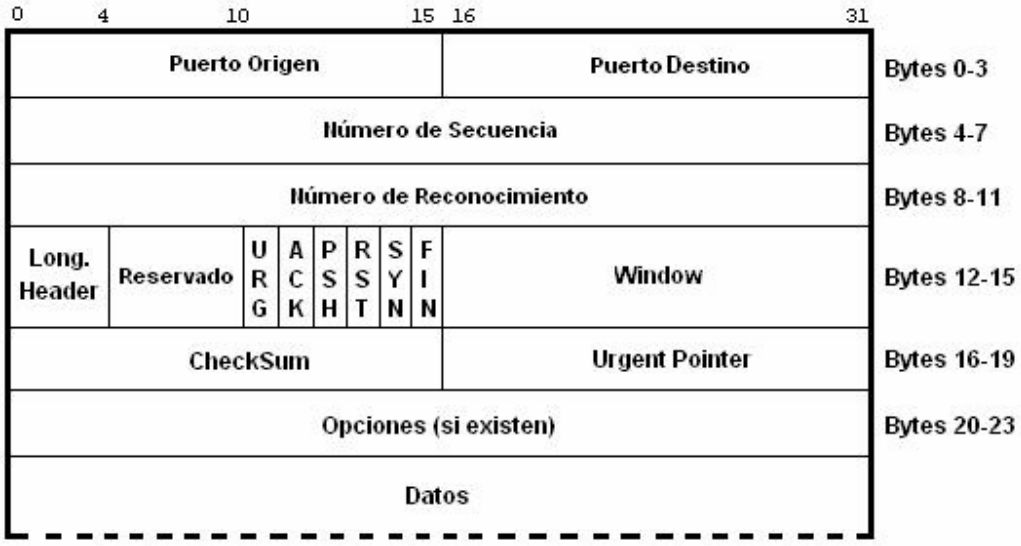
Transferencia con memoria intermedia. La aplicación utiliza paquetes del tamaño de crea conveniente, pero el software del protocolo puede dividir el flujo en subpaquetes o armar uno con un grupo de ellos, independientemente de la aplicación. Esto se realiza para hacer eficiente el tráfico en la red. Así, si la aplicación genera piezas de un byte, el protocolo puede armar datagramas razonablemente mas largos antes de hacer el envío, o bien forzar la transferencia dividiendo el paquete de la aplicación en datagramas más pequeños.

Flujo no estructurado. Posibilidad de enviar información de control junto a datos.

Conexión full duplex. TCP garantiza la concurrencia de los flujos de datos en ambos sentidos e la conexión.

La cabecera del segmento TCP (figura 1-12), es bastante más compleja que la de UDP debido a que la comunicación es más elaborada y debe proporcionar fiabilidad. Esto implica una serie de información adicional que debe mantenerse para poder conocer el estado de la comunicación en cualquier momento. Detallándose:

2.3.4.1.1. Constitución de un datagrama TCP.



El número de **puerto origen** (16 bits) y número de **puerto destino** (16 bits), sirven para diferenciar una comunicación en un ordenador de las demás.

El **número de secuencia** (32 bits), identifica el byte concreto del flujo de datos que actualmente se envía del emisor al receptor. De esta forma, TCP numera los bytes de la comunicación de una forma consecutiva a partir del número de secuencia inicial (valor aleatorio negociado por ambas partes).

El **número de reconocimiento**, es el número de secuencia más uno. De este modo se especifica al emisor que los datos enviados hasta este número de secuencia menos uno son correctos. De aquí la importancia de la elección al principio de la comunicación de un número de secuencia común.

La **longitud de la cabecera,** especifica en palabras de 32 bits el tamaño de la cabecera del segmento TCP incluyendo las posibles opciones. Indica donde empiezan los datos.

Las **banderas** (flags) 6 bits, son las encargadas de especificar los diferentes estados de la comunicación. Así mismo, también validan los valores de los distintos campos de la cabecera de control. Puede haber simultáneamente varios flags activados. Los distintos flags existentes y su significado, son:

URG	Indica si es válido el puntero de urgencia.
ACK	Indica si es valido el valor situado en el campo de confirmación (acknowledge).
PSH	El receptor debe pasar los datos a la aplicación o antes posible.
RST	Resetea la conexión
SYN	Inicio de comunicación. Búsqueda de un número de secuencia común.
FIN	El emisor finaliza el envío de datos.

El **tamaño de la ventana** (Window Size), es el número de bytes desde el número especificado en el campo de confirmación, que el receptor está dispuesto a aceptar.

El **checksum del segmento** TCP (16 bits), tiene la función de controlar los posibles errores que se produzcan en la transmisión. Consiste en un campo opcional consistente en el complemento a uno de 16 bits de la suma en complemento a uno de una pseudocabecera IP, la cabecera UDP y los datos del datagrama UDP.

El **puntero de urgencia** (Urgent Poiner), es válido sólo si el flag de **URG** se encuentra activado. Consiste en un valor positivo que se debe sumar al número de secuencia especificando una posición adelantada dónde podemos enviar datos urgentes.

Las **opciones** (Options), Permite que una aplicación negocie durante la configuración de la conexión, como el tamaño de segmento a utilitzar.

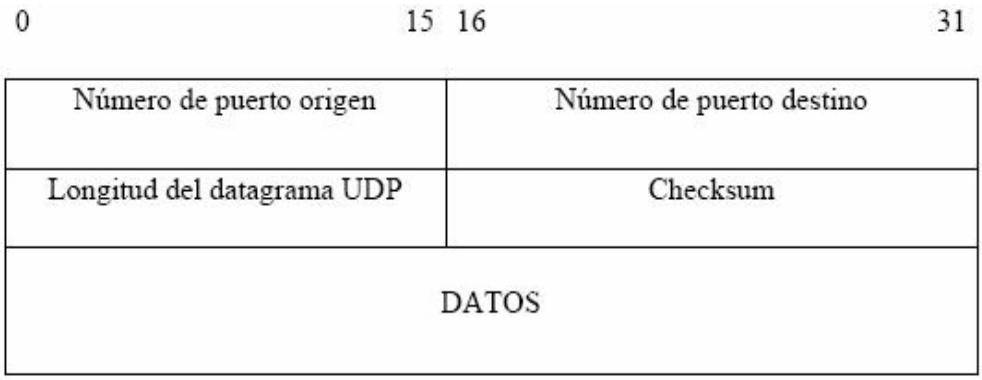
Los **datos** (Data) son opcionales. Esto significa que podemos enviar simplemente cabeceras TCP con diferentes opciones. Esta característica se utiliza por ejemplo al iniciar la comunicación o en el envío de confirmaciones.

2.3.4.2. Protocolo UDP (User Data Protocol).

El Protocolo de datos de usuario (UDP) proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre máquinas. Se utiliza en aplicaciones DNS, RPC, TFTP, SNMP, NCS y NFS.

UDP recibe los datos del nivel de aplicación, les añade su cabecera, y los envía directamente al destino dentro de un datagrama IP. Conceptualmente, este datagrama se divide en: un encabezado UDP y un área de datos UDP. Este encabezado se divide en cuatro campos de 16 bits, especificando el puerto desde el que se envió el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación.

2.3.4.2.1. Formato de los mensajes UDP.



Los campos **puerto origen** y **puerto destino**, 16 bits cada uno, identifican el puerto UDP al cual va dirigido el datagrama dentro de la máquina destino, y el puerto al cual tendrá que dirigir su posible respuesta.

La **longitud del datagrama** (UDP Length), 16 bits, hace referencia al tamaño del datagrama en bytes, y engloba la cabecera (8 bytes) más los datos que transporta.

El campo de **checksum** (16 bits) al igual que en IP, sirve como método de control de los datos, verificando que no han sido alterados. Este checksum cubre tanto la cabecera UDP como los

datos enviados. Si se detecta un error en este campo, el datagrama es descartado sin ningún tipo de aviso.

2.3.4.2.2. Puertos.

Las aplicaciones que envían datagramas necesitan identificar un objetivo más específico que la dirección IP, deben focalizarse a un determinado proceso, lográndose esto a través de los puertos. Estos puertos son bastantes independientes, ya que un servidor usara TCP o UDP, pero hay excepciones, por ejemplo, los servidores DNS que en ambos usa el puerto 53.

Un puerto es un número de 16 bits que identifica qué proceso de un host está asociado con un cierto datagrama, dividiéndose en: el **well-known** (bien conocidos) que permite a los clientes tener la capacidad de encontrar servidores sin información de configuración. La mayoría de los servidores requiere solo un puerto, a excepción del servidor BOOTP que usa dos (67 y 68). Y **efímeros**, los clientes no necesitan números de puertos bien-conocidos porque inician la comunicación con servidores y el número de puerto que usan ya está contenido en los datagramas UDP enviados al servidor.

2.3.5. Capa de Aplicación.

Existen multitud de aplicaciones que usan la torre de protocolos TCP / IP como servicio de transporte. Los protocolos en los que se basan la mayoría de ellas están normalizados por la principal organización normalizadora de estándares de Internet, el IETF. Algunos de estos protocolos de nivel de aplicación son:

2.3.5.1. FTP.

El Protocolo de Transferencia de Archivos, File Transfer Protocol, se incluye como parte del TCP/IP, estando destinado a proporcionar el servicio de transferencia de archivos a través de la red.

FTP se basa en una arquitectura Cliente / Servidor, dependiendo del protocolo TCP (puerto 21) para funciones de transporte y está relacionado con Telnet para la conexión remota.

Para acceder a archivos de carácter publico por medio de FTP, se utiliza el acceso FTP anónimo, mediante el cual se pueden realizar ciertas acciones (por ejemplo, copiar archivos), limitando el acceso a ciertas acciones tales como añadir archivos o modificar los existentes. Y en tal caso al iniciar una sesión el servidor FTP solicitará el nombre de usuario y clave de acceso.

Gran parte de las páginas Web son subidas mediante este protocolo a sus servidores de alojamiento.

2.3.5.2. HTTP.

Hiper Text Tranfer Protocol es la base de toda la comunicación en la Web (www). Cosiste en un protocolo de transferencia de hiper texto que utiliza por defecto el puerto TCP 80. El "hipertexto" es el contenido de las páginas web, y el "protocolo de transferencia" es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. Además, establece acciones como enviar información adicional en ambos sentidos, como formularios con mensajes y otros similares.

El protocolo HTTP es un protocolo sin estado; está basado en el modelo cliente-servidor: Un cliente HTTP abre una conexión y realiza su solicitud al servidor, el cual responde generalmente el recurso solicitado y la conexión se cierra.

El formato tanto del mensaje como de la respuesta es como sigue:

<Línea inicial>
Header-1: value-1
Header-n: value-n
<Cuerpo del mensaje (Opcional)>

La línea inicial es diferente en las solicitudes y en las respuestas. En las solicitudes van tres campos separados por un espacio en blanco: "Método recurso versiónDelProtocolo". Por ejemplo: "GET /path/to/file/index.html HTTP/1.0". La línea inicial de una respuesta tiene tres campos separados por un espacio: "versiónDelProtocolo códigoRespuesta Mensaje". Por ejemplo: "HTTP/1.0 200 OK" o bien "HTTP/1.0 404 Not Found".

Los encabezados están normados en el protocolo, e incluyen, en el caso de una solicitud, información del navegador y eventualmente del usuario cliente; En el caso de una respuesta, información sobre el servidor y sobre el recurso.

El cuerpo del mensaje contiene el recurso a transferir o el texto de un error en el caso de una respuesta. En el caso de una solicitud, puede contener parámetros de la llamada archivos enviados al servidor.

2.3.5.3. SMTP.

Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo electrónico. Protocolo de red (emplea redes TCP/IP) basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras y/o distintos dispositivos (PDA's, Celulares, etc).

2.3.5.3.1. Funcionamiento.

SMTP se basa en el modelo cliente-servidor, donde un cliente envía un mensaje a uno o varios receptores. Generalmente los mensajes de correo electrónico no se envían directamente a las computadoras personales de cada usuario, sino aun servidor que actúa como almacén de los mensajes recibidos. Los mensajes permanecen en este sistema hasta que el usuario los transfiera a su propio equipo para leerlos de forma local (vía POP).

El cliente de correo envía una solicitud a su e-mail Server (al puerto25) para enviar un mensaje (y almacenarlo en dicho servidor). El Server establece una conexión SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mail. Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión.

En el siguiente ejemplo se establece el escenario de conexión típica. Las líneas que empiezan por S, son las enviadas por el emisor, y las precedidas por R son las enviadas por el receptor.

```
R: 220 Servidor SMTP
S: HELO
R: 250 Hello, please meet you
S: MAIL FROM: <yo@midominio.com>
R: 250 OK
S: RCPT TO: <destinatario@sudominio.com>
R: 250 OK
S: DATA
R: 354 End data with <CR><LF>.<CR><LF>
S: Date: día/mes/año  hora/min/seg
S: Subject: Campo de usuarios
S: From: <yo@midominio.com>
S: To:  <destinatario@sudominio.com>
S:
S: Hola,
S: Estoy  realizando pruebas
S: Hasta luego.
S: .
R: 250 OK
S: QUIT
R: 221 Bye
```

2.3.5.3.2. Formato del mensaje.

Como se muestra en el ejemplo anterior, el mensaje es enviado por el cliente después de que éste mande la orden DATA al servidor. El mensaje está compuesto por dos partes:

Cabecera: En ellas se usan unas palabras clave para definir los campos del mensaje. Éstos campos ayudan a los clientes de correo a organizarlos y mostrarlos. Los más típicos son subject (asunto), from (emisor) y to (receptor). Estos dos últimos campos no hay que confundirlos con las órdenes MAIL FROM y RCPT TO, que pertenecen al protocolo, pero no al formato del mensaje.

Cuerpo del mensaje: es el mensaje propiamente dicho. En el SMTP básico está compuesto únicamente por texto, y finalizado con una línea en la que el único carácter es un punto.

2.3.5.4. TELNET.

Este protocolo fue diseñado para proporcionar el servicio de conexión remota (remote login). Forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP (por defecto, puerto 23,) para el nivel de transporte.

TELNET es un emulador que permite acceder a los recursos y ejecutar los programas de un equipo remoto en la red. Utiliza Internet para conectarse al ordenador que se le especifica. Sólo puede acceder en modo terminal, es decir, sin gráficos, pero es una herramienta muy útil para arreglar fallos a distancia, sin necesidad de estar físicamente, como también para consultar datos a distancia.

Una gran desventaja de TELNET es “la baja seguridad” dado que este protocolo no utiliza ningún tipo de cifrado, por lo que todo el trafico se realiza en texto claro. Siendo reemplazada por la versión cifrada: SSH o SSL-Telnet.

2.3.5.5. SNMP.

El Simple Network Management Protocol se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y, aunque es parte de la familia TCP/IP no depende del IP ya que fue diseñado para ser independiente y puede correr igual, por ejemplo, IPX de Novell.

2.3.5.6. POP.

El servidor Post Office Protocol (POP) fue diseñado para la recuperación de correo desde el e-mail Server hacia la computadora destinataria del mensaje.

Al igual que sucede con SMTP, inicialmente el proceso escucha el puerto del protocolo POP (el 110) y cuando el emisor solicita el mensaje se establece una conexión full duplex donde se intercambian los mensajes Emisor-Server para luego finalizar la conexión cuando se hallan enviado cada uno de los mails que se almacenaban en el servidor.

Actualmente el protocolo POP se encuentra en una tercera implementación por lo que generalmente se escuchara sobre POP3.

2.3.5.7. DNS.

Las máquinas en Internet se identifican entre sí mediante una **dirección IP** (por ejemplo, 216.32.74.52) que las identifica. Sin embargo los seres humanos preferimos utilizar nombres (como www.yahoo.com), porque son más fáciles de recordar, y porque ofrecen la flexibilidad de poder cambiar la máquina en la que están alojados (cambiaría entonces la dirección IP) sin necesidad de cambiar las referencias a él. Para realizar esta conversión entre nombres y direcciones IP se utilizan los servidores DNS.

El Domain Name System (DNS), o Sistema de Nombres de Dominio, es un sistema jerárquico y descentralizado que permite la administración local de un segmento de una base de datos, que contiene información para localizar a los objetos que integran Internet

DNS se atribuye a tres acrónimos: sistema de nombres de dominio, servidor de nombres de dominio o servicio de nombres de dominio.

2.3.5.7.1. Nombres de Dominio.

La información relacionada con los nombres de dominio se almacena en un servidor, capaz de asociar distintos tipos de información a cada nombre de dominio, pero el uso más común es la asignación de nombres a una dirección IP con el fin de localizar servidores web y servidores de correo electrónico, a los cuales ha sido delegada la administración. Cada servidor de nombres almacena dicha información a través de los denominados RRs (Resource Records).

Al ser el DNS una base de datos distribuida, la veremos reflejada de muchas formas, una de ellas es a través de lo que comúnmente se conoce como zonas (un dominio o subdominio). La autoridad o el mando de una zona se delega a un servidor de nombres, y una zona puede contener varios RRs, éstos se dividen en clases, las cuales pertenecen a un tipo de red o de software. Dentro de una clase, los RRs también son de varios tipos y corresponden a las diversas variedades de datos que se pueden almacenar en el espacio del nombre de dominio.

2.3.5.7.2. Formato RRs.

El formato que tienen es el siguiente:

[Name] [ttl] <class> <type> <RDATA>

Name es el nombre de dominio por definir;

ttl (time-to-life): 32 bits, es el tiempo en segundos que el registro será válido en la caché de un servidor de nombres;

class (clase): 16 bits, es el tipo de red o software (existe la clase IN Internet), y se refiere a redes basadas en TCP/IP, redes basadas en protocolos Chaosnet (CH) y redes que usan software Hesiod (HS), la clase IN es la más utilizada;

type (tipo, 16 bits) define el tipo de RR;

RData: precisa los datos en relación con el tipo de RR.

2.3.5.7.3. Formato mensaje DNS.

El Protocolo DNS utiliza mensajes enviados por el **UDP** para trasladar solicitudes y respuestas entre servidores de nombres. La transferencia de zonas completas la hace el **TCP**.

El formato de un mensaje DNS tienen 5 partes.

- **Cabecera,** define el formato del mensaje.
- **Pregunta,** cuestión formulada al servidor de mensaje.
- **Respuestas**, contestación a la consulta.
- **Autoridad**, referencia a un servidor autorizado.
- **Adicional**, otra información no relacionada con la respuesta.

2.3.5.7.3.1. Formato de Cabecera.

Todos los mensajes generados por el protocolo DNS utilizan un único formato de cabecera, que contiene los siguientes campos:

ID: 16 bits, asignado para diferenciar respuestas en concurrencia de múltiples respuestas.

QR: 1 bits, flag que indica un mensaje como consulta (0) o respuesta (1).

OP code: 4 bit que especifica el tipo de consulta: 0 consulta estándar (QUERY), 1 consulta inversa (IQUERY) y 2 solicitud del estado del servidor (STATUS).

AA: 1 bits (flag de respuesta autoritativa). Cuando tiene valor 1, especifica que el servidor de nombres que responde tiene autoridad para el nombre de dominio enviado en la consulta.

TC: 1 bits (flag de truncado). Activo si el mensaje es más largo de lo que permite la línea de transmisión

RD: 1 bits (flag de recursividad). Este bit se copia en la respuesta e indica al servidor de nombres una resolución recursiva.

RA: 1 bits (flag de recursividad disponible). Indica si el servidor de nombres soporta resolución recursiva.

Z: 3 bits, reservados para uso futuro. Deben ser cero.

Rcode: es un código de respuesta de 4 bits. Los posibles valores son: **0** Ningún error. **1** Error de formato, el servidor fue incapaz de interpretar el mensaje. **2** Fallo en el servidor, el mensaje no fue procesado debido a un problema con el servidor. **3** Error en nombre, el nombre de dominio de la consulta no existe, siendo sólo válido si el bit AA está activo en la respuesta. **4** No implementado, el tipo solicitado de consulta no está implementado en el servidor de nombres. **5** Rechazado, el servidor rechaza responder por razones políticas.

QDcount: 16 bits, que especifica el número de entradas en la sección de preguntas (question).

ANcount: 16 bits, que especifica el número de RRs en la sección de preguntas (answer).

NScount: 16 bits, que especifica el número de RRs en la sección de autoridad (authority).

ARcount: 16 bits, que especifica el número de RRs en la sección de archivos adicionales (additional records).

3. CAPITULO III. PROTOCOLOS Y ESTÁNDARES DE SEÑALIZACIÓN PARA EL TRANSPORTE DE VOZ EN REDES IP.

En este capitulo se presentan las diferentes arquitecturas que están siendo propuestas para soportar la señalización de sistemas VoIP (voz sobre las redes IP), que hacen posible el desarrollo de servicios de Telefonía y Videoconferencia. Prestando especial atención a los estándares H.323, SIP y MGCP, junto con un breve resumen de los mecanismos de señalización en redes telefónicas clásicas (SS7).

3.1. INTRODUCCIÓN.

En los últimos años, los protocolos de señalización para el servicio de transmisión de voz han experimentado una fuerte evolución junto con la tendencia a trasportar dicho tráfico desde las redes de conmutación de circuitos hacia las redes de conmutación de paquetes. Esta tendencia queda reflejada con la fuerte evolución de estándares en este ámbito y la aparición de productos en el mercado que cubren las necesidades de operadores, grandes empresas y PYMES

Para que se pueda establecer este servicio comercialmente, que es VoIP, es necesario alcanzar niveles de servicio y calidad de los mismos en correspondencia con los que dan las redes circuitales clásicas, aunque existe la posibilidad, no remota, que aún con niveles por debajo de éstas se logren establecer por lo económico que resultan.

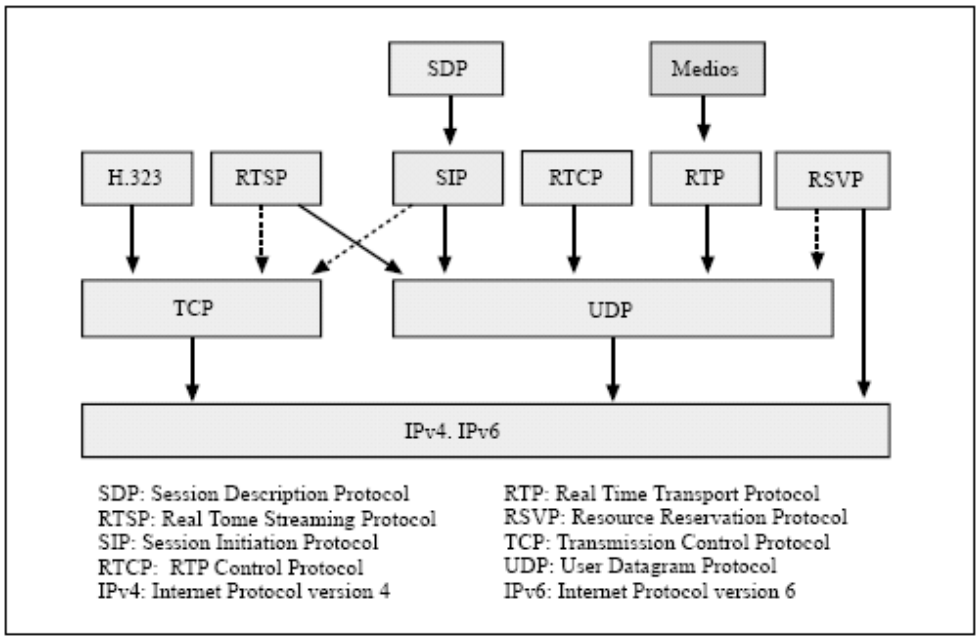
Para soportar el servicio de VoIP se requiere, además de los protocolos para el transporte de la información de usuario en tiempo real, también de la correspondiente señalización, es decir, de los protocolos necesarios que garanticen el establecimiento, mantenimiento - modificación y terminación de las llamadas de voz sobre las redes IP, lo que quiere decir que es necesario la señalización de control de las llamadas, todo el control de la comunicación, como pueden ser:

- Negociar el tipo de codificador a utilizar
- negociar los parámetros de empaquetado de la voz (y video);
- intercambio de número de puertos a través de los que se llevará a cabo la comunicación...etc.

El flujo de la información de usuario y el flujo de la señalización siguen trayectorias diferentes en su paso por las redes IP. La voz (información de usuario) y la señalización no presentan los mismos requerimientos de transporte por la red. La voz tiene que ser tratada con demora y jitter mínimos, pues pierde valor con el tiempo, dados sus requerimientos de tiempo real, y en cambio la señalización no requiere de esto último. Es decir, el tráfico de información de usuario es tratado por la red IP de manera diferente a como lo hace con el tráfico de señalización.

Con respecto a lo señalado anteriormente, se han desarrollado diferentes soluciones para la problemática de la señalización de control de llamada en sistemas de VoIP. Evidenciando cada modelo, con la arquitectura funcional y protocolos que lo caracterizan respectivamente.

Los protocolos de señalización utilizados son de diversos tipos, siendo transportados sobre los protocolos TCP/IP o UDP/IP:



Arquitectura de protocolos de telefonía IP

- El ITU-T **H.323** es una cobertura para diversos protocolos H.225, H.245 y RAS que se soportan en TCP y UDP. Siendo el primero aplicado para acciones dentro de una Intranet, cuya finalidad amplia, apoya la conferencia multimedios audio y vídeo, el establecimiento y control de llamadas, la gestión de anchura de banda y las interfaces entre diferentes arquitecturas de red.

- El protocolo mixto **MEGACO** (nombre asignado por la ITU-T) o H.248 (nombre asignado por la IETF), el cual define un protocolo que controla pasarelas de medios que pueden hacer pasar tráfico vocal, vídeo, facsímil y de datos entre las redes RTPC y las basadas en el IP
- EL IETF define los protocolos SIP/SAP/SDP para el control hacia las redes privadas. El protocolo de señalización SIP es propuesto como alternativa a la recomendación H.323, el cual cuya funcionalidad proporciona conferencia, telefonía y detección de presencia, notificación de eventos y mensajería instantánea.
- La señal vocal se transmite sobre el protocolo de tiempo real RTP (con el control RTPC) y con transporte sobre UDP. El protocolo de reservación de ancho de banda RSVP puede ser de utilidad en conexiones unidireccionales.
- La señalización **SS7** se utiliza hacia la red pública PSTN. De forma que se disponen de los protocolos ISUP/SCCP/TCAP que se transmiten sobre MTP en la PSTN y sobre TCP/IP en la red de paquetes. El protocolo **Q.931** (derivado de ISDN) se utiliza para establecer la llamada en H.323.

3.2 SEÑALIZACIÓN EN REDES TELEFÓNICAS CLÁSICAS.

La señalización en las redes telefónicas clásicas ha experimentado una intensa evolución a lo largo del siglo XX, al ritmo marcado por el propio desarrollo de las tecnologías de conmutación de circuitos en las que estas redes se fundamentan. Tras la conmutación manual de finales del siglo XIX y principios del XX, 1910 trajo la conmutación electromecánica. En esta etapa tecnológica, que duró hasta los años 60, la señalización se transportaba "en banda" (cambios de nivel y tonos dentro del propio canal telefónico) y era interpretada por elementos electromecánicos (relés) y electrónicos (filtros) en su tránsito por la red.

A mediados de los 60, el proceso de digitalización de la red alcanzó la propia tecnología de conmutación - red digital integrada de transmisión más conmutación- con la llegada de las centrales digitales y el control de la conmutación por CPU (control por programa almacenado). De este modo, los canales síncronos de 64 Kbps son conmutados octeto a octeto espacial y temporalmente. Estos conmutadores ya están controlados íntegramente por procesadores que hablan un protocolo de señalización con procesadores de otras centrales.

Los primeros protocolos de señalización instalados en estos sistemas tenían una expresividad muy limitada y se basaban en el estado de ciertos bits de la trama TDM permanentemente asociados a cada canal de voz, como meras representaciones binarias de las señales analógicas de los sistemas

precedentes. El salto cuántico se consiguió realmente cuando se aplicó totalmente la tecnología de redes de ordenadores y las señales devinieron en mensajes intercambiados por aplicaciones sobre una red de conmutación de paquetes independiente y dedicada a este fin.

Si bien en la actualidad la red telefónica utiliza internamente esta forma de funcionamiento prácticamente en su totalidad, el último segmento por digitalizar, la red de acceso del abonado, permanece masivamente análogica, con una penetración discreta de accesos íntegramente digitales (RDSI). Consecuentemente, la señalización de abonado del servicio de telefonía tradicional ha evolucionado muy poco y es dentro de la red donde se realizó una revolución muy importante, transparente al usuario, que ha permitido la introducción de servicios suplementarios, de telefonía móvil, de red inteligente, B-ISDN e interfuncionamiento con sistemas de ToIP entre otros.

El sistema de señalización de red que ha soportado esta evolución con gran flexibilidad es el Sistema de Señalización nº 7 (SS7).

3.2.1 Señalización Signaling System Number 7 (SS7).

El Sistema de Señalización nº 7 es un arquitectura de protocolos de señalización completa en el que las unidades de señal son mensajes de las aplicaciones de señalización transportados en paquetes. Está formada por nodos y diversos tipos de enlaces que están configurados de forma que aporten la máxima fiabilidad al sistema. Esta red se define de forma separada de la red de transporte de información y en su forma básica consta de nodos llamados puntos de señalización (SPs, Signaling Points) interconectados por enlaces de transmisión. La red se constituye con los siguientes tipos de nodos:

Service Switching Point (SSP). Punto de conmutación de servicio. Dispone de software especial para proporcionar servicios AIN (Advanced Intelligent Network)

Signal Transfer Point (STP). Punto de transferencia de señal. Proporcionan servicio de encaminamiento en la red de forma ininterrumpida.

Service Control Point (SCP). Punto de control de servicio. Tienen capacidades para realizar decisiones. Los AIN SCPs contienen programas lógicos de servicios que reflejan los servicios de clientes y que interactúan con SSP para gestionar decisiones en el procesado de llamadas.

Service Management System (SMS). Sistema de gestión de servicios. Realiza funciones de mantenimiento, administrativas y de provisión para los SCPs. También realiza la función de creación de servicios.

Signaling Links (SLs). Enlaces de señalización.

Intelligent peripheral (IP). Periférico inteligente. Añaden funciones de comprensión a la red tales como reconocimiento de voz, síntesis y anuncios de voz específicos.

Service Data Point (SDP). Punto de datos del servicio.

Service Creation Environment (SCE). Entorno de creación de servicios.

Adjunct (AD). Adjunto. Son nodos que se conectan a los SSPs y que realizan las mismas funciones que SCPs.

Services Node (SN). Nodo de servicios.

3.2.2. Arquitectura.

Con el objeto de independizar el transporte de la información de señalización del tratamiento, por software, de la misma se divide en dos:

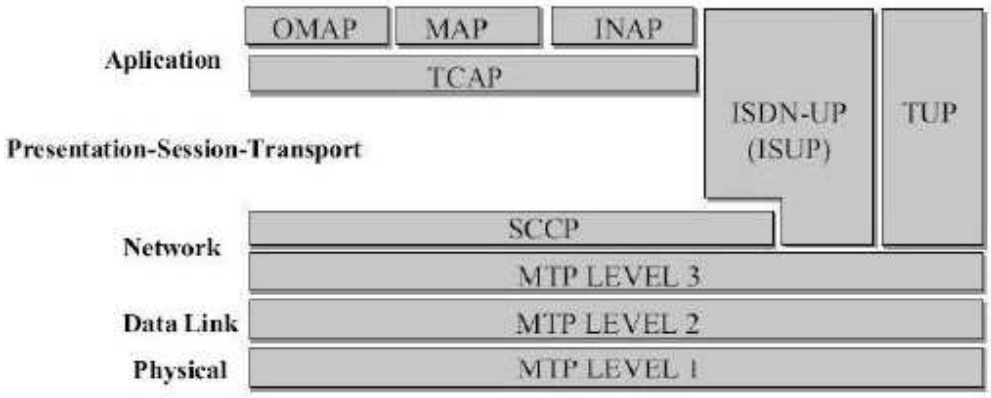
La parte de transferencia de mensaje (MTP): la cual garantiza el transporte fiable de la información de señalización.

Las diferentes partes de usuario (UP) y/o aplicaciones (AP): específica de usuario-aplicación y encargada de la comunicación y tratamiento de los mensajes de señalización.

Se asimila como un software que se usa para comunicarse con otro semejante cada usuario/aplicación, del SS7, utiliza las facilidades de transferencia de mensajes.

Inicialmente la SS7 se basa en requisitos necesarios para el control de telefonía relacionados con circuitos. Con estos objetivos como premisa se especifico los niveles funcionales que son cuatro. La MTP en donde se contienen los tres primeros niveles y los UPs que incluye el nivel 4.

Con las nuevas evoluciones en el área de la comunicación también han aparecidos nuevos circuitos, por ello fue necesario que el SS7 también evolucionara. Se necesito adaptar el SS7 del CCITT a algunos elementos del modelo OSI (Open Sistem Connection). Esto se refleja en la conexión de los niveles funcionales y las capas del modelo OSI, por ejemplo, la SCCP es una parte de usuario de nivel 4 en MTP, pero también, proporciona un servicio de capa 3 en la red OSI.



Pila de protocolos SS7

3.2.3. Modelo de capas para el sistema de señalización SS7.

Las capas **MTP** proporcionan las funciones para disponer de un enlace de señalización fiable para la transferencia de mensajes (información) a través de la red hacia el punto de destino. MTP se compone de tres niveles:

- Enlace de datos de señalización (Nivel 1);
- Enlace de señalización (Nivel 2);
- Red de señalización (Nivel 3)

MTP-1 (Capa 1). Tiene las funciones de conexión física entre módulos a interconectar.

MTP-2 (Capa 2). Mediante banderas (Flag) al inicio y final se ocupa del alineamiento de paquete. Permite la detección de errores mediante un código CRC-16.

MTP-3 (Capa 3). Posee una dirección de punto de acceso al servicio SAP en la información de servicio SIO. Por otro lado identifica el enlace de señalización utilizado cuando existe más de uno. Realiza las funciones de Routing dentro de la red de señalización SS7.

En los demás niveles se definen las funciones de transferencia y los procedimientos de operación sobre MTP en la PSTN y sobre TCP/IP en la red de paquetes de comunicación, de los distintos protocolos:

UP (Capa 7). Parte de usuario. Asegura la generación y tratamiento del mensaje de señalización. Contiene: usuario de telefonía (TUP**)**, usuario de datos (DUP**)** y usuario de red ISDN (ISUP**)**. Esta es la capa utilizada para enlaces internacionales de telefonía o de datos.

ISUP (Capa 7). Este protocolo sirve para los mensajes de señalización de usuario ISDN. Algunos tipos de mensajes, que contienen la información inicial de llamada para el encaminamiento (IAM), la indicación que el usuario llamado ha respondido (ANM). Permitiendo además el bloqueo/desbloqueo del canal útil (BLO/UBL).

SCCP (Capa 3). Efectúa funciones de direccionamiento adicionales a MTP3, especial para sistemas celulares. La combinación de SCCP y el MTP3 se denomina parte de servicio de red NSP. Además puede brindar servicios con y sin conexión. En telefonía celular se trata de un servicio sin conexión y la capa superior es TCAP. En el caso de servicio con conexión la capa superior es ISUP.

TCAP (Capa7). Es un servicio de transporte, que facilita la transferencia de mensajes en tiempo real entre MSC, HLR y VLR. La información contiene: tipo de mensaje (unidireccional, inicio, final, intermedio, aborto); longitud del mensaje (número de bytes total); identificador de origen y destino de transacción; tipo de componente (retorno de resultado, reporte de error y de reject) y contenido de información (código de operación, de error, de problema, parámetros, etc.).

MAP (Capa 7). Está especificado para transferencia de información que no es de circuitos de usuario. Se utiliza para interconectar los siguientes elementos entre sí: HLR (Home Location Register), VLR (Visitor LR), MSC (Mobile Switching Center), EIR (Equipment ID Register), además permite conectar a varios MSC de distinto proveedor de servicio SP (Service Provider). Permite las operaciones de: Actualización de localización; Roaming; Handover; autentificación; información de llamada entrante; información de servicio de subscriptor; identificación de equipos móviles; carga de información a los registros; etc.

3.3. MULTIMEDIA SOBRE REDES DE PAQUETES: SEÑALIZACIÓN H.323.

Es una recomendación que fija los estándares para comunicaciones multimedia (audio, video, datos) sobre redes que no ofrecen una calidad de servicio (Qos) garantizada, como lo son las redes basadas en IP. Versa sobre el control de llamadas, la gestión de multimedios y la gestión de la anchura de banda para conferencias punto a punto y multipunto, en conjunto a protocolos como RTP y RTCP. H.323 además define otras características como estandarización de códecs (audio, video, datos), interoperabilidad, además independencia de la aplicación y plataforma.

3.3.1. Características de H.323.

3.3.1.1. Codec estándar.

El H.323 establece normas para la compresión y descompresión de audio, datos y video asegurando que los equipos de diferentes proveedores tengan alguna área de apoyo en común.

3.3.1.2. Interoperatibilidad.

H.323 se diseña para correr en lo alto de las arquitecturas comunes de red. Como la tecnología de red evoluciona, y como las técnicas de gestión de ancho de banda mejoran, las soluciones basadas en H.323 serán capaces de aprovechar esas capacidades.

3.3.1.3. Soporta multipunto.

Aunque el H.323 puede soportar conferencias de tres o más terminales sin requerir una Unidad de control multipunto (MCU) especializada, las MCU´s proveen una arquitectura más poderosa para patrocinar conferencias multipunto. Las capacidades multipunto pueden incluirse como otro componente de un sistema H.323.

3.3.1.4. Administración de ancho de banda.

El trafico de video y audio es intenso y puede atascar la red, sobre este punto el H.323 provee gestión de ancho de banda. Los administradores de red pueden limitar el número simultáneo de conexiones dentro de su red o la cantidad de ancho de banda disponible a las aplicaciones H.323.

3.3.1.5. Soporta multicast.

El H.323 soporta transporte multicast en conferencias multipunto. El multicast envía un solo paquete al subconjunto de destinos sobre la red sin repetición. En contraste, unicast envía múltiples paquetes a las transmisiones “punto a punto”, mientras envían a todos los destinos. En unicast o broadcast, la red es usada ineficientemente ya que los paquetes se duplican a lo largo de la red. La transmisión multicast usa el ancho de banda más eficientemente ya que todas las estaciones en el grupo multicast leen un solo flujo de datos.

3.3.1.6. Conferencia entre distintas redes.

Muchos usuarios requieren conferenciar desde una red LAN a un sitio remoto. Por ejemplo, el H.323 establece un medio de vinculación de sistemas de escritorio LAN con grupos de sistemas

basados en ISDN. El H.323 usa tecnología de codificación común de diferentes estándares de videoconferencia para minimizar los retardos y proveer un óptimo desempeño.

3.3.2. Arquitectura.

H.323 define cuatro componentes principales para un sistema de conferencia multimedia, siendo: Terminales, Pasarelas, Unidades de Control Multipunto (MCUs) y GateKeepers. Los terminales, pasarelas y MCUs son considerados extremos porque pueden generar y/o terminar sesiones H.323. El gatekeepers es considerado una entidad de red porque no puede ser llamado, pero se le puede solicitar que lleve a cabo funciones específicas tales como traducción de direcciones o control de acceso. Cada componente se describe a continuación.

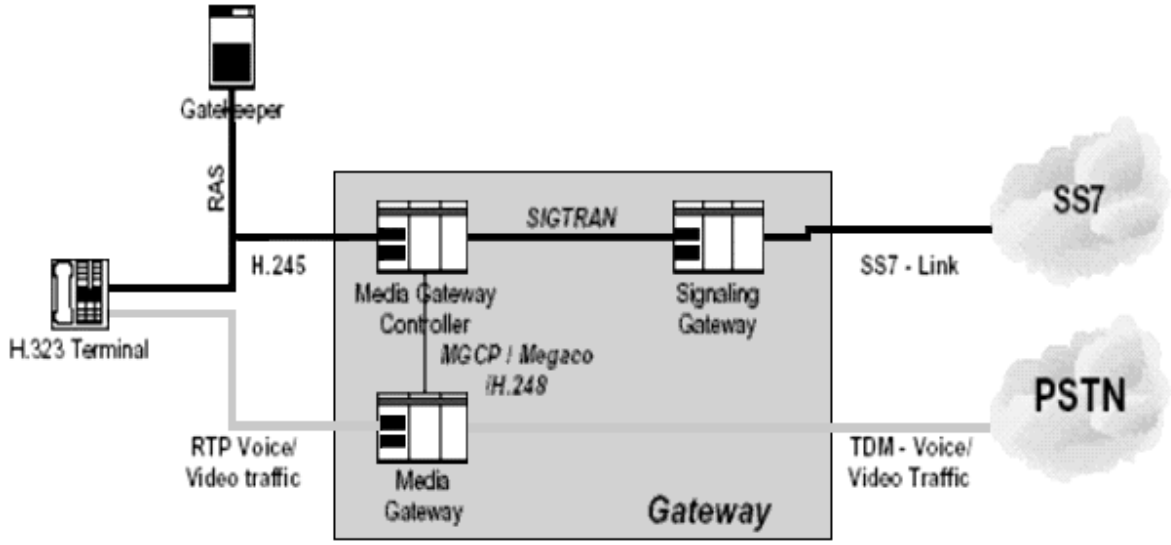
3.3.2.1. Terminales.

Un terminal H.323 es el interfaz entre el usuario final y 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.

3.3.2.2. Gateway (GW).

El Gateway es básicamente un dispositivo lógico que actúa como pasarela de interconexión entre la red telefónica clásica (modo circuito) y las redes de datos (modo paquete). Siendo las responsables de traducir el control del sistema, los codecs de audio, y los protocolos de transmisión entre los diferentes estándares de la ITU. Este dispositivo es fundamental durante la necesaria fase de coexistencia entre la telefonía analógica y la telefonía digital sobre IP.

Un modelo genérico para un Gateway H.323 puede ser una caja como la de la figura:



Dentro del tipo de pasarelas encontramos dos formas principales:

Media Gateway: por un lado está conectado a una red de área local y del otro asume una conexión a la red telefónica como un troncal T1 o línea RDSI para comunicación de video. Esta debe permanecer activa todo el tiempo para evitar cualquier interrupción de servicio entre dos terminales conectados. Este nodo controla el jitter, el retardo, la cancelación de eco y cualquier otro componente que constituye la calidad de servicio (QoS). De esta se deriva además una que proporciona el control general del Gateway (Media Gateway Controller). Se comunica con el Gatekeeper para solicitar información referente al mapeado entre una dirección IP y la red telefónica.

Signalling Gateway: responsable de la interfaz entre la red de señalización SS7 y la señalización VoIP, como H.323.

Cabe mencionar que existen unos gateways denominados especiales en tanto que se posicionan entre redes IP para desempeñar determinadas funciones de mapping, por ejemplo en la capa IP. Dentro de esta categoría podemos citar los proxies VoIP, transcodificadores VoIP, traductores de direcciones de red VoIP, etc.

3.3.2.3. MCU (Unidad de Control Multipunto).

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 MCU consta

de dos partes: un controlador multipunto (MC) el cual es obligatorio y un procesador multipunto (MP) opcional. En el caso más simple, una MCU puede estar formada por un MC únicamente.

3.3.2.3.1. MC (Controlador Multipunto).

Un controlador multipunto (MC) es un componente de H.323 que provee capacidad de negociación con todos los terminales para llevar a cabo niveles de comunicaciones. También puede controlar recursos de conferencia tales como multicasting de vídeo. El Controlador Multipunto no ejecuta mezcla o conmutación de audio, vídeo o datos.

3.3.2.3.2. MP (Procesador Multipunto).

El Procesador Multipunto (MP) es un componente de H3.23 que recibe flujos de audio, video o datos desde los extremos, estos pueden estar involucrados en una conferencia centralizada, descentralizada o híbrida. Donde éste procesa esos flujos medios (único o múltiples) dependiendo de la conferencia soportada y los devuelve a los extremos, a cada terminal participante.

Las capacidades del MC y MP pueden estar implementadas en un componente dedicado o ser parte de otros componentes H.323, en concreto puede ser parte de un Gatekeeper, un Gateway, un terminal o una MCU.

3.3.2.4. GateKeeper (GK).

El Gatekeeper es una entidad que se encarga del control, el enrutamiento y la seguridad de la comunicación, de manera que no se produzcan situaciones de saturación en la red. El cual proporciona la traducción de direcciones de redes (IP) en los alias de los usuarios, es decir, cada una de las terminales H323 recibe un nombre, facilitando así el marcado cuando los usuarios tienen sus libretas de direcciones y poder así conectarse a otros sistemas.

Es responsabilidad de éste, el control de acceso a la red de los terminales H.323, gateways y MCUs. Y otros servicios a éstos como localización de los gateways (zona H3.23) y gestión de ancho de banda, el cual mediante los protocolos adecuados puede indicar a cada terminal el ancho de banda total disponible según el tipo de llamada, las categorías de los terminales, etc.

Otro aspecto importante, es el tipo de servicios adicionales, como lo es la señalización para el establecimiento y liberación de llamadas, la cual puede efectuarse directamente entre dos terminales, o a través del gatekeeper. Las razones para autorizar o negar llamadas pueden incluir criterios de restricciones de ciertos terminales, horarios del día, etc.

Es necesario además definir dos términos que se utilizan en toda la literatura relacionada con este tema.

3.3.2.5. Entidad.

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

3.3.2.6. 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.

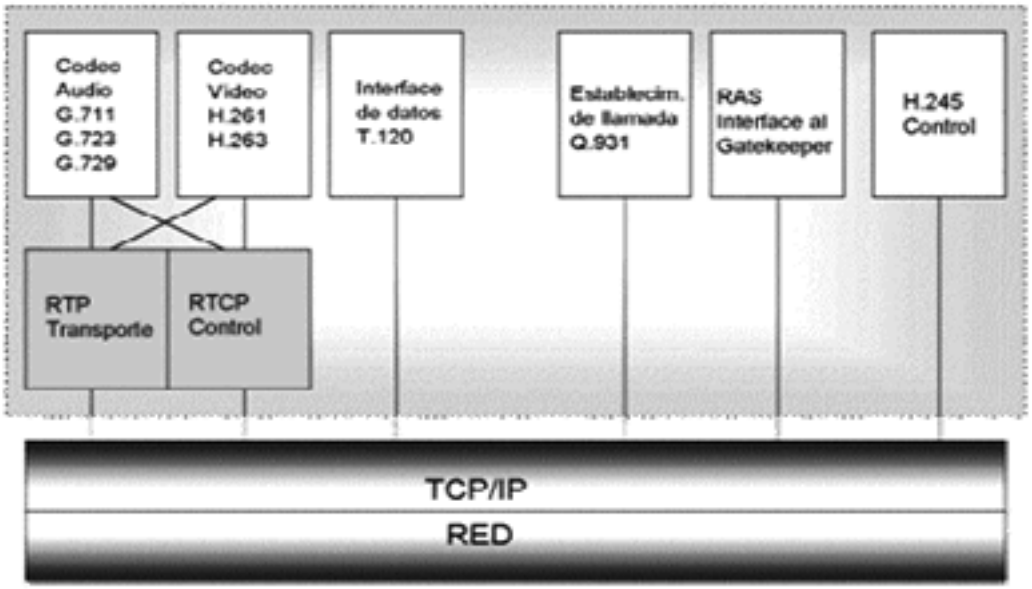
3.3.2.7. Zona H.323.

Es una colección de todas las terminales, gateways y MCUs, manejadas por un simple gatekeeper. Puede ser una topología de red independiente y estar comprendida por múltiples segmentos de red los cuales están conectados utilizando ruteadores u otros dispositivos. Otra forma de describir una zona gatekeeper es llamándola “dominio administrativo”.

3.3.3. Protocolos especificados por H.323.

El protocolo H.323 es complejo y orientado a las aplicaciones en multimedia; por esta razón existen generaciones de protocolos posteriores, los cuales interactúan entre si y con H.323.

Esta pila de protocolos realizan las funciones necesarias para establecer y mantener una sesión de conferencias en tiempo real de audio, video y datos sobre redes IP de datos. Este sistema completo e integrado incluye Q. 931, RAS, y RTP/RTCP (el cual maneja el empaquetamiento y la sincronización de todas las fuentes de video, voz y datos durante la sesión o sesiones múltiples simultáneas), y un H. 245 para controlar la comunicación entre los equipos terminales. Además de otros protocolos que están soportados en la especificación, pero no están incluidos (pila), el H. 261 y el H. 263 (Video Codecs), los G.722, G. 728 y G. 729 (Audio Codecs).



Estructuración Pila de Protocolos H.323

3.3.3.1. Canal de registros, administración y situación (RAS, Canal Registration Admission and Status).

El canal RAS es utilizado entre los terminales y el Gatekeeper. A través de éste canal, el terminal realiza las funciones de registro, admisión, solicitud de ancho de banda, status, etc. Este canal de señalización es independiente del canal de control H.245 y del canal de señalización de llamadas.

En ambientes de red dónde se dispone de un Gatekeeper, el canal de RAS debe ser abierto entre el terminal y el gatekeeper, antes de ser abierto cualquier otro canal entre terminales. El protocolo utilizado en el canal RAS está descrito en la recomendación de la ITU-T H.225.

3.3.3.2. Entramado y control de llamadas.

Los siguientes estándares constituyen la Unidad de Control del Sistema y proveen las capacidades de control de llamada y entramado:

3.3.3.2.1. Canal de señalización H.225.0.

El canal de señalización del terminal H.323 utiliza funciones de señalización del protocolo H.225.0 para establecer conexiones con otro terminal H.323. Este canal de señalización es independiente del canal de RAS y del canal de control H.245.

El canal de señalización es abierto por el terminal antes de establecer el canal de control H.245. En ambientes de red en los que no hay Gatekeeper, el canal de señalización es establecido directamente entre dos terminales. En ambientes de red en los que se dispone de un Gatekeeper, el canal de señalización es abierto entre el propio terminal y el Gatekeeper, o entre el propio terminal y otro terminal, de acuerdo a lo indicado por el Gatekeeper.

3.3.3.2.2. Canal de control H.245.

Los terminales H.323 utilizan uno o varios canales de control para enviar y recibir mensajes desde y hacia otros terminales y dispositivos H.323 (gateways, gatekeepers, etc.), El estándar H.245 provee el mecanismo de control de llamadas, a través de la definición de una serie de comandos y requerimientos, que le permite a los terminales compatibles H.323 interconectarse, estableciendo los medios para conexiones de audio y video.

Generalmente los elementos negociados por este estándar, es la selección de codec y la negociación de capacidades con H.323. La velocidad de bits y de trama, el formato de la figura y la selección del algoritmo.

La Recomendación UIT-T H.245 especifica varias entidades de protocolo independientes que soportan señalización de punto extremo a punto extremo. Una entidad de protocolo se especifica por su sintaxis, su semántica y un conjunto de procedimientos que establecen el intercambio de mensajes y la interacción con el usuario. Los puntos extremos H.323 soportarán la sintaxis, la semántica y los procedimientos de las siguientes entidades de protocolo:

- Determinación maestro/esclavo.
- Intercambio de capacidades.
- Señalización de canal lógico unidireccional.
- Señalización de canal lógico bidireccional.
- Señalización de cierre de canal lógico.
- Petición de modo.
- Determinación de retardo de ida y vuelta.
- Señalización de bucle de mantenimiento.

Los mensajes H.245 se clasifican en cuatro categorías: de petición, respuesta, instrucción e indicación. Los mensajes de petición y respuesta son utilizados por las entidades de protocolo. Los mensajes de petición requieren una acción específica por parte del receptor, incluyendo una respuesta

inmediata. Los mensajes de respuesta responden a una petición correspondiente. Los mensajes de instrucción requieren una acción específica, pero no una respuesta. Los mensajes de indicación son informativos solamente y no requieren ninguna acción o respuesta. Los terminales H.323 responderán a todas las instrucciones y peticiones H.245 y transmitirán indicaciones que reflejen el estado del terminal.

Cabe mencionar, los terminales H.323 deben mantener un canal de control H.245 por cada llamada en la que el terminal esté participando. Dado que un terminal puede estar participando en forma simultánea en varias llamadas, puede tener también varios canales de control H.245 abiertos.

3.3.3.2.3. Establecimiento de la llamada Q.931.

Como parte del control de llamada de H.323, Q.931 es un protocolo de capa de enlace para establecer conexiones y entramado de datos. Este protocolo define como interactúan cada una de las capas con sus correspondientes en el otro extremo. El cual reside con el H.225.0. Provee un método para definir canales lógicos dentro de un gran canal. Los mensajes Q.931 contienen un discriminador de protocolo que identifica cada mensaje con un valor de referencia de llamada y un tipo de mensaje. La capa H.225.0 luego especifica como son recibidos y procesados estos mensajes.

3.3.3.3. Codec de audio.

Todo terminal H.323 debe obligatoriamente disponer de un codec de audio, para llevar a cabo el proceso de Compresión de Voz. Este codec debe soportar como mínimo la codificación G.711, G.723 y opcionalmente las otras admitidas por la recomendación H.323 (G.722/G.728/G.729.). El tipo de codec a utilizar al establecer una comunicación de audio con otro terminal es negociado por el Canal de Control de Llamadas, utilizando un codec en la recepción y otro diferente en la transmisión.

3.3.3.3.1 Codec G.711.

Es el estándar para enviar audio en un canal de 48, 56 y 64kbps. Muestrea la señal a 8Khz, es decir, transmitirá la banda de 0 a 4KHz de la voz. Trabaja de forma fija en PCM (Pulse Code Modulation), siendo apropiado para audio sobre conexiones de alta velocidad.

3.3.3.3.2. Codec G.723.

Este codec especifica el formato y algoritmo usado para enviar y recibir comunicaciones de voz sobre la red. Es un codec de alta velocidad que transmite audio a 5.3 y 6.3 Kbps, reduciendo el ancho de banda.

3.3.3.3.3. Codec G.722.

Como es un estándar diferencial, funciona mejor para bandas reducidas, encontrando tres velocidades: 48, 56 y 64kbps. Muestrea la señal a 16KHz, ofreciendo un ancho de banda de 8KHz. En realidad, la señal se va a dividir en dos bandas, y cada una de ellas se enviará mediante un ADPCM (Adaptive Differential Pulse Code Modulation).

3.3.3.3.4. Codec G.728.

Este codec establece codificación/decodificación de voz a 9.6, 12.8 o 16 kbps usando métodos predictivos lineales de bajo retardo. Basado en un algoritmo (LD-CELP) que realiza la codificación como variación respecto al filtro anterior.

3.3.3.3.5. Codec G.729.

Lleva a cabo la Codificación/decodificación de voz a 6.4, 8, 11.8 kbps usando métodos predictivos lineales de estructura conjugada, codificación-algebraica. Divide la señal de excitación en dos contribuciones, a través del algoritmo CS-ACELP.

3.3.3.4. Codec de video.

Un mismo terminal H.323 puede soportar a la vez varios canales de video, tanto en la transmisión como en la recepción. Asimismo, en una misma comunicación, utilizar un codec en la recepción y otro diferente en al transmisión. A través de la recomendación H.245, por el Canal de Control de Llamadas, son negociados el tipo de codec (H.261/H.263) al establecer una comunicación de video con otro terminal, la velocidad de transmisión, el formato de la imagen y las opciones de los algoritmos utilizados.

3.3.3.4.1. Codec H.261.

Es un estándar de comunicación que transmite imágenes de video a 64 Kbps (calidad VHS). Es apropiado para video sobre conexiones de alta velocidad.

3.3.3.4.2. Codec H.263.

Este codec especifica el formato y algoritmo usado para enviar y recibir imágenes de video sobre la red. Soporta codificación con cuantización por compresión, pero es acompañado de predicción y estimación de movimiento. Ofrece muy buen desempeño para transmisión sobre conexiones de baja velocidad como las de los modem de 28.8 Kbps.

3.3.3.5. Interface de datos T.120.

Los terminales H.323 pueden establecer comunicaciones de datos con otros terminales H.323. Para ello, pueden abrir canales de datos, los que pueden ser bidireccionales o unidireccionales.

La recomendación T.120 provee un estándar de interoperabilidad para el intercambio de datos entre terminales H.323. Puede usar la capa de H.225.0 para enviar y recibir los paquetes de datos o simplemente crear una asociación con la sesión de H.323 y usar sus propias capacidades de transporte para transmitir datos directamente a la red.

3.3.3.6. Protocolo de tiempo real (RTP, real time protocol).

Para ser transmitido, un fichero de audio o vídeo debe ser fragmentado, encapsulado en un datagrama y enviado. Es necesario añadir información relativa al contenido y al flujo. El protocolo RTP define una cabecera que incluye dichos parámetros, asegurando Qos para servicios de tiempo real.

RTP provee transporte (capa 4) para direcciones unicast y multicast. Por esta razón, también se encuentra involucrado el protocolo IGMP para administrar el servicio multicast. El paquete de RTP incluyen un encabezado fijo y el payload de datos; RTCP utiliza el encabeza del RTP y ocupa el campo de carga útil

Trabaja sobre **UDP** de forma que posee un checksum para detección de error y la posibilidad de multiplexación de puertas (port UDP). Las sesiones de protocolo RTP pueden ser multiplexadas. Para ello se recurre a un doble direccionamiento mediante las direcciones IP y el número de port en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz (H.32x).

Cada paquete RTP consiste en un cabezal y los datos de voz. El cabezal contiene números de secuencia, marcas de tiempo, y monitoreo de entrega.

Los campos más relevantes de la cabecera RTP son:

La identificación del payload, hace referencia al tipo de información que viaja en el paquete. Es un campo de 7 bits, lo que permite diferenciar hasta 128 tipos de información. En audio, este campo indica el tipo de codificación. Algunos valores de ejemplo se muestran en la siguiente tabla:

Payload	Formato de audio	Sampling Rate	Throughput
0	PCM mu-law	8 KHz	64 Kbps
1	1016	8 KHz	4.8 Kbps
3	GSM	8 KHz	13 Kbps
7	LPC	8 KHz	2.4 Kbps
9	G.722	8 KHz	48-64 Kbps
14	MPEG Audio	90 KHz	-
15	G.728	8 KHz	16 Kbps

La **numeración secuencial** (Sequence number), cuyo campo corresponde al número de secuencia de 16 bits. Con cada paquete enviado, el emisor incrementa en uno el número de secuencia. Esto permite al receptor detectar paquetes perdidos, o fuera de orden.

Otro factor es la **medición de tiempo** (Time Stamp), este campo es de 32 bits. Indica el momento al que corresponde la primer muestra de la ventana de información que viaja en el paquete. Este campo es utilizado por el receptor, para reproducir las muestras con la misma cadencia con las que fueron obtenidas. Es a su vez útil para medir el "jitter". En audio, el campo "Time Stamp" se mide en unidades de 125 μs.

Cabe destacar además, **Identificador del origen** (SSRC - Synchronization Source Identifier), el cual incluye un campo correspondiente de 32 bits. Típicamente cada flujo en una sesión RTP tiene un identificador diferente. El origen establece este número, asegurando que no se repita.

Y el **reporte de la calidad** (función del protocolo RTCP). Entre sus funciones se encuentran la memorización de datos, la simulación de distribución interactiva, el control y mediciones de aplicaciones.

Para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio QoS del tipo Garantizada, RTP funciona en conjunto con **RSVP** (capa 3). La QoS del tipo Diferenciada se logra mediante la priorización de tráfico que puede adoptar dos alternativas. En IP se pueden asignar diversas alternativas de prioridad para formar una cola de espera en routers.

3.3.3.7. Protocolo de control de tiempo real (RTCP, real time control protocol).

Es un protocolo basado en la transmisión periódica de paquetes de control a todos los participantes en una sesión. Utiliza el mismo mecanismo de transmisión que los paquetes de datos RTP. El protocolo subyacente, en este caso el UDP, se encarga de multiplexar los paquetes de datos RTP y los paquetes de control RTCP.

El paquete RTCP sólo contiene la información necesaria para el control de transporte y no transporta ningún contenido. Está compuesto por un encabezamiento de conjunto, similar al de los paquetes RTP que transportan el contenido, seguido de otros elementos que dependen del tipo de paquete RTCP. Se definen varios tipos de paquete RTCP, para transportar una amplia variedad de información de control. A continuación se muestran los cinco tipos más comunes de paquetes RTCP.

RR (receive report): Es enviado por los receptores y contiene información sobre la calidad de la entrega de datos, incluyendo último número de paquete recibido, número de paquetes perdidos y timestamps para calcular el retardo entre el emisor y el receptor.

SR (sender report): es enviado por el emisor y además de contener información similar a los mensajes RR, incorpora datos sobre sincronización, paquetes acumulados y número de bytes enviados.

SDES (source description items): contiene información que describe al emisor.

BYE: indica la finalización de la participación en una sesión.

APP (application specific functions): Por ahora es experimental. Está reservado para aplicaciones futuras.

Los destinatarios de los paquetes RTP devuelven información sobre de la calidad de recepción, utilizando diferentes formas de paquetes RTCP, según si ellos mismos son emisores de contenido o no. Los dos tipos, **SR** y **RR**, contienen ninguno, uno o varios bloques de informe de receptor, previstos para la sincronización de las fuentes de las cuales el receptor ha recibido un paquete de contenido RTP desde el último informe. La evaluación de la calidad de recepción no es sólo útil para el emisor, sino también para el receptor y cualquier supervisor de red que pudiera existir. El emisor puede modificar su transmisión de acuerdo con la información recibida; el receptor puede inferir si las dificultades de recepción que observa son de origen local, regional o más amplio. El supervisor recibirá solamente los paquetes RTCP, con lo cual podrá evaluar la calidad de funcionamiento de la red.

3.3.4. Fases de una Llamada H.323.

En una comunicación, de una llamada H.323 se distinguen las siguientes fases:

Inicialmente se realiza el **Establecimiento de la comunicación,** donde el usuario que desea establecer la comunicación envía un mensaje de SETUP, el remitente contesta con un mensaje de CallProcceding y Alerting indicando el inicio de establecimiento de la comunicación. Cuando el usuario descuelga el teléfono, se envía un mensaje de connect.

Posteriormente la **Negociación de los parámetros**, en cuya fase se abre una negociación mediante el protocolo H.245 (control de conferencia), el intercambio de los mensajes (petición y respuesta) entre los dos terminales establecen quién será master y quién slave, las capacidades de los participantes y codecs de audio y video. Como punto final de esta negociación se abre el canal de comunicación (direcciones IP, puerto).

La siguiente fase, dado lo anterior es la **Comunicación**: los terminales inician la comunicación mediante el protocolo RTP/RTCP. Y por ultimo la **Finalización de una llamada**, donde cualquiera de los participantes activos en la comunicación puede iniciar el proceso de finalización de llamada mediante mensajes CloseLogicalChannel y EndSessionComand para indicar la finalización de ésta.

3.4. PROPUESTA DE LA IETF PARA LA TRANSMISIÓN DE VOIP: SEÑALIZACIÓN SIP.

El protocolo SIP (Session Initiation Portocol), ó protocolo de iniciación de sesión, es un protocolo de señalización que se utiliza para establecer, modificar y terminar llamadas vocales y sesiones multimedios, a través de redes IP (redes intranet y/o Internet), como también con usuarios de las redes telefónicas por intermedio de gateways.

Para comunicaciones multimedia interactúa (especificaciones IETF), conjuntamente con otros protocolos como RTP/RTCP y SDP, pero su funcionalidad no depende de ninguno de éstos. El protocolo RTP se usa para transportar los datos de voz en tiempo real (igual que para el protocolo H.323), mientras que el protocolo SDP se usa para la negociación de las capacidades de los participantes, tipo de codificación, etc.

Se trata de un protocolo cliente-servidor similar en cuanto a sintaxis y semántica al protocolo HTTP que se utiliza en la web. Los cometidos de cliente y servidor son funcionales, es decir, un cliente puede comportarse como servidor y viceversa. Para establecer una llamada, el cliente envía

peticiones SIP al servidor y éste las recibe y avisa al usuario o ejecuta un programa para determinar la respuesta.

Además por su naturaleza, al ser un protocolo **'peer-to-peer'**, admite que en el control de la llamada puedan intervenir terceros agentes o aplicaciones, capaces de modificar los mensajes SIP que se intercambian entre los extremos de una comunicación, habilitando a través de dichas aplicaciones funciones como el desvío de llamadas entrantes en base a ciertas reglas o la transferencia de sesiones de video conferencia al ordenador personal entre otras.

El SIP define tres tipos de servidores: registradores, intermediarios y retransmisores. Un servidor registrador recibe los registros de clientes sobre su ubicación, lo que ulteriormente ayuda a localizarlos para terminar las llamadas. Un servidor intermediario reenvía las peticiones del cliente a su destino final o a otro u otros servidores SIP. Un servidor retransmisor retransmite los usuarios para que prueben otro servidor SIP que se encuentra en el siguiente tramo en la dirección del destino.

3.4.1. Arquitectura SIP.

SIP utiliza una arquitectura del tipo "Cliente-Servidor", y tiene los siguientes componentes:

Terminales SIP (SIP User Agents);

Servidores SIP (Registrar, Proxy, Redirect, Location);

Pasarelas SIP (Gateways)

3.4.1.1. Terminales SIP.

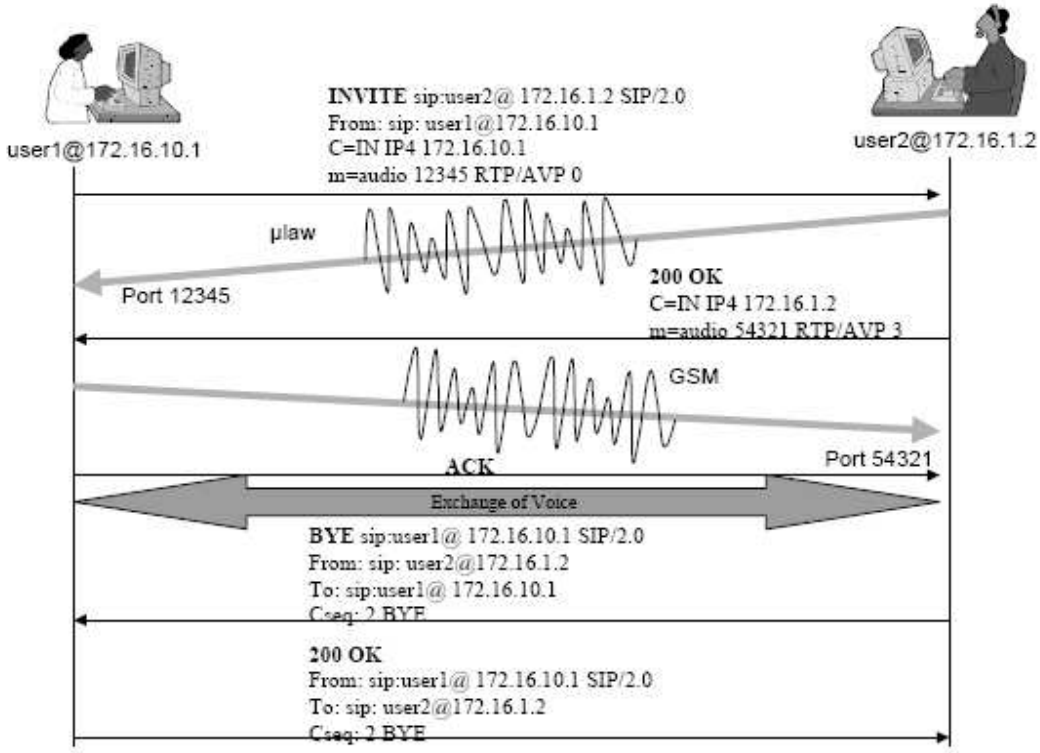
Al igual que los H.323 son teléfonos multimedia IP (terminales SIP). Estos teléfonos pueden ser aplicaciones informáticas, que utilizan las capacidades multimedia del PC (parlantes y micrófono), o terminales físicos de similar aspecto a cualquier teléfono o videoteléfono.

Los terminales SIP, llamados "**SIP User Agents**", pueden iniciar y recibir "sesiones" SIP. Cada terminal dispone de un **"User Agent Client"** (UAC) y un **"User Agent Server**" (UAS). Los UAC son los encargados de iniciar requerimientos SIP hacia otros terminales. Los UAS son quienes escuchan y atienden los requerimientos remotos. Implementado el transporte tanto sobre TCP como sobre UDP.

Estos se identifican a través de su "dirección SIP". El direccionamiento en SIP utiliza el formato de URL (Uniform Resource Locater) de Internet: sip:nombre@dominio

Los establecimientos de comunicaciones SIP se realizan mediante el intercambio de mensajes (SIP INVITE) con formato similar al http, del tipo "Request" – "Response". El componente UAC envía un

"Request" invitando a una conversación a su contraparte. El componente UAS del destino recibe el "Request", y lo contesta con el correspondiente "Response". Un ejemplo de llamada SIP se muestra en la figura a continuación:



Establecimiento de llamada SIP

El funcionamiento requiere que el usuario al iniciar la sesión se registre con su **dirección SIP,** un identificador similar a los utilizados en correo electrónico (el formato es user@domain), y su actual **dirección IP** en el registrar. En este caso, es el registrar el que mantiene la base de datos con las direcciones SIP-URI asociadas a cada dirección IP.

El establecimiento de llamada requiere el envío de un mensaje SIP INVITE destinado al proxy, quien tras contactar con distintos servidores reenvía la petición al usuario destinatario quien puede aceptar o rechazar la llamada.

3.4.1.2. Servidores SIP.

Los UAC y UAS pueden, por si solos y sin los servidores de red, ser capaces de soportar una comunicación básica (entre endpoints). No obstante, la potencialidad de SIP se aprovecha con el

empleo de los servidores de red. Los servidores de red se clasifican, desde un punto de vista lógico, de la manera siguiente:

- Redirect Server (Servidores de redirección)
- Proxy Server (Servidores proxy)
- Registrar Server (Servidores de registro)

3.4.1.2.1. Servidores de redirección.

Procesan mensajes INVITE, que son solicitudes SIP, y retornan la dirección (o direcciones) de la parte llamada, esto es, el SIP – URL (Uniform Resource Locator) de la parte llamada, o cómo contactar con ella (respuesta 3xx). De lo contrario rechaza la llamada, enviando una respuesta de error (error de cliente 4xx o error de servidor 5xx). Desarrollan una funcionalidad similar al Gatekeeper H.323, cuando se emplea el modelo de llamada directo.

3.4.1.2.2. Servidores proxy.

Se ocupan de reenviar las solicitudes y respuestas SIP para el establecimiento y liberación de llamadas de VoIP, con los medios necesarios para garantizar que los mensajes de señalización SIP de ida y vuelta sigan la misma ruta.

Un servidor proxy puede re-enviar solicitudes hasta el destino final sin efectuar cambio alguno en ellas, o cambiar alguno de sus parámetros si se requiere, por ejemplo, en el caso de las cabeceras “Via”“Record Route”.

Desarrollan el “routing” de los mensajes de solicitudes y respuestas SIP. Pueden ser “stateful” o “stateless”. Los servidores proxy **stateful** retienen información de la llamada durante el tiempo que dure el establecimiento de ésta, no así los servidores proxy **stateless**, los que procesan un mensaje SIP y entonces “olvidan” todo lo referente a la llamada hasta que vuelven a recibir otro mensaje SIP asociado a la misma. Esto se refiere al “estado” de la llamada, sin embargo, pueden mantener un “estado” para una simple transacción SIP, lo que es denominado “minimal state”. La implementación stateless provee buena escalabilidad, pues los servidores no requieren mantener información referente al estado de la llamada una vez que la transacción ha sido procesada.

Además, esta solución es muy robusta dado que el servidor no necesita “recordar” nada en relación con una llamada. Sin embargo, no todas las funcionalidades pueden ser implementadas en un servidor proxy stateless, por ejemplo, las funcionalidades relativas a la contabilización y facturación

de las llamadas puede requerir funcionalidades proxy stateful, de manera que se le pueda "seguir el rastro" a todos los mensajes y estados de una comunicación.

3.4.1.2.3. Servidores de registro.

Es un servidor que registra las direcciones SIP (SIP – URL) y sus direcciones IP asociadas, es decir, garantizan el "mapping" entre direcciones SIP y direcciones IP. Típicamente están localizados con servidores proxy o servidores de redirección.

Acepta solo mensajes de solicitud REGISTER, posibilitando el registro correspondiente a la localización actual de los usuarios, esto es, "seguir el rastro" de los usuarios, pues por diferentes razones (conexión vía ISP, usuarios móviles, conexión vía LAN con DHCP) las direcciones IP de éstos puede cambiar. También se les denomina servidores de localización (Location Server), pues son utilizados por los servidores proxy y de redirección para obtener información respecto a la localización o localizaciones posibles de la parte llamada.

Ahora bien, en rigor, los Location Server (LS) no son servidores SIP, ni entidades SIP, si no bases de datos, que pueden formar parte de arquitecturas de comunicaciones que utilicen SIP. Entre un LS y un servidor SIP no se utiliza el protocolo SIP, por ejemplo, en ocasiones se emplea entre éstos el protocolo LDAP (Lightweight Directory Access Protocol).

La información registrada en los servidores de registro, esto es, el registro del mapping de direcciones SIP correspondiente a un usuario, no es permanente, requiere ser "refrescado" periódicamente, de lo contrario, vencido un "time out" (por defecto, una hora), el registro correspondiente será borrado. Este valor por defecto del "time out" puede ser modificado según valor que se especifique en la cabecera "Expires" de un mensaje de solicitud REGISTER. En consecuencia, para mantener la información de registro, el terminal (o el usuario) necesita refrescarlo periódicamente.

Igualmente, un registro vigente puede ser cancelado y/o renovado por el usuario. Usualmente, un servidor de red SIP implementa una combinación de los diferentes tipos de servidores SIP ya comentados: servidor proxy + servidor de registro y/o servidor de redirección + servidor de registro. En cualquier caso deben implementar el transporte sobre TCP y UDP.

3.4.1.3. Gateway SIP.

Al igual que en H.323, existen pasarelas SIP hacia la PSTN y también hacia H.323. Los gateways son responsables de adaptar el audio, video y los datos, así como también la señalización,

entre los formatos propios de SIP y otras redes de telecomunicación, de manera transparente para los usuarios. En redes dónde no es necesario tener comunicación con terminales externos a la propia red, no es necesario disponer de gateways.

3.4.2. Mensajería SIP.

Los mensajes SIP, Request-Response (solicitudes-respuestas) de http, emplean el formato de mensaje genérico establecido en la RFC 822, esto es: una línea de inicio, uno o más campos de cabeceras (header), una línea vacía (indica final del campo de cabeceras) y finalmente el cuerpo del mensaje (opcional).

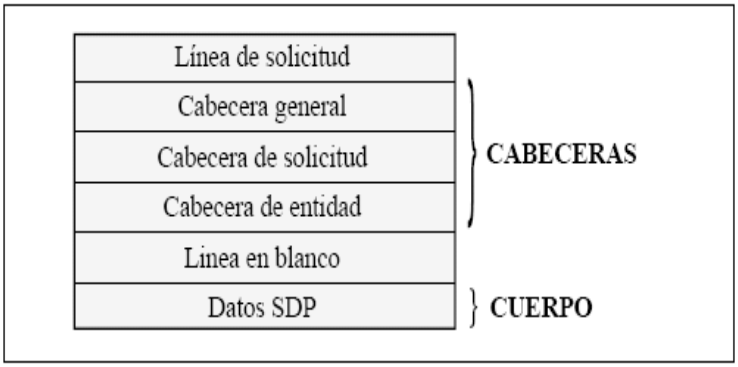
3.4.2.1. Request SIP.

Los usuarios SIP disponen de direcciones de correo electrónico similares a los URL SIP (análogos a los de http). El formato de los mensajes de solicitud es como sigue:

<Función><URL><SIP-Version>

Ej: INVITE sip:pepe@fing.com SIP/2.0

En la figura siguiente se muestra el formato general de los mensajes de solicitud o métodos SIP.



Formato general de los mensajes de solicitudes SIP.

Estos URL pueden indicar que el usuario pertenece a un dominio (sip:usuario@dominio), a un determinado computador (sip:usuario@computador), a una dirección IP de un computador determinado (sip:usuario@dirección_IP), o incluso a un número de teléfono (número E.164) accesible a través de una pasarela IP/RTPC (sip:número_teléfono@pasarela).

SIP- Versión da cuenta de la versión del protocolo SIP en uso, y se incluye tanto en mensajes de solicitud (métodos) como en mensajes de respuesta (códigos de estado).

Para ello se han definido 6 métodos para estos tipos de mensajes, los cuales son descritos a continuación:

INVITE: invita a un usuario, o servicio, a participar en una sesión. El cuerpo del mensaje contiene, generalmente, una descripción de la sesión.

ACK: confirma que el cliente solicitante ha recibido una respuesta final desde un servidor a una solicitud INVITE, reconociendo la respuesta como adecuada. Solo para reconocer solicitudes INVITE, y no otros mensajes de solicitud.

OPTIONS: posibilita "descubrir" las capacidades del receptor, las cuales pueden ser configuradas entre agentes o mediante un server SIP.

BYE: finaliza una llamada, o una solicitud de llamada. Puede ser enviado por el agente llamante o por el agente llamado.

CANCEL: cancela una solicitud pendiente, pero no afecta una solicitud ya completada. Este método finaliza una solicitud de llamada incompleta.

REGISTER: se utiliza este método como un servicio de localización que registra la localización actual de un usuario.

Los métodos que no sean soportados por servidores, Proxy o de redirección, son tratados por éstos como si se tratase de un método OPTION, y en consecuencia reenviados. Y por otro lado los métodos que no sean soportados por los servidores UAS o Registrar, provocan el mensaje de respuesta 501, "no implementado".

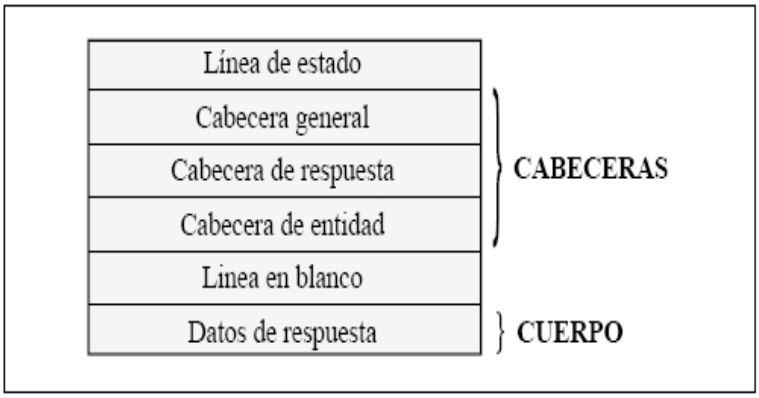
3.4.2.2. Response SIP.

Después que se recibe e interpreta un mensaje de solicitud SIP, el receptor del mismo (servidor SIP) responde con un mensaje (o varios) de respuesta (código de estado) El formato de los mensajes de respuesta es como sigue:

<SIP-Version> < Status-Code> <Reason>

Ej: SIP/2.0 404 Not Found

En la figura que se muestra a continuación, representa el formato general de los mensajes de respuesta.



Formato general de los mensajes de respuesta SIP.

El formato, comprende la versión del protocolo SIP, un código de tres enteros los cuales son interpretados por máquinas, indicando el resultado de comprender y satisfacer o no una solicitud. Y finalmente una explicación textual (Reason-Phrase) muy breve del Status Code (códigos de respuesta), para ser interpretada por las personas.

Encontrando seis diferentes tipos de Códigos de respuesta:

1xx: Informativo. Solicitud recibida, se continua para procesar la solicitud. (Ej: 180 Ringing)

2xx: Solicitud exitosa. La solicitud (acción) fue recibida de forma adecuada, comprendida y aceptada. (Ej: 200 OK)

3xx: Redireccionado. Más acciones deben ser consideradas para completar la solicitud. (Ej: 302 Moved Temporarily)

4xx: Error de cliente. La solicitud contiene mal la sintaxis o no puede ser resuelta en este servidor. (Ej: 404 Not Found)

5xx: Error de servidor. El servidor ha errado en la resolución de una solicitud aparentemente válida. (Ej: 501 Not Implemented)

6xx: Fallo global. La solicitud no puede ser resuelta en servidor alguno. (Ej: 600 Busy Everywhere)

Destacando de lo dicho anteriormente que los mensajes respuestas 2xx, 3xx, 4xx, 5xx y 6xx son “respuestas finales”, y terminan la transacción SIP. En cambio, los mensajes de respuestas 1xx`s son “respuestas provisionales”, y no terminan la transacción SIP.

3.4.2.3. Encabezado.

Las cabeceras SIP son similares a las cabeceras utilizadas en el protocolo HTTP (Hyper Text Transfer Protocol), tanto en la sintaxis como en la semántica. Se utilizan para transportar información necesaria a las entidades (SIP).

Determinadas cabeceras están presentes en todos los mensajes, otras no, solo en algunos. Igualmente, una aplicación que contenga el protocolo SIP no requiere necesariamente tener que comprender todas las cabeceras, aunque si es deseable. En el mismo sentido, si un participante SIP no entiende una cabecera, la ignora. Las cabeceras no especificadas deben ser ignoradas por los servidores. Detallándose los siguientes campos más significativos

Vía: Indica el transporte usado para el envío e identifica la ruta del request, por ello cada proxy añade una línea a este campo.

From: Indica la dirección del origen de la petición.

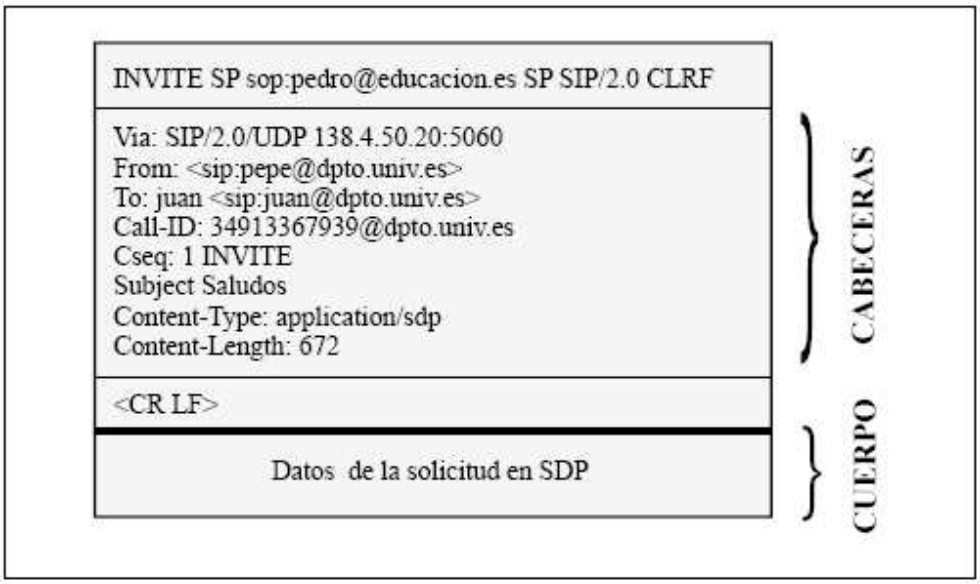
To: Indica la dirección del destinatario de la petición.

Call-Id: Identificador único para cada llamada y contiene la dirección del host. Debe ser igual para todos los mensajes dentro de una transacción.

Cseq: Se inicia con un número aleatorio e identifica de forma secuencial cada petición.

Contact: Contiene una (o más) dirección que pueden ser usada para contactar con el usuario.

User Agent: Contiene el cliente agente que realiza la comunicación.



Ejemplo de un mensaje de solicitud SIP

Generalmente, el orden en que aparecen las cabeceras no tiene mayor importancia, siempre que se cumpla que las cabeceras del tipo "salto a salto" (hop-by-hop) deben aparecer antes que cualquier cabecera del tipo "extremo a extremo" (end-to-end). Las primeras pueden ser modificadas o añadidas por los servidores proxy, en cambio las segundas deben ser transmitidas por éstos sin modificación alguna.

Una implementación mínima de SIP bebe cumplir, en relación con los elementos funcionales clientes y servidores, lo siguiente:

A nivel de **Clientes:** deben ser capaces de generar las solicitudes INVITE y ACK, así como las cabeceras Call-Id, Content-Length, Content-Type, Cseq, Require, From y To. También deben "entender" el protocolo SDP y ser capaces de reconocer las clases 1 hasta la 6 de los status code.

Y como **Servidores:** deben "entender" las solicitudes INVITE, ACK, OPTIONS y BYE. De tratarse de servidores proxy, también la solicitud CANCEL. También deben ser capaces de generar de manera apropiada las cabeceras Call-Id, Content-Lenght, Content-Type, CSeq, Expires, From, Max-Forwards, Require, To y Via.

3.4.3. Direccionamiento SIP.

Una de las funciones de los servidores SIP es la localización de los usuarios y resolución de nombres. Normalmente, el agente de usuario no conoce la dirección IP del destinatario de la llamada, sino su e-mail.

Las entidades SIP identifican a un usuario con las SIP URI (Uniform Resource Identifiers) definido en el RFC 2396. Una SIP URI tiene un formato similar al del e-mail, consta de un usuario y un dominio delimitado por una @, como muestra los siguientes casos:

usuario@dominio, donde dominio es un nombre de dominio completo.
usuario@equipo, donde equipo es el nombre de la máquina.
usuario@dirección_ip, donde dirección_ip es la dirección IP del dispositivo.
número_teléfono@gateway, donde el gateway permite acceder al número de teléfono a través de la red telefónica pública.

La solución de identificación de SIP, también puede ser basada en el DNS (descrito en el RFC 3263), donde se describen los procedimientos DNS utilizados por los clientes para traducir una SIP

URI en una dirección IP, puerta y protocolo de transporte utilizado, o por los servidores para retornar una respuesta al cliente en caso de que la petición falle.

3.4.4. Descripción de SDP (Session Description Protocol).

El protocolo de descripción de sesión (SDP, RFC 2327), se utiliza para describir sesiones multicast en tiempo real, siendo útil para invitaciones, anuncios, y cualquier otra forma de inicio de sesiones.

La propuesta original de SDP fue diseñada para anunciar información necesaria para los participantes y para aplicaciones de multicast MBONE (Multicast Backbone). Actualmente, su uso está extendido para el anuncio y la negociación de las capacidades de una sesión multimedia en Internet. Puesto que SDP es un protocolo de descripción, los mensajes SDP se pueden transportar mediante distintos protocolos con SIP, SAP, RTSP, correo electrónico con aplicaciones MIME o protocolos como HTTP.

Como el SIP, el SDP utiliza la codificación del texto. Un mensaje del SDP se compone de una serie de líneas, denominados campos, dónde los nombres son abreviados por una sola letra, y está en una orden requerida para simplificar el análisis. El SDP no fue diseñado para ser fácilmente extensible. La única manera de ampliar o de agregar nuevas capacidades al SDP es definir un nuevo atributo. Sin embargo, los atributos desconocidos pueden ser ignorados. En la tabla siguiente podemos observar todos los campos.

Tipo	Descripción	Obligatorio
V	Versión del protocolo	o
o	Identificador	o
S	Nombre de sesión	o
I	Información de la sesión	o
U	URI de la descripción	*
e	Dirección de correo	*
p	Número de teléfono	*
C	Información de conexión	*
b	Ancho de banda	*
Z	Tiempo de corrección	*
K	Clave de encriptación	*
a	Atributos	*
T	Tiempo de sesión(Start y stop)	o
R	Tiempo de repetición	*
m	Información del protocolo de transporte(media)	o

Descripción de la sesión

3.4.5. Fases de una Llamada SIP.

En una llamada SIP hay varias transacciones SIP, cuya transacción se realiza mediante un intercambio de mensajes entre un cliente y un servidor. Consta de varias peticiones y respuestas y para agruparlas en la misma transacción esta el parámetro CSeq.

Inicialmente las dos primeras transacciones corresponden al **registro de los usuarios**. Los usuarios deben registrarse para poder ser encontrados por otros usuarios. En este caso, los terminales envían una petición REGISTER, donde los campos from y to corresponden al usuario registrado. El servidor Proxy, que actúa como Register, consulta si el usuario puede ser autenticado y envía un mensaje de OK en caso positivo.

La siguiente transacción corresponde a un **establecimiento de sesión** Esta sesión consiste en una petición INVITE del usario a proxy. Inmediatamente, el proxy envía un TRYING 100 para parar las retransmisiones y reenvía la petición al usuario B. El usuario B envía un Ringing 180 cuando el teléfono empieza a sonar y también es reenviado por el proxy hacia el usuario A. Por ultimo, el OK 200 corresponde a aceptar la llamada (el usuario B descuelga).

Posteriormente en el momento que la llamada está establecida, pasa a funcionar el protocolo de transporte **RTP** con los parámetros (puertos, direcciones, codecs, etc.) establecidos en la negociación mediante el protocolo SDP.

La última transacción corresponde a una **finalización de sesión**. Esta finalización se lleva a cabo con una única petición BYE enviada al Proxy, y posteriormente reenviada al usuario B. Este usuario contesta con un OK 200 para confirmar que se ha recibido el mensaje final correctamente.

3.5. VOIP EN LA RED DE TRÁNSITO: MEGACO y MGCP.

H.323 y SIP se desarrollaron teniendo como objetivo el desarrollo de terminales que estuvieran directamente conectados a la red IP e intercambiaran tráfico de voz directamente entre sí o bien con terminales tradicionales (conectados a redes conmutadas) mediante el uso de pasarelas. El objetivo inicial de MEGACO fue la utilización de redes de paquetes como backbone para la transmisión de tráfico de voz originado por redes tradicionales. Los operadores tradicionales fueron uno de los que mayor interés han mostrado en esta propuesta, pensando en integrar progresivamente sus redes de telefonía basadas en conmutación de circuitos y sus redes de datos basadas en conmutación de paquetes en una red homogénea que transportará ambos tipos de tráfico (voz y datos) y que fuera transparente a los usuarios finales. MEGACO (Media Gateway Control)/H.248 elaborado

de manera conjunta por IETF/ITU-T, resuelve este problema dividiendo las pasarelas en tres entidades diferentes:

3.5.1. Entidades.

3.5.1.1. Pasarelas de medios (Media Gateways - MG).

Son básicamente matrices de conmutación con puertos TDM y puertos de datos, con capacidad de traducir señal TDM a paquetes IP y con funcionalidades VoIP y RAS. Según su función específica o su ubicación, los media gateways se pueden clasificar en:

MG's residenciales (entre teléfonos y red IP);

MG's troncales (entre redes PSTN y red IP);

MG's de acceso (entre PBX's y red IP).

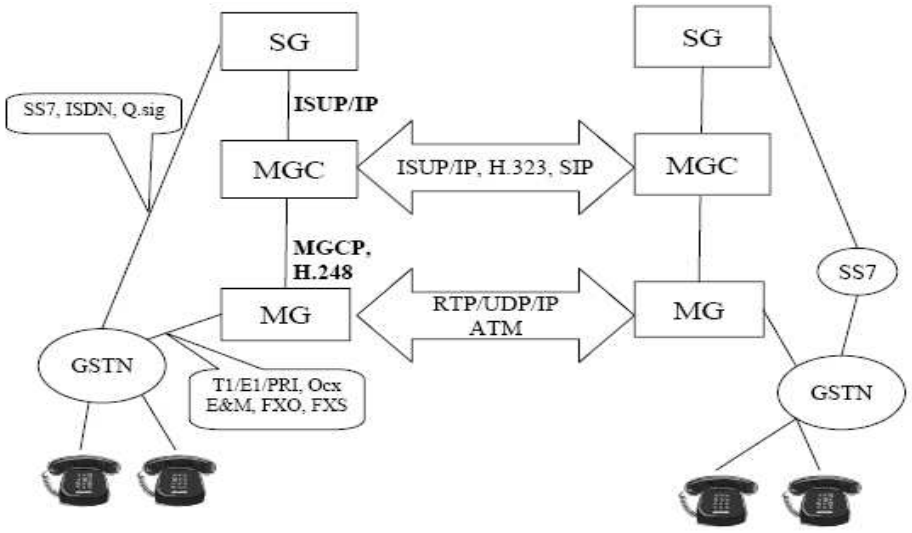
3.5.1.2. Pasarelas de señalización (Signalling Gateways - SG).

En este caso, este elemento realiza la traducción de la señalización SS7 a los protocolos de gestión de la sesión (H.323/SIP), cuyos mensajes procesa el softswitch. En ocasiones su funcionalidad la realiza directamente el media gateway o los controladores de sesión (Softswitches-SS).

3.5.1.3. Controlador de Medios (Media Gateway Controller - MGC).

Proporciona la señalización H.323 o SIP y realiza el mapping entre la señalización de redes tradicionales y las redes de paquetes.

En un escenario habitual los tres elementos están físicamente separados de modo que pueden proporcionar ventajas como la concentración de muchos MG (conectados a usuarios finales) en algunos MGC controlados por un SG. La figura a continuación muestra la arquitectura de MEGACO:



Arquitectura de MEGACO

La conexión entre endpoints (teléfonos, software, etc.), a través de las redes IP se desarrolla bajo el control de los MGC y el MG que corresponda. Toda la información generada por los endpoints se maneja por el MGC, aunque el MG puede desarrollar también este tipo de tareas

3.5.2. Protocolo MGCP (Media Gateway Controller Protocol).

Éste es un protocolo que permite comunicar al controlador de gateway MGC (también conocido como Call Agent) con las gateway de telefonía GW (hacia la PABX o PSTN). Se trata de un protocolo de arquitectura master/slave (maestro/esclavo), donde el MGC informa las acciones a seguir al GW. Los mensajes MGCP viajan sobre UDP/IP, por la misma red de transporte IP con seguridad IPsec.

El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El GW solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto. Entrega a GW la dirección IP, el port de UDP y los perfiles de RPT; siguiendo los lineamientos del protocolo SDP.

Los comandos disponibles en MGCP son:

Notifications Request, indica al GW de eventos, como ser la señalización DTMF en el extremo.

Notification Command, confirma las acciones del comando NotificationsRequest.

Create Connection, usado para crear una conexión que se inicia en el GW.

Modify Connection, usado para cambiar los parámetros de la conexión existente.

Delete Connection, usado para cancelar la conexión existente.

AuditEndpoint, usado para requerir el estado del extremo al GW.

AuditConnection, usado para requerir el estado de la conexión.

RestartInProgress, usado por el GW para notificar que un grupo de conexiones se encuentran en falla o reinicio.

EndpointConfiguration, usado para indicar al GW las características de codificación esperadas en el extremo final.

Obsérvese que los comandos AuditEndpoint y AuditConnection permiten obtener información que posteriormente forman parte de la MIB y pueden consultadas mediante el protocolo SNMP por el sistema de Management.

Como respuesta al comando DeleteConnection el GW envía una serie de informaciones obtenidas desde el protocolo RTP: número de paquetes y de Bytes emitidos; número de paquetes y Bytes recibidos; número de paquetes perdidos; jitter promedio en mseg, retardo de la transmisión.

4. CAPITULO IV. FUNCIONAMIENTO DE LA TELEFONÍA IP (TOIP).

En este capitulo se analizan los requerimientos necesarios para utilizar ToIP. Se describen las técnicas de codificación y de medición de calidad más importantes usadas en transmisión de voz en redes de datos. Posteriormente la multiplicidad de implementos que permiten la comunicación de ToIP en el mercado hoy en día, como también, la forma de implementar ToIP dependiendo del equipo terminal (fijo/móvil) en el extremo de la comunicación: PC, teléfono IP o teléfono análogo tradicional. Y finalmente se analizan los diferentes escenarios actuales de implementación, como lo son los ambientes públicos y/o privados.

4.1. INTRODUCCIÓN.

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

Hoy en día estamos siendo testigos de un cambio en el paradigma de las comunicaciones privadas en las empresas. La telefonía privada tradicional, basada en PBX o PABX (Private Automatic Branch Exchange), está siendo reemplazada por una nueva generación de soluciones estándares que permite utilizar la red de datos de las empresas para transportar las comunicaciones telefónicas.

Esta tecnología, conocida como ToIP, ofrece a las empresas un menor costo total de propiedad y la posibilidad de implementar servicios de valor agregado en una forma eficiente en costo.

El concepto original es relativamente simple: se trata de transformar la voz en “paquetes de información” manejables por una red IP. Gracias a otros protocolos de comunicación, como lo es el RSVP, es posible reservar cierto ancho de banda dentro de una red que garantice la calidad de la comunicación, así como también el protocolo RTP, el cual distribuye el tráfico en tiempo real.

La voz puede ser obtenida desde un micrófono conectado a la placa de sonido de un PC, o bien desde un teléfono común: existen gateways (dispositivos de interconexión) que permiten intercomunicar las redes de telefonía tradicional con las redes de datos.

Para poder ofrecer este servicio de ToIP se tienen dos soluciones: aumentar el ancho de banda de los canales de comunicación o comprimir la información de voz digitalizada antes de transmitirla. Aunque las dos soluciones son utilizadas, la segunda solución es la más económica y es la más usada por la mayoría de las compañías que ofrecen el servicio de voz por Internet.

Para establecer una comunicación de voz (como, de video) utilizando la red IP, lo primero que se necesita es establecer una sesión IP; a partir de ahí se digitaliza la voz y mediante técnicas de compresión se comprime para que no ocupe un ancho de banda excesivo y transmitiéndose a través de la red como si fuese un flujo de datos.

Dentro de esta telefonía se distinguen las comunicaciones **"On-Net"** y **"Off-Net"**. Las primeras son aquellas que comienzan y terminan en accesos Internet (o una Intranet) y cuyo costo es básicamente el contrato de banda ancha. Y las segundas son aquellas que comienzan en un acceso Internet y terminan en la red pública conmutada o en las redes móviles nacionales o internacionales y cuyo costo es más bajo al de un carrier. De esta forma, la comunicación se puede dar desde un teléfono IP a otro; desde un teléfono IP a un PC; desde un PC a otro PC por Internet; desde un PC hacia la red pública; desde un teléfono IP a uno analógico, etc. Para que se lleve a cabo esta última modalidad existen los gateways, aparatos que convierten la señala analógica en un caudal de paquetes de datos. Pero en relación a la telefonía IP no está todo dicho dado que se trata de una tecnología nueva, que depende en gran medida de la maduración de la infraestructura comunicacional del país.

4.2. FUNCIONAMIENTO TÉCNICO.

4.2.1. Introducción técnica.

Según los diferentes diseños que permiten construir las aplicaciones de ToIP podemos encontrar elementos tales como teléfonos IP, adaptadores para PC, hubs telefónicos, gateways (pasarelas RTC / IP), gatekeepers, unidades de audioconferencia múltiple (MCU voz), etc. El gateway es un elemento esencial y su misión es enlazar la red VoIP con la red telefónica analógica o RDSI. Se puede considerar como un dispositivo con una interfaz LAN y uno o varias interfaces analógicas.

Dentro de este contexto, existen tres tipos de llamadas de voz sobre las redes IP, encontrándonos con, llamadas de PC a PC, de PC a teléfono y de teléfono a teléfono, siendo las pasarelas (gateways) los dispositivos encargados de adaptar la telefonía tradicional al tráfico IP.

Como la ToIP, necesita un elemento que se encargue de transformar las ondas de voz en datos digitales y que además los divida en paquetes susceptibles de ser transmitidos haciendo uso del

protocolo IP. Este elemento es conocido como **Procesador de Señal Digital (DSP)**, el cual está ya disponible **y** utilizan las "Teléfonos IP" o las propios "Gateways" encargados de transmitir los paquetes IP una vez paquetizada la voz. Cuando los paquetes alcanzan el Gateway de destino se produce el mismo proceso a través del DSP pero a la inversa con lo cual el receptor podrá recibir la señal analógica correspondiente a la voz del emisor.

El proceso que se desencadena durante una llamada, se inicia en el DSP y comienza con la digitalización mediante técnica PCM de la señal de voz analógica. Posteriormente se analiza la ráfaga de bits PCM con el fin de eliminar ecos y silencios y llevar a cabo la detección de tono. Una vez hecho esto, los tonos de señalización detectados se dirigen al CODEC, el cual lleva a cabo la compresión y codificación de la ráfaga PCM. La norma G.711 genera un flujo de 64 kbps, la G.729 un flujo de 8 kbps y la G.723 uno de 6,3 Kbps (5,3 kbps según la norma estadounidense). Empleando la compresión G.729 obtenemos una calidad muy aceptable con retardos del orden de 30 mseg obteniendo tramas de 10 mseg de longitud. A continuación el Software de ensamblado de paquetes toma las tramas del CODEC y crea paquetes a los que añade una cabecera de 12 bytes correspondiente al Real Time Protocol (RTP) que proporciona un número de secuencia que sirve como marca temporal. El paquete se dirige ahora al microprocesador de la pasarela, llevándose a cabo en primera instancia el direccionamiento. Los dígitos identificados por el detector de tono del DSP se utilizan para determinar el número destino al que se le asigna una dirección IP, estableciéndose una llamada en el caso de que el destino esté libre. Al paquete se le añade una cabecera IP de 20 bytes con la dirección IP de la pasarela origen y la dirección IP de la pasarela destino. Por último, se añade una cabecera UDP de 8 bytes con los sockets de origen y destino.

Una magnitud fundamental a la hora de dimensionar un sistema de comunicaciones de ToIP es la medida del retardo. Analizando los diversos tramos de transmisión en la red IP, y utilizando una compresión según G.729, se obtienen retardos del orden de 90 mseg para cada sentido de comunicación. Teniendo en cuenta que el máximo retardo permisible para garantizar una calidad de conversación adecuada se sitúa en torno a los 300 mseg (ida y vuelta). Asegurando de esta forma que estamos dentro de los márgenes deseados.

Una vez que el paquete llega a su destino, se lleva a cabo la reproducción para la cual se eliminan en el microprocesador las cabeceras IP y UDP, se encamina el paquete al DSP donde se elimina la cabecera RTP y finalmente se desensambla el paquete dejando libres las tramas de voz.

Para preservar el resultado final relativamente libre de posibles errores que se puedan producir inherentes a la transmisión por conmutación de paquetes, los sistemas de VoIP cuentan con mecanismos de corrección de errores.

Los paquetes de voz se generan con una tasa constante mientras alguien está hablando. En cambio, los dispositivos de red, pueden provocar una cantidad impredecible de retardos entre paquetes. Estos saltos reciben el nombre de jitter y deben eliminarse en la pasarela receptora con el fin de reproducir fielmente el sonido. Para ello, en el DSP destino se utiliza un buffer adaptativo que minimiza la distorsión inducida por jitter.

Otro fenómeno común en la red debido a la congestión es la pérdida de paquetes. Cuando se produce esto, un algoritmo en el DSP lo detecta y reemplaza los paquetes perdidos por el último paquete correcto recibido disminuyendo su volumen, de este modo se evita que haya "huecos" en la trama de voz. Del mismo modo, los protocolos de transmisión para la VoIP no garantizan la recepción en el orden correcto de los paquetes por lo que al tomar éstos diferentes rutas por la red, pueden llegar desordenados. Cuando se detecta una situación de desorden, el paquete desordenado se reemplaza por su predecesor como si se hubiese perdido.

4.2.2. Componentes del sistema.

Las necesidades de equipamiento que implica cada una de las modalidades de funcionamiento varían. Cuando la comunicación es entre ordenadores, únicamente es necesario que dispongan de ciertos elementos (tarjetas de sonido, micrófono y altavoz, software de comunicación). Sin embargo, el problema es mucho mayor cuando en uno o en los dos extremos de la comunicación existe un terminal telefónico. En estos casos se hace necesario el uso de ciertos equipos, conocidos como pasarelas.

De lo anterior, los principales son:

4.2.2.1. Terminales de Usuario.

Pueden encontrarse clientes que desean utilizar sus teléfonos convencionales y aquellos que cambian hacia una ToIP integrada con su LAN. Cuando un cliente desea instalar un servicio integrado de telefonía y datos, la red LAN es donde se conectan los terminales, los elementos de interconexión al exterior (router, proxy o gateway) y el gatekeeper GK local. El servicio de ToIP puede ofrecerse sin necesidad de una LAN, por ejemplo mediante líneas analógicas que se conectan a la vieja PABX del usuario.

En el caso de utilizar la LAN, los terminales se comunican en forma bidireccional en tiempo real. Se utilizan software en la PC (SoftPhone) o teléfonos dedicados (IP-Phone). De esta forma el mismo terminal de cableado estructurado se utiliza para ambos componentes del escritorio (el teléfono y la PC). Para el caso de utilizar la vieja PABX, se requiere instalar un Gateway de usuario FXS o E1.

4.2.2.2. Gateway.

El Gateway es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red IP con la red telefónica analógica. 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:

- **FXS.** Para conexión a enlaces o a teléfonos analógicos.
- **FXO.** Para conexión a líneas de la red telefónica.
- **E&M.** Para enlaces de audio de 4 hilos.
- **BRI.** Acceso básico RDSI.
- **PRI.** Acceso primario RDSI.
- **G703/G.704.** (E&M digital) Conexión especifica a un conmutador a 2 Mbps.

Con la interface apropiada, una solución VoIP se conectará directamente al equipo de teléfono ó fax, permitiendo a los negocios de todos tamaños agregar fácilmente voz sobre IP.

La primera de las interfaces es llamada FXS (estación de intercambio remota o "foreing exchange station"), la cual se conecta directamente a teléfonos ó faxes. La interface FXO (oficina de intercambio remota o "foreign exchange office") se conecta a un PBX y proporciona accesos externos mientras que la interface E&M (interface de un dispositivo VOIP) se conecta a las líneas troncales de un PBX. Varios gateways de VoIP también ofrecen interfaces de tipo E&M.

Dentro de este contexto, el núcleo del sistema propuesto por Cisco, que es “Cisco Call Manager Express (CME), el cual consiste en un software que se instala en los routers Cisco (con soporte para voz), ejerce dentro de una multitud de servicios, la de pasarela del sistema de telefonía IP con las centralitas PBX tradicionales.

Esta es una solución ideal para empresas con necesidades inferiores a 100 usuarios. Y en caso que las necesidades de la empresa sean mayores es aconsejable utilizar CM (Cisco Call Manager).

4.2.2.3. IP-PBX (Internet Protocol-Public Branch Exchange).

Debido a que la ventaja de las IP-PBX es poder conectar un grupo de gente con otros grupos en locaciones remotas, está destinada a utilizarse en empresas u organizaciones con buen tráfico de larga distancia o en sucursales de empresas internacionales.

Una central IP-PBX es un conmutador telefónico que maneja todas las comunicaciones externas e internas por ToIP. De esta manera todos las extensiones manejadas por este equipo terminan en teléfonos IP, teléfonos comunes con ATA, o otros servidores SIP.

Otras funciones de una IP-PBX son:

- voice mail personalizado.
- ACD (automatic call distribution): coloca los llamados en colas y los rutea a los grupos. Si dentro de un grupo una extensión esta ocupada, el llamado es ruteado a la próxima extensión libre de ese grupo.
- IVR (interactive voice response): reconoce sonidos y automáticamente ejecuta una acción. Ejemplos: ayuda al ACD a reconocer los tonos de discado; interactúa con base de datos (ejemplo clásico es obtener el saldo de la cuenta bancaria por teléfono).
- Dial plan: muy importantes en centrales IP-PBX, permite automáticamente permitir/ bloquear/ reemplazar dígitos / anteponer dígitos a números discados desde las extensiones. El dial plan permite rutear llamados locales al gateway para salir a línea convencional. El dial plan es totalmente configurable.
- todas las funciones de las centrales telefónicas convencionales

Las funciones anteriores hacen que el IP-PBX sea optimo para ser utilizado como Call Center ubicados en lugares remotos.

4.2.2.4. Servidores.

El servidor provee el manejo y funciones administrativas para soportar el enrutamiento de llamadas a través de la red. En un sistema basado en H.323, el servidor es conocido como un Gatekeeper. En un sistema SIP, el servidor es un servidor SIP. En un sistema basado en MGCP o MEGACO, el servidor es un Call Agent (Agente de llamadas).

El **gatekeeper** actúa en conjunción con varios gateways, y se encarga de realizar tareas de autenticación de usuarios, control de ancho de banda, encaminamiento IP, siendo el cerebro de la red de telefonía IP.

Los **servidores SIP** actúan generalmente como varios tipos de servidores de forma simultánea (servidores de redirección, de registro y proxys). Gracias a una infraestructura de servidores SIP, es posible gestionar las llamadas de forma distribuida entre equipos personales, equipos de proveedores de servicios y pasarelas corporativas, con la consiguiente flexibilidad y control por parte del usuario, que puede mantener la privacidad de sus datos personales en todo momento.

El **Call Agente** puede actuar como punto de origen y terminación para protocolos SCN (ISUP/SS7, Q.931/DSS1). Casi toda la "inteligencia" recae en los MGC's y una pequeña parte en los G's. Por lo tanto es adecuado cuando los terminales disponen de poca inteligencia como son los teléfonos convencionales.

Dentro de la arquitectura, además encontramos los **Servidores Backend**, que corresponde a la serie de aplicaciones de backoffice que constituyen el corazón del sistema operativo de un proveedor de servicios. Poseen las bases de datos inteligentes y redundantes que almacenan información crítica que intercambian con los gatekeepers durante las fases de inicio y término de las llamadas. En el entorno de una oficina central, resulta vital preservar la integridad de los datos de las bases de datos de backend. La solución ofrece un enfoque único que garantiza la resistencia de los servidores de backend y la seguridad de sus bases de datos. Los servidores SQL (Structured Query Language) de Microsoft están integrados dentro de la arquitectura del sistema de backend y administran las bases de datos SQL para las funciones de autentificación, mapeo de directorios, contabilidad y determinación de tarifas. Este nivel de la arquitectura fue optimizado a fin de responder a las necesidades exclusivas de seguridad y disponibilidad de los proveedores de servicios. Para implementaciones a menor escala, el sistema ofrece flexibilidad para consolidar las bases de datos en un solo servidor robusto o en la plataforma de un gatekeeper.

4.2.2.5. Adaptador análogo para el teléfono (ATA).

Un Analog Telephone Adaptor es un dispositivo para conectar un teléfono estándar a un computador o a una red para que el usuario pueda hacer llamadas telefónicas por la Internet. Llamadas de larga distancia basadas en la Internet son substancialmente más baratas que las llamadas transmitidas sobre el sistema telefónico tradicional, y los ATA's son generalmente más baratos que teléfonos especializados para ToIP que se conectan al puerto USB de un computador.

Hay varios tipos de adaptadores análogos para el teléfono. Todos los ATA's crean una conexión física entre un teléfono y un computador o un dispositivo de red. Algunos efectúan

conversión de análogo a digital y conectan directamente a un servidor VoIP, mientras que otros utilizan software para cualquiera o las dos tareas.

4.2.2.6. Las nubes IP y PSTN.

Los Router conforman la "nube" IP. Son los componentes que distribuidos en la red IP permiten el enrutamiento de los paquetes entre Gateways (reemplazan a los centros de conmutación de las PSTN). La PSTN (Public Switched Telephone Network) conforma la "nube" de telefonía convencional con conmutación de circuitos.

4.2.2.7. Operadores.

Para acceder a Internet, es necesario contratar el servicio correspondiente a un **Proveedor de Servicio Internet (ISP)**. El ISP, por su parte, recurre generalmente a una **Compañía Telefónica Local** (para el caso de usuarios residenciales), para que ésta suministre la conexión física con el computador del usuario, que se establece mediante una llamada telefónica convencional (acceso conmutado a Internet), o mediante un equipo adicional que deja libre a la línea telefónica y crea una vía separada para Internet (acceso de banda ancha a Internet). Para el caso de usuarios privados o "corporativos", no se requiere de este último, debido a que la conexión física consiste en una red diseñada por la propia empresa.

Además de los dos tipos de operadores recién mencionados (ISP y Compañía Telefónica Local), en Internet existe un tercer tipo de operadores conocido como **Proveedor de Aplicaciones sobre Internet (ASP)**, tales como Yahoo, E-Bay, Hotmail o Skype, que venden o regalan sus respectivos servicios a los usuarios de Internet. Por ejemplo, RedVoiss S.A. es un "ASP" cuyo rubro principal es la prestación de servicios de ToIP. Conocidos también como ITSP, Internet Telephony Service Provider.

Para expandir el servicio de ToIP (internacional), se requiere de acuerdos entre varios ITSP. Para ello, hay que tener en cuenta los conceptos de "clearinghouse" e "interoperatividad".

Los servicios de clearinghouse son ofrecidos por proveedores de servicios de interconexión entre varios ISTP, denominados **"Proveedores de Servicios de Clearinghouse" (CSP)**, a través de los cuales, un ISTP puede generar mayores ingresos económicos, intercambiando minutos de tráfico con otros ITSP. Una vez firmado un acuerdo con un CSP, el ITSP puede terminar minutos generados desde sus clientes, más allá de su propia red de gateways y, por consiguiente, también puede terminar el tráfico generado por otros ITSP en su propia red de gateways.

Los CSP facilitan a un ITSP la ardua y costosa tarea de llegar a un acuerdo individual y bilateral con otros ITSP para terminar las llamadas en los gateways remotos de cada ISTP. Por lo tanto, el ITSP sólo tiene que negociar con el CSP, que manejará el encaminamiento de llamadas, administración de la red, autorización de llamadas y liquidación económica del acuerdo. Ejemplos de CSP son ITXC, AT&T y Arbinet.

También al margen de un CSP, los ITSP pueden intercambiar minutos de tráfico con otros ITSP. Para ello, es muy importante considerar el equipamiento necesario para ToIP. Este debe ser compatible con los estándares del mercado y, por lo tanto, asegurar una completa interoperatividad con los productos existentes.

4.2.3. Procesamiento de la voz.

En una llamada telefónica por IP, la voz se digitaliza, se comprime y se envía en paquetes de datos IP. Estos paquetes se envían a través de Internet o una Intranet a la persona con la que estamos hablando. Cuando alcanzan su destino éstos paquetes son ensamblados de nuevo, descomprimidos y convertidos en la señal de voz original.

Al comprimir la voz su calidad va disminuyendo debido a la pérdida de información que se produce en el proceso, por consiguiente mayores compresiones implican mayores pérdidas de información con mayor degradación de la voz.

Como se había mencionado anteriormente, los sistemas de ToIP utilizan algún algoritmo de compresión de audio llamado codec, siendo responsable tanto de codificar (convertir el sonido analógico recibido por el micrófono en forma digital) y decodificar (convertir el sonido codificado en su forma analógica y enviarla). Algunos codecs trabajan mejor para conexiones en bandas angostas, otros son optimizados para conexiones en diferentes velocidades.

La voz digitalizada probablemente va atravesar varios servidores antes de que llegue a su destino, así pues, debemos esperar retardos en la transmisión de voz que puede ser en fracciones de segundos y hasta varios segundos. Algunos de estos retardos dependen de las conexiones del Internet y otras del sistema de telefonía que se esté usando.

Existen múltiples estrategias para codificar una señal de voz, que se basan en algoritmos de compresión y en codificación multicanal. Entre ellos tenemos desde los más elementales, como PCM, hasta los más sofisticados, como los que utilizan técnicas de codificación híbrida, como el CELP.

PCM es el estándar de codificación de 64 Kbps aceptado internacionalmente para la transmisión de voz de calidad. Existen además otros estándares de compresión de voz como ADPCM (G.726) a 32 kbps, LDCELP (G.728) a 16 Kbps, ACELP (G.729) a 8 Kbps y MPMLQ (G.723.1) a 6,4 Kbps.

4.2.3.1. Atributos a la codificación.

La codificación de la voz se refiere al proceso de reducir la velocidad binaria de la representación digital del habla para la transmisión o almacenamiento, mientras se mantenga una calidad de habla que sea aceptable para la aplicación.

De esta manera cuando se consideran codificadores de voz es importante revisar todos los atributos. Cada uno de estos atributos está estrechamente relacionados. Por ejemplo, los codificadores de baja velocidad binaria tienden a tener mas retardo que los codificadores de alta velocidad binaria. Ellos también pueden requerir alta complejidad para implementarlos y frecuentemente poseen baja calidad en comparación con los codificadores de alta velocidad binaria.

4.2.3.1.1. Velocidad binaria.

Debido a que los codificadores de voz están compartiendo el canal de comunicación con otros datos, el pico de velocidad binario deberá ser tan bajo como sea posible para no provocar un uso inapropiado de dicho canal. Muchos codificadores de voz operan en una velocidad binaria fija independiente de las características de la señal de entrada. Dado a que los codificadores de voz multimedios comparten el canal con otras formas de datos, es mejor hacer el codificador de velocidad variable. Para aplicaciones de voz y datos simultáneos un buen compromiso es crear un esquema de compresión de los silencios como parte del estándar de codificación.

Una solución común es usar velocidad fija para habla activa y baja velocidad para ruido de fondo.

La compresión de silencio se basa en dos algoritmos principales:

- el primero es un **detector activo de voz** (VAD), el cual determina si la señal de entrada es habla o algún tipo de ruido de fondo. Si la señal es considerada como habla, ésta es codificada totalmente a velocidad binaria fija. Si la señal detectada es considerada como ruido, ésta es codificada a baja velocidad binaria;

- el segundo algoritmo, **generación de ruido confortable** (CNG), es invocado en el receptor para reconstruir la característica principal del ruido de fondo. El nombre de ruido confortable es usado ya que oído prefiere un ruido de bajo nivel que un silencio total.

Obviamente la composición del VAD es vital para la obtención de la calidad del habla. Si el habla ocurre demasiado frecuente, la potencial ganancia de la compresión de silencio no será lograda. Sin embargo para altos ruidos de fondo puede ser difícil distinguir entre el habla y ruido. Si el VAD falla para reconocer la presencia del habla, entonces el comienzo del habla puede ser cortado. Afectando seriamente la inteligibilidad del habla codificada. Por lo tanto el esquema de ruido confortable debe ser diseñado de tal manera que el codificador y el decodificador están sincronizados, aun si no hay bits transmitidos durante algún intervalo. Esto permite lentas transiciones entre intervalos de habla activos y no activos.

4.2.3.1.2. Retardo.

La tecnología actual puede ser calificada como buena, pero en ningún caso comparable a la telefonía tradicional. Se debe considerar que la voz es sensible a retardos. Sin embargo la mejora en los algoritmos de compresión, está generando una disminución en los tiempos de retardo.

El retardo de un sistema de codificación de habla usualmente consiste de tres importantes componentes. La mayoría de los codificadores de baja velocidad binaria procesan una trama de datos a la vez. Los parámetros del habla son actualizados y luego transmitidos para cada trama. Adicionalmente, para analizar los datos apropiadamente es necesario analizar el comportamiento de los datos y de la trama. Además, antes de que el habla sea analizada es necesario almacenar una trama de datos. El retardo resultante debido a los procesos anteriores se denomina **retardo algorítmico**, siendo el único componente del retardo que no puede ser reducido cambiando la implementación. La segunda mayor contribución viene del tiempo que toma al codificador analizar el habla y al decodificador reconstruir la señal de habla

Este es conocido como **retardo de procesamiento**, el cual depende de la velocidad de hardware utilizado para implementar el codificador.

La suma del retardo algorítmico y el de procesamiento es denominado **retardo de codificación del codec**.

El tercer componente es el **retardo de comunicación**, siendo el tiempo que toma una trama entera de datos ser transmitida del codificador al decodificador. La suma de los tres retardos, se denomina **retardo en un sentido del sistema**, debiendo ser menor que 200 mseg. Si hay presencia de eco, el máximo de retardo del sistema tolerable es de solo 25 mseg, esto muestra porque el uso del supresor de eco se hace necesario.

4.2.3.1.3. Medición de calidad.

La necesidad de sistemas de medición, comenzó en los años 1950 con el desarrollo del sistema de comunicación análogo. Estas técnicas fueron esenciales en la optimización de diseños de sistemas de codificación. Los constantes avances en este campo de estudio han llevado a concluir que existen diferentes métodos o formas para medir dicha calidad de servicio, clasificándose la mayoría en métodos subjetivos y objetivos.

Los métodos subjetivos de medición de calidad entregan una herramienta adecuada para este tipo de codificadores, pero producto del elevado costo de las evaluaciones, debido a los requerimientos necesarios para llevar a cabo este tipo de pruebas, hacen complicada su utilización

La forma de comparar las distintas metodologías a nivel de calidad, dependerá del tipo de codificación que se trate.

4.2.3.1.3.1. Métodos subjetivos.

Estos métodos están basados en la opinión de grupos de personas sobre la calidad de frases codificadas. Las personas son entrenadas auditivamente, para posteriormente en laboratorios con equipos altamente especializados realizar las pruebas.

Algunos de los métodos subjetivos buscan medir la inteligibilidad de los codificadores. Para ello, utilizando palabras que se pronuncien parecidas se evalúa a los codificadores. Ejemplo de este tipo de sistemas de medida son MRT (Modified Rhyme Test) y DRT (Diagnostic Rhyme Test). Sin embargo, la inteligibilidad es sólo una parte en la calidad de voz, por lo que estos sistemas de medidas son incompletos, si el objetivo es medir la calidad.

Otro tipo de metodología utilizada es entrenar a los evaluadores con señales de referencia, para evitar diferencias de criterios. Alguno de estos sistemas de medida son: MOS (Mean Opinión Score), PAR (Paired Acceptability Rating) y ACR.

De los cuales el test MOS o "puntuación en base a la opinión promedio", es el más importante y el más utilizado. Esta escala de medida está fijada por el estándar P.800 de la ITU-T.

En estas encuestas, se colocan grupos de personas a realizar evaluaciones sobre la calidad de la voz percibida, escuchando la voz reconstruida con los diferentes métodos de compresión, utilizando puntuaciones que varían en una escala de cinco valores (Excelente = 5, Buena = 4, Regular = 3, Mediocre = 2, Mala = 1) y se ponderan para obtener una taza de puntuación media.

Una de las características interesantes de destacar, es que este método es aplicable a un amplio rango de distorsiones. La desventaja que presenta el sistema de medida MOS es que los resultados pueden variar por factores como la selección de los evaluadores, las instrucciones dadas, el equipamiento utilizado, el orden en que se realiza la prueba, etc.

4.2.3.1.3.2. Métodos objetivos.

A diferencia, los métodos objetivos de medición de calidad para señales de voz se basan en comparaciones matemáticas entre la señal original y codificada. La mayoría de estos métodos utilizan medidas de distancia para cuantizar la diferencia entre la señal distorsionada y la original. Una de las ventajas de este tipo de prueba es que permite obtener un valor cuantitativo de la calidad que no depende de factores externos, como en el caso de las medidas de calidad subjetivas. Es decir, cada vez que se realice la medición se obtendrá el mismo valor. Esto permite medir variaciones pequeñas en la calidad producidos por modificaciones poco significativas en los codificadores. Si se quisiera medir estas variaciones con métodos objetivos, se tendría que utilizar un gran número de evaluadores para tener un resultado significativo estadísticamente

Los métodos más elementales de este tipo de codificadores son el SNR y la razón señal a ruido segmentada (Segmental Signal to Noise Ratio, SEGSNR), los cuales miden la razón entre la potencia de la señal y la potencia del ruido.

Una de las recomendaciones más utilizadas, basada en este método, podría bien ser el que fija la ITU-T como estándar, el P.862, que proporciona un modelo psico-acústico, denominado PESQ (Perceptual Speech Quality Measure).

El método PESQ presenta mayor exactitud que cualquier otro modelo en promedio, es altamente robusto y da predicciones exactas de calidad para un amplio rango de condiciones. Es ideal para medir efecto de pérdida de paquete, jitter, ruido ambiental y errores en transmisión de canal en codificadores como G.711, G.726, G.728, G729 y G723.1. El resultado entregado por el estándar

PESQ es normalizado a una escala similar al sistema MOS en el rango 0.5 y 4.5, sin embargo en la mayoría de los casos el rango de salida varia entre 1.0 y 4.5, rango normal para valores MOS encontrados en los experimentos de calidad subjetivos.

En consecuencia, el problema inherente a estos los métodos subjetivos, es el tiempo necesario para realizarlos, el costo y que no pueden ser usados para monitorear la calidad en períodos largos de tiempo. Esto ha hecho a los métodos objetivos atractivos para estimar la calidad percibida en redes de comunicaciones.

4.2.3.2. Codificación de la voz.

La codificación de la voz, que comprende la digitalización y la compresión de la voz, puede ser realizada mediante tres técnicas principales: por codificación de forma de onda, por codificación basada en modelos matemáticos sobre la producción de la voz y por último, en modelos híbridos que combinan ambas técnicas.

Los codificadores de **forma de onda** se basan en la codificación de la señal a partir de las muestras de la señal, reproduciendo una aproximación de la señal original a través de una serie de muestras reconstruidas que tratan de acercarse lo más posible a las muestras originales de la señal. Entre estos tipos de codificadores tenemos el PCM y el ADPCM. Dichos codificadores se basan en el teorema de Nyquist, que señala que una señal puede ser reconstruida si se muestrea a por lo menos el doble de su frecuencia máxima.

Los codificadores basados en **modelos matemáticos** no trabajan con muestras de la voz, como los codificadores de forma de onda, sino que utilizan segmentos de voz de corta duración (de 10 a 40 mseg). Por cada segmento de voz se calcula un conjunto de parámetros que lo caracteriza, convirtiendo dichos parámetros en un conjunto de bits. Estos codificadores se basan en el modelaje matemático del tracto vocal.

El tercer método de codificación es el **híbrido**, que como su nombre lo indica es una combinación de los dos anteriores.

A continuación analizaremos un poco en detalle estos codificadores.

4.2.3.2.1. PCM (modulación de impulsos codificados) o MIC.

PCM (Pulse Code Modulation), modulación por pulsos codificados, es una codificación de forma de onda que se basa en un proceso de tres pasos: muestreo, cuantificación y codificación.

4.2.3.2.1.1. Muestreo.

El teorema de Nyquist señala que si una señal es muestreada a por lo menos el doble de la frecuencia máxima de la misma, la señal puede ser reconstruida fielmente a partir de estas muestras.

Como la señal de voz está contenida fundamentalmente dentro de una banda de frecuencias entre 300 y 3400 Hz la misma se filtra para que no exista prácticamente ninguna componente de frecuencia por encima de 4 KHz, procediéndose, después de este filtraje a tomar 8000 muestras por segundo (2 x 4 KHz).

El resultado del proceso de muestreo es una serie de pulsos con una amplitud igual al valor de cada muestra (PAM, Pulse Amplitud Modulation, modulación por amplitud de pulsos).

4.2.3.2.1.2. Cuantificación.

La idea fundamental de PCM es la de convertir una señal analógica a su equivalente digital, sin embargo, el proceso de muestreo nos da una serie de pulsos cuya amplitud se encuentra en una gama infinita de valores. Para asignar una secuencia binaria diferente a cada valor de una señal que presenta una gama infinita de valores, se requeriría un código de longitud infinita.

La idea del proceso de cuantificación es la de relacionar esa gama infinita de valores a una serie de valores discretos, de forma tal de minimizar el número de valores discretos requeridos (minimizando la longitud del código), sin sacrificar de forma apreciable la calidad de la señal reconstruida.

De esta manera, se le asigna a un valor de muestra el valor discreto que más se le aproxima. Esto trae como consecuencia que la señal reconstruida no sea exactamente igual a la señal original. A esta diferencia se le denomina error de cuantificación.

En el proceso de cuantificación se trata de disminuir el error de cuantificación, tratando de que la señal reconstruida se asemeje lo más posible a la original, al mismo tiempo que se trata de minimizar la cantidad de valores discretos que se utilizan.

Por estas razones el proceso de cuantificación que se utiliza no es uniforme. Es decir, los valores discretos no se encuentran equidistantes entre sí. En la gama de valores pertenecientes a las amplitudes más bajas se asigna un mayor número de valores discretos. A medida que se acerca a la gama de valores de amplitudes más altas, el número de valores discretos asignados disminuye.

Si la gama fuera lineal, las muestras de menor amplitud tendrían un error de cuantificación porcentual (relación entre amplitud de la muestra y amplitud del error) mucho mayor que las muestras

que se encuentran en la gama de las amplitudes altas. La idea de la cuantificación no uniforme es la de que el error de cuantificación sea relativamente uniforme en todo la gama de la señal.

Adicionalmente tenemos que existe mucho mayor probabilidad de que las muestras de las señales de voz se encuentren en la gama de las amplitudes menores, por lo que se hace todavía más importante minimizar el error de cuantificación para estas amplitudes.

En América del Norte y en Japón se utiliza una cuantificación donde las muestras están espaciadas logarítmicamente, denominada ley μ. En Europa y en América del Sur se utiliza principalmente una cuantificación también logarítmica, denominada ley A.

4.2.3.2.1.3. Codificación.

En el proceso de codificación, a cada valor discreto de la muestra se le asigna un código único de 8 bits (con lo cual podemos representar 256 valores discretos diferentes).

De todo esto tenemos que, siguiendo el teorema de Nyquist, transmitimos 8000 muestras por segundo (4 KHz x 2), y dado que cada muestra está constituida por 8 bits, para transportar una señal de voz, requerimos un canal de 64 Kbps (8000 m/s x 8b/m = 64000 b/s).

4.2.3.2.1.4. Características del PCM.

La tecnología PCM se desarrolló en los años 60 y fue estandarizado por la ITU bajo el nombre de Recomendación G.711.

Esta recomendación representa el método más común de codificación de forma de onda utilizado alrededor del mundo.

Mediante el uso de la recomendación G.711 se logra transmitir una señal de voz en forma digital y reconstruirla en el destino de una forma que, para el oído humano, es esencialmente idéntica a la original.

En PCM, cada una de las muestras enviadas al codificador es totalmente independiente una de las otras, por lo que PCM permite codificar forma de ondas totalmente arbitrarias cuya frecuencia máxima no exceda la mitad de la velocidad de muestreo.

El problema de la codificación PCM es el gran ancho de banda requerido, 64 Kbps por canal de voz, por lo que han surgido nuevos tipos de codificación que han logrado reducir considerablemente este ancho de banda, sin sacrificar demasiado la calidad de la voz reconstruida.

Análisis sobre las formas de onda de la voz indican que existe una redundancia considerable entre una muestra de voz y la siguiente. El coeficiente de correlación (medida de predictibilidad)

entre dos muestras PCM de voz es de más de 0.85. De aquí tenemos que, al tomar en cuenta estas redundancias, se pueden lograr reducciones significativas del ancho de banda requerido.

4.2.3.2.2. Modulación diferencial adaptativa por pulsos codificados (ADPCM).

En ADPCM (Adaptive Differential Pulse Code Modulation,), a diferencia del PCM, no se codifica cada una de las muestras, sino que se codifica la diferencia entre la predicción de la muestra y la muestra original. Dado el alto grado de correlación entre las muestras, se pueden realizar predicciones cercanas a los valores de las muestras, por lo que se requiere enviar menos bits para indicar cuál es el error de la predicción (diferencia entre la predicción y la muestra real) que el número de bits que se requiere para enviar la muestra en su totalidad.

De esta manera, el codificador hace una predicción de la muestra a partir de las muestras previas y envía al decodificador la información que indica cuánto debe sumar (restar) a la predicción para obtener la muestra real. Por su lado, el decodificador también hace una predicción de la muestra (la cual coincide con la predicción hecha por el codificador) y le suma ó resta a esta predicción la cantidad indicada por el codificador.

Con ADPCM se muestrea la señal de voz 8000 veces por segundo (como en PCM), pero dado que se envía solamente el error de predicción, solamente se requiere transmitir 4 bits de información en lugar de los 8 que se requerirían para enviar la información de la muestra en su totalidad. Con esto se logra disminuir la velocidad de transmisión en la mitad (32 Kbps, 8000 muestras por segundo x 4bits por muestra) con respecto al PCM.

El ADPCM fue estandarizada por la ITU a mediados de los años ochenta bajo la recomendación G.721. En 1988 surgieron extensiones al G.721 (la G.723) que permiten reducir la velocidad de bits en el canal cuando la red presenta congestión. Con esta extensión se puede ajustar los bits por muestra a 3 y a 5, obteniéndose velocidades de 24 Kbps y 40 Kbps, respectivamente.

En 1990 surgió una nueva versión de ADPCM (G.726) la cual es capaz de ajustar la velocidad de bits, cambiando el número de bits por muestra de 2 hasta 5, obteniéndose velocidades entre 16 Kbps y 40 Kbps.

A diferencia del PCM, donde todas las muestras son independientes unas de otras, para estos algoritmos de ADPCM la predicción de la muestra presente depende de las muestras precedentes. De esta manera, si al utilizar PCM se pierde una muestra de la señal, la calidad de la señal se ve afectada solamente por la pérdida de esa muestra, sin embargo, si se utiliza ADPCM la pérdida de una muestra

afecta la predicción de las muestras siguientes, teniendo esto un mayor impacto en la calidad de la señal.

De PCM, se deriva el algoritmo Embedded ADPCM, definido en la recomendación G.727, el cual, provee una capacidad para asignar el ancho de banda de una manera mucho más flexible, sin requerir ningún tipo de negociación.

Por estas razones, se hace muy importante que todos los bits generados en el transmisor lleguen correctamente al receptor de forma tal de mantener la predicción de ambos equipos sincronizada.

4.2.3.2.3. Codificación predictiva lineal (LPC).

Los métodos de codificación de forma de onda discutidos previamente se basan en la representación de la señal de voz en el dominio del tiempo. LPC (Linear Predictive Coding) analiza la señal en el dominio de la frecuencia.

En gamas de milisegundos, las señales de voz no varían significativamente y esta característica es lo que permite la posibilidad de sintetizar la voz. Con este tipo de codificación, en lugar de digitalizarse la señal analógica, se digitaliza los parámetros del modelo de voz y el nivel de excitación pertenecientes a una gama pequeña de tiempo (alrededor de 20 mseg) enviando esta información al decodificador.

Básicamente, LPC divide la señal de voz en segmentos temporales de alrededor de 20 mseg. (lo que equivaldría a 160 muestras PCM). Para cada segmento el codificador calcula el filtro que ha de utilizarse para modelar el tracto vocal (a partir de la ecuación lineal y de los valores de las muestras) y le envía los parámetros que caracterizan a este filtro al decodificador. Adicionalmente le envía los parámetros que caracterizan al formante (vibración de las cuerdas vocales) presente en ese lapso de tiempo en que se está analizando la señal (frecuencia e intensidad). Con esta información el decodificador puede reconstruir la señal fuente, la cual hace pasar por el filtro, obteniéndose la voz sintetizada.

Actualmente se puede codificar la voz con LPC a velocidades entre 2.4 y 4.8 Kbps con una señal de voz reconstruida con una calidad razonable. Desafortunadamente, ciertos sonidos no se pueden reproducir fielmente con este método. La representación del tracto vocal por una serie de tubos acústicos concatenados no permite representar los sonidos nasales, los cuales, requieren una representación matemática mucho más compleja.

Adicionalmente, el modelaje del tracto vocal también conlleva a que la señal reconstruida difiera de la real, debido a las diferencias entre el modelo y el tracto vocal real.

La principal ventaja de la utilización del LPC es su capacidad de producir voz inteligible a muy bajas velocidades (entre 2,4 y 4,8 Kbps). Sin embargo, al utilizar este tipo de codificación generalmente se hace imposible reconocer, a partir de la voz sintetizada, a la persona que la origina.

La razón de esto es que las características del tracto vocal varían enormemente de persona a persona, lo cual hace el modelaje sumamente difícil. Adicionalmente, cuanto más complejo se haga el modelaje, se requieren más bits para representarlo, y por tanto las velocidades de transmisión aumentan, no viéndose justificadas la complejidad del modelo con la velocidad de transmisión obtenida.

Por otro lado, LPC basa su funcionamiento en dos tipos de sonidos: con voz y sin voz, por lo que no puede representar los otros tipos de sonidos existentes, resultando esto en la producción de una voz artificial.

Estas razones hacen que la calidad de la voz sea muy inferior a la obtenida a través de las técnicas de PCM y ADPCM.

4.2.3.2.4. Codificación por excitación lineal predictiva (CELP).

CELP (Code Excited Linear Prediction) es una técnica híbrida de codificación, donde se combinan la codificación por forma de onda y la codificación por modelaje de la voz.

La idea es tratar de obtener las ventajas de ambas técnicas. A través de la codificación por forma de onda se logra reconstruir la señal con un grado de fidelidad alto (pero utilizando un ancho de banda significativo). Por otro lado, con la codificación por modelaje logro transmitir la señal de voz utilizando un ancho de banda muy pequeño (pero con una calidad muy inferior).

Como vimos anteriormente, LPC basa su algoritmo en los sonidos con voz y los sonidos sin voz, para lo cual elimina los componentes de la voz que no se encuentran dentro de estas dos clases. La información eliminada se denomina residuo de la voz y contiene información importante que puede permitir la reconstrucción mucho más fiel de la voz.

CELP utiliza un modelo del tracto vocal muy similar al utilizado por LPC y la diferencia fundamental se basa en que, adicionalmente, CELP utiliza un libro de códigos que contiene una tabla con las señales residuo típicas. En operación, el codificador compara el residuo con todas las entradas en el libro de códigos, eligiendo la que más se parece y enviando el código de la misma. El receptor

recibe el código, y elige el residuo relacionado con el mismo, el cual utiliza para excitar el filtro. De aquí el nombre de predicción lineal con excitación por código.

De esta manera, CELP, además de enviar los parámetros que modelan el tracto vocal, la intensidad de la excitación, y la frecuencia de la formante (sonidos con voz), también envía el código que permite obtener una aproximación al residuo de la señal de voz.

En el decodificador, tanto la señal del generador de excitación (con los valores de intensidad y frecuencia indicados por el codificador) como la señal reconstruida del residuo (obtenida a partir del libro de códigos y del código enviado por el codificador) se pasa a través del filtro que modela el tracto vocal (construido a través de los parámetros enviados por el codificador), obteniéndose así la reconstrucción de la voz.

Con esta codificación se logra obtener una calidad mucho mayor a la obtenida con LPC sin sacrificar mucho ancho de banda adicional (velocidades entre 4.8 y 16 Kbps).

4.2.3.2.5. Codificación CS-ACELP.

La codificación CS-ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction, predicción por excitación lineal de código algebraico de estructura conjugada) fue estandarizada por la ITU en Noviembre de 1995 bajo la recomendación G.729. Con la utilización de esta recomendación se codifica la voz a 8 Kbps.

Esta codificación opera con segmentos de voz de 10 mseg, correspondientes a 80 muestras PCM. Cada 10 mseg se analiza la señal de voz y se extrae los parámetros del modelo CELP.

La característica principal de CS-ACELP es que las entradas del libro de códigos ya no vienen dadas por un conjunto de valores que caracterizan las formas de onda de los residuos, sino que dichas formas de onda son representadas por un conjunto de ecuaciones algebraicas.

Los procesadores de señales digitales manipulan con mucha mayor facilidad las formas de onda de los residuos cuando estos son representados como funciones matemáticas que cuando estas son representadas por un conjunto de valores.

CS-ACELP utiliza dos libros de códigos, uno fijo y otro adaptable. El libro fijo contiene formas de onda preestablecidas, las cuales no varían. En el libro adaptable, las formas de onda se van adaptando a las señales reconstruidas, permitiendo con esto que la reconstrucción de la voz se vaya ajustando a las características de la misma, obteniéndose con esto una mayor fidelidad.

Como vimos antes, G.729 utiliza segmentos de voz de 10 mseg. Adicionalmente, el cálculo de los coeficientes del filtro se basa no solamente en las muestras tomadas durante esos 10 mseg, sino

que también toma en consideración las muestras de los 5 mseg siguientes, teniéndose con esto un retardo del algoritmo de 15 mseg.

4.2.3.2.6. Codificación LD-CELP.

LD-CELP (Low Delay CELP, CELP de bajo retardo) fue estandarizado por la ITU en 1992 bajo la recomendación G.728.

Con esta codificación ya no se transmite los parámetros del filtro, la frecuencia y amplitud de la excitación y el código del residuo, sino que se transmite el código de la excitación. Realmente, se transmite aquél código que, al pasarlo por un filtro adaptable, genera la señal más similar a la señal de entrada (el menor error). En el decodificador, los parámetros que caracterizan al filtro son calculados a partir de los segmentos previos de voz reconstruida.

Esta codificación opera con segmentos de voz de 0,625 mseg, correspondientes a 5 muestras PCM. Por cada segmento de voz, el codificador analiza entre los 1024 vectores de su libro de códigos para encontrar la forma de onda del mismo que más se aproxime a la excitación de entrada (el que minimiza el error medio cuadrático compensado en frecuencia con respecto a la señal de entrada). Los 10 bits correspondientes al vector del libro de código seleccionado son enviados al decodificador. De esta manera, cada 0,625 mseg el codificador envía 10 bits, lo que da una velocidad de 16 Kbps.

En la práctica, 7 bits son utilizados para representar 128 formas de onda patrón y los otros bits se utilizan para indicar la amplitud de la señal. Sabiendo que una señal analógica puede poseer una variedad infinita de valores la selección entre 1024 posibilidades se ve muy débil, y realmente lo sería si esta selección fuera estática. Sin embargo, esta selección no es estática, como en ninguna de las codificaciones CELP. Justamente la reputación de altamente compleja que posee la codificación CELP viene dada de la actualización constante de los libros de código y de los filtros, a partir del pasado reciente de la señal de entrada.

Esta codificación presenta un retardo de algoritmo de apenas 0,625 mseg, el cual es bastante bajo sobre todo si se lo compara con el de la recomendación G.729, el cual posee un retardo de algoritmo de 15 mseg. (Un retardo 24 veces mayor).

Al acumular solamente 5 muestras PCM para procesar el segmento de voz (en lugar de 80 para G.729) se logra tiempos de acumulación mucho menores que reducen el retardo del algoritmo, y, adicionalmente, resultan bloques de información más pequeños que se procesan de una manera mucho más rápida.

4.2.3.3. Calidad de la compresión de voz.

Con los métodos de compresión de voz se logra reducir el ancho de banda requerido para transmitirla, permitiendo reconstruirla en el destino. Sin embargo, la forma de onda reconstruida es una aproximación a la forma de onda generada, no siendo exactamente igual a la que se generó, y por tanto, se observan pérdidas en la calidad de la misma.

Cada uno de los métodos de compresión explicados posee diferentes algoritmos de compresión y reconstrucción de la señal, aproximando la señal que se originó de manera diferente y percibiéndose la voz reconstruida de manera diferente para cada uno de estos métodos.

Una manera en que se evalúa la calidad que se percibe en la voz reconstruida es a través de la encuesta MOS.

En la tabla a continuación se muestra la evaluación MOS de diferentes métodos de compresión.

Método de compresión	Velocidad requerida	MOS
PCM (G.711)	64 Kbps	4,4
ADPCM (G.726)	32 Kbps	4,2
LD-CELP (G.728)	16 Kbps	4,2
CS-ACELP (G.729)	8 Kbps	4,2
MPMLQ (G.723.1)	6,3 Kbps	3,98
ACELP (G.723.1)	5,3 Kbps	3,5

Dadas estas evaluaciones, se considera la gama entre 4 y 5 como de muy buena calidad, la gama entre 3 y 4 como calidad adecuada para ser utilizada en los sistemas de telecomunicación (obteniéndose una buena calidad, reconociéndose a la persona que habla y lográndose una voz reconstruida que se percibe natural), y entre 1 y 3 como calidad sintética (donde no se reconoce a la persona que habla, y la voz reconstruida no se percibe de manera natural).

Observándose como con ADPCM, LD-CELP, y CSACELP se percibe la misma calidad de la voz reconstruida, con PCM la calidad es algo superior (aunque no de manera significativa), y con MPMLQ la calidad es algo inferior (aunque tampoco de manera significativa). Con el método de la tabla con que se obtiene la menor calidad es con G.723.1, cuando se utiliza en la modalidad ACELP, sin embargo, dicho método se encuentra dentro de la gama que se considera adecuado para las telecomunicaciones.

4.2.4. Seguridad de los servicios de ToIP.

Como la ToIP consiste, en definitiva, en datos que viajan por la red, en cuanto a seguridad tiene los mismos riesgos que el resto de los datos que viajan por ella pero también puede tener la misma protección.

La **"seguridad"** de los servicios telefónicos por IP requiere por lo menos de confidencialidad y disponibilidad. Actualmente hay varios tipos de ataques (DoS, Eavesdropping, hijack) que son producidos por deficiencias en el protocolo TCP/IP. Los dispositivos de redes, los servidores y sus sistemas operativos, los protocolos, los teléfonos y su software, todos son vulnerables.

Dado lo anterior, la minimización de los riesgos de confidencialidad, disponibilidad, Integridad y la posibilidad de lograr algún grado de autenticación se logra por medio de la **"Encriptación"**, que es el mecanismo más óptimo para prevenir ataques. Se puede llevar adelante por medio de:

- VPN (Virtual Private Network);
- IPsec (Internet Protocol Security);
- SRTP (Secure Real-time Transport Protocol);

Y adicionalmente, se pueden emplear:

- **Firewall;** y
- **Tecnología IDS/IPS** (Intrusion Detection/Protection Systems).

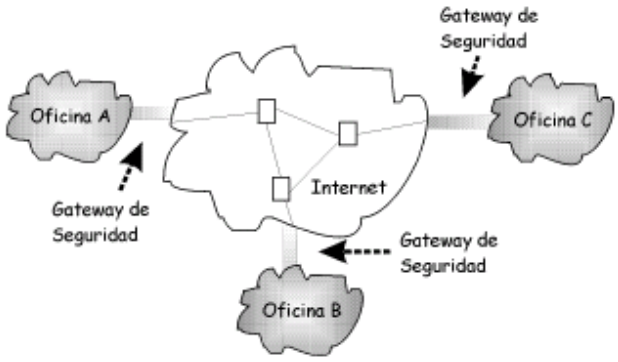
4.2.4.1. VPN (Virtual Private Network).

Una VPN o "red privada virtual" es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autentificación criptográfica. Una VPN es virtual porque no es físicamente un red distinta, es privada porque la información que transita por los túneles es encriptada para brindar confidencialidad, y es una red porque consiste de computadoras y enlaces de comunicación, pudiendo incluir enrutadores, switches y gateways de seguridad.

Esta tecnología punto a punto, es ampliamente adoptada en ambientes de transacciones financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN, la figura siguiente se ilustra un ejemplo de interconexión de oficinas sucursales de un corporativo, interconectadas vía VPN usando la Internet como dorsal de su red. Cada oficina tiene

un gateway de seguridad que provee una interfaz con Internet y la red interna del corporativo. Los gateways de seguridad se configuran para definir las políticas de control de acceso para cada oficina.

Las VPNs tienen cierto nicho de aplicación, en ambientes punto a punto que requieren canales seguros de forma permanente (telefonía IP, por ejemplo).



Ejemplo. VPN interconectando las oficinas A, B, y C, utilizando a la Internet como backbone de su red.

Por ello, los servicios de seguridad de IPSec (Internet Protocol Security) son ampliamente utilizados para la implementación de VPNs, así como también, otra solución para la confidencialidad e integridad del tráfico, es MPLS (Multi Protocol Label Switching). Las VPN basadas en IPSec y MPLS representan el siguiente nivel de la tecnología WAN, permitiendo la creación de redes multiservicio capaces de transportar cualquier tipo de tráfico.

4.2.4.2. IPSec (Internet Protocol Security).

IPSec o "protocolo de seguridad IP" es un conjunto de extensiones al protocolo IP. Es un estándar de la IETF (Internet Engineering Task Force) definido en el RFC 2401, diseñado para proveer seguridad interoperable de alta calidad basada en criptografía, tanto para IPv4 como para IPv6. Provee servicios de seguridad como autenticación, integridad, control de acceso y confidencialidad. Es implementado en la capa de Red, de tal forma que su funcionamiento es completamente transparente al nivel de aplicaciones, y es mucho más poderoso. IPSec provee un mecanismo estándar, robusto y con posibilidades de expansión, para proveer seguridad al protocolo IP y protocolos de capas superiores.

Es considerado una excelente opción para implementar VPN (Virtual Private Networks), de hecho se le conoce también como el protocolo VPN. Soporta dos modos de encripción: **Transport y Tunnel**. El "modo Transport" encripta solamente la porción de datos (carga) de cada paquete, pero no

toca el encabezado. En cambio, el “modo Tunnel”, más seguro, encripta tanto el encabezado como la carga del paquete. Del lado del receptor, un equipo compatible con IPSec decodifica cada paquete. Para que funcione el IPsec, los dispositivos emisores y receptores tienen que compartir una clave pública. Esto se logra mediante un protocolo conocido como **Internet Security Association and Key Management Protocol/Oakley** (ISAKMP/Oakley), el cual le permite obtener al receptor una clave pública y autenticar al emisor usando certificados digitales.

4.2.4.3. SRTP (Secure Real-time Transport Protocol).

Igualmente, para la protección de la conversación puede lograrse utilizando, el protocolo SRTP (Secure Real-time Transport Protocol), definido por la RFC 3711. Es una extensión del perfil de RTP (Real-time Transport Protocol), que incorpora confidencialidad encriptando el campo de voz del paquete, así como un mecanismo para comprobar la integridad del mensaje, es decir que no haya sido alterado en lo más mínimo y protección de reenvío para flujos (audio y/o video).

4.2.4.4. Firewall.

Es un sistema o grupo de sistemas que refuerzan la seguridad en las redes corporativas o proveedores de servicios con protocolos IP. El firewall determina los servicios que pueden ser accedidos desde el exterior de la red (desde la conexión a Internet). Todo el tráfico debe pasar por el firewall para ser inspeccionado.

El módulo de firewall instalado como un software sobre el router o servidor de acceso permite realizar las siguientes funciones:

- **Control de acceso.** Es el principal objetivo del firewall. Crea un perímetro de defensa diseñado para proteger las reservas corporativas. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es: "todas las conexiones son denegadas a menos que estén expresamente autorizadas".
- **Logging.** Es el inicio de las conexiones entrantes y salientes. El uso de un sistema proxy y cache incrementa la velocidad de respuesta de estas operaciones.
- **Traslación de direcciones.** Permite realizar las funciones de **NAT** (Network Address Translator) asegura la supervisión de la información de entrada y salida. El NAT permite aliviar la escasez de direcciones IP y eliminar la necesidad de renumeración cuando se realiza un cambio de ISP.

- **Autentificación.** El proceso de autentificación involucra a 3 componentes: el servidor, el agente y el cliente.
- **Reportes.** El firewall ofrece un punto conveniente para monitorear (Audit and log) y generar alarmas.

El firewall genera dos áreas en una red: el área pública con facilidad de acceso desde el exterior (para visita de Web, por ejemplo) y el área interna, detrás del firewall que se encuentra protegida contra la penetración no deseada. El perímetro de defensa se denomina zona desmilitarizada **DMZ** (De-Militarized Zone) y puede ser accedida por un cliente externo. El firewall puede trabajar sobre un server o sobre un router. La ventaja es que se concentra esta acción en un centro de la red consolidado en lugar de estar distribuido en cada host. Esta acción es más útil cuando es llevada a cabo por el router de entrada a la red. Por otro lado, ofrece un punto óptimo para instalar el Web y Server de FTP.

Al comunicarnos con usuarios externos a la red LAN, en ToIP, es casi seguro que este firewalls no permitirá establecer la comunicación. Esto es porque los protocolos SIP y RTP son nuevos, y la mayoría de los firewalls no permiten tráfico SIP y RTP.

Algunas formas de resolver problemas de firewall son:

- Permitir en el firewall tráfico SIP y RTP abriendo el puerto 5060 para paquetes TCP y UDP.
- Abrir un rango de puertos UDP para RPTP. Configurando los PC de la red para que utilicen el rango de puertos que se configuró.
- Deshabilitar el NAT.
- Reemplazar el firewall por versiones que permitan el protocolo SIP.

Acotar los puertos TCP/UDP de un teléfono IP (hardware), resulta sencillo al ser un equipo dedicado, pero en los clientes software el rango de puertos es dinámico ya que hay múltiples aplicaciones sobre el mismo equipo utilizando recursos de red.

En la práctica, en el caso de utilizar un firewalls **"packet filtering"**, se deben indicar todos los puertos que serán utilizados, ya que la función que realiza es la de simple filtrado de paquetes según reglas. En cambio cuando se dispone de un firewalls **"stateful inspection"** se puede simplificar el problema. Este tipo de firewalls es capaz de analizar y mantener las conversaciones, identificando protocolos como H.323 o SIP. Donde en este caso no sería necesario definir todos los puertos

utilizados dinámicamente ya que el propio firewalls los puede obtener al analizar el cuerpo de los mensajes y establecimiento de llamadas.

4.2.4.5. Tecnología IDS/IPS (Intrusion Detection/Protection Systems).

La implementación de esta tecnología es otra de las opciones a la problemática de seguridad de los elementos que intervienen en los servicios de ToIP.

El sistema de detección/protección de intrusos (IDS/IPS) es un programa usado para detectar y/o prevenir accesos desautorizados a un PC o a una red. Están basados en una arquitectura para detección y prevención, en tiempo real, de intrusos de redes. Integra técnicas de análisis de firmas, anomalías del trafico de red e intentos de Denial of Service (DoS), permitiendo la detección y prevención precisa e inteligente de ataques en alta velocidad

El **Sistema de Detección de Intrusos o IDS** (Intrusion Detection System) detecta y registra los ataques comunes y otras actividades sospechosas, por toro lado como **Sistema de Prevención de Intrusos o IPS** (Intrusion Prevention Systems) controla los paquetes de datos de entrada o salida en busca de transferencias de datos o métodos de transferencia sospechosos y reacciona de forma activa evitado este tipo de amenaza.

4.3. TIPOS DE LLAMADAS EN FUNCIÓN DEL TERMINAL UTILIZADO.

4.3.1. Soporte de clientes.

Dadas las características de las soluciones de la ToIP, existen dos tipos de clientes de este Servicio, los clientes de Software y los de Hardware.

4.3.1.1. Cliente de Hardware.

Es todo dispositivo físico que accede directamente a la Red de ToIP mediante el cableado de red LAN, ya sea por tener una interface nativa de Red (IP Phone, o teléfonos IP) o mediante un dispositivo adaptador (ATA). Además debe prestar todas las funciones de un teléfono estándar.

CISCO, IP Phone

CICO, ATA

La principal diferencia entre un teléfono convencional y un teléfono IP es que el segundo, es un dispositivo que cuenta con inteligencia propia para múltiples procesos que tramita con el Servidor de Llamadas (SoftSwitch). En este servidor es donde los protocolos de señalización residen.

Estos IP Phones, permiten la autorización de uso por medio de un usuario y clave, facilitando la movilidad. Esto quiere decir, que si un empleado necesita cambiarse de oficina, no requiere de un técnico que configure la central para asignarle su actual interno a la nueva oficina. Con sólo ingresar su usuario y clave en el teléfono, la central IP se encarga de reasignar su interno, mensajes de voz y configuración actual, a la nueva oficina.

Además, se amplían las ventajas de las comunicaciones IP, mediante "IP Phones" inalámbricos, eliminando la necesidad de realizar cableado tanto de datos como de voz.

4.3.1.2. Cliente de Software.

En vez de disponer de un teléfono multilínea al lado del PC, la ToIP admite la instalación de software en su PC que hace las funciones de un "soft-phone". El software, a diferencia del hardware telefónico, se implementa y actualiza en poco tiempo, sin interrupción de trabajo y sin costo en equipamiento.

Esta aplicación se instala en un computador y permite utilizar el acceso de red de la estación y sus recursos multimedia para acceder a la Red de ToIP, mediante el uso de un protocolo de transmisión de voz paquetizada (H.323/SIP).

CISCO – SoftPhone

NORTEL – SoftPhone

Debido a que se busca optimizar los recursos y disminuir los costos, es importante que la solución escogida soporte el uso de estos clientes para garantizar el crecimiento en usuarios así como de el aprovechamiento de la infraestructura física a ser instalada (cableado estructurado). El manejo de un solo tendido de cableado para aplicaciones de voz y datos es fundamental para justificar una integración inicial con la Telefonía Tradicional y una migración paulatina a una solución basada en la ToIP.

Dentro de las soluciones existentes, las que incluyen clientes Hardware, algunas son:

- CISCO, Teléfonos IP Cisco.
- 3COM, Teléfonos IP 3Com y Teléfonos Análogos con adaptador IP.

Las que incluyen clientes de Software son:

- Ericsson, utilizando MS Netmeeting.
- NORTEL, programando una aplicación.
- 3COM, utilizando su aplicación NBX IP Software.
- CISCO, utilizando su aplicación SoftPhone.

4.3.1.3. Distintas Soluciones.

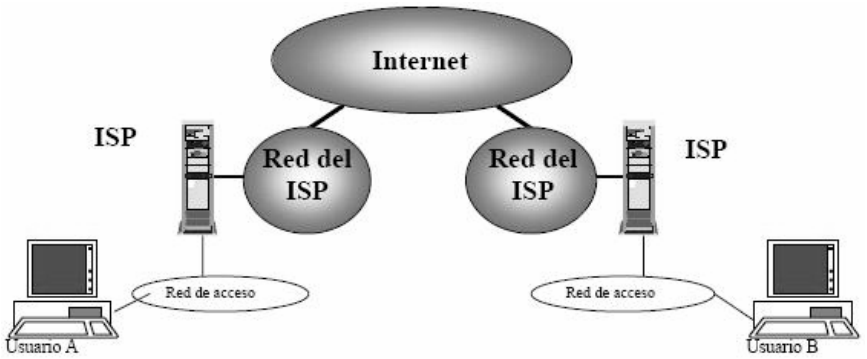
Las soluciones de implementación son variadas, está lo que se llama “modelo híbrido”, que incluye la comunicación con la red pública de telefonía mediante un dispositivo que transforma los

paquetes IP en señales que viajen a través de los cables de cobre, este tipo de modelo necesita de las dos redes, la de telefonía tradicional (PSTN) y la red IP. El modelo híbrido integra el uso de teléfonos IP y teléfonos analógicos. El otro modelo es el de "ToIP pura", que contempla una sola red y el uso de teléfonos IP únicamente.

En la actualidad existen tres variantes para la prestación del servicio. La primera de ellas consiste en una comunicación entre computadores personales, que requieren estar conectados y activos simultáneamente (este tipo de llamadas siempre son gratis). La segunda se produce entre un computador y un equipo telefónico convencional, caso en el cual sólo el usuario que utiliza el computador debe estar conectado a la red IP, ya que por la naturaleza de la RTC el usuario que utiliza un equipo telefónico tiene acceso permanente a ella (gratis en algunas ocasiones, depende del destino). Finalmente, la tercera y más novedosa variante es la que se produce entre dos usuarios que utilizan equipos convencionales conectados a la RTC, pero en que el transporte se realiza parcialmente a través de una red IP (llamadas por lo general muy baratas).

4.3.2. Llamada de PC a PC.

En este escenario, ambas partes (emisor/receptor) disponen de computadores que les permiten conectarse a la red Internet, por lo general a través de la red de un proveedor de servicio de Internet (ISP), o en otro caso como parte de una red LAN o WAN, sin la intervención de un ISP. La comunicación vocal se produce sólo mediante acuerdo previo, ya que ambos usuarios tienen que estar conectados a Internet al mismo tiempo (para lo cual habrán fijado con anterioridad la hora en la que se comunicarán a través de Internet, a menos que se encuentren en línea permanentemente) y utilicen software compatible con VoIP.



Asimismo, el llamante debe conocer la dirección IP de la parte llamada; para ello, las partes deben ponerse de acuerdo para consultar un servidor de directorio en línea (que se actualiza con cada conexión) en el cual se registran los usuarios antes de cada comunicación o deben disponer de otras formas para localizarse o tener conocimiento de la disponibilidad de la conexión de su corresponsal a Internet (tecnologías de mensajería instantánea).

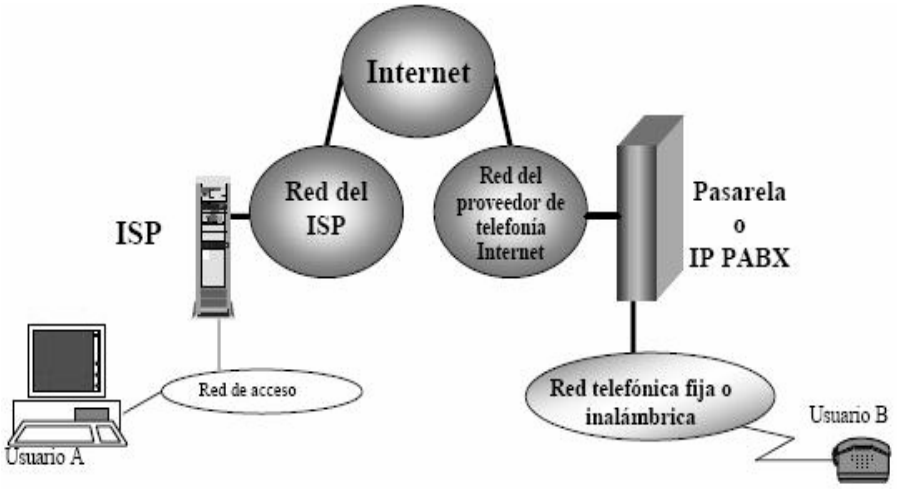
Normalmente, el cometido del ISP se limita simplemente a proporcionar acceso a la red, lo que a su vez permite que el usuario acceda a Internet. La aplicación vocal que emplea el cliente es transparente para el ISP, que no toma medidas específicas para garantizar la calidad del servicio vocal. En pocas palabras, en tal escenario no puede hablarse de "telefonía" en el sentido convencional de la palabra, es decir la prestación de un servicio por un tercer proveedor, sino simplemente de la utilización de una aplicación vocal a través de Internet, utilización que se ha vuelto tan común como cualquier otra aplicación de red. A menudo, el protocolo utilizado entre las dos partes en comunicación es el protocolo H.323; no obstante, el protocolo SIP podría tener una utilización más generalizada en el futuro.

Todos los productos de softwares orientados a telefonía que están disponibles en el mercado tienen una estructura similar, ya que muestran un panel de control a partir del cual pueden controlarse las principales funciones de telefonía y pueden consultarse los menús de configuración y de opciones. Proporcionan acceso a las zonas de charla interactiva Internet (IRC), donde los usuarios pueden intercambiar mensajes de texto en tiempo real, para cuyo fin se visualiza una lista de los individuos que utilizan el mismo software y se encuentran en línea. Según el producto, también hay un menú que permite al usuario llamar a una dirección IP específica que es permanente y corresponde a una máquina que ya está conectada a la red. Algunos productos pueden incluir el cifrado de la comunicación vocal. Una opción de correo vocal facilita que los mensajes vocales sean grabados por la máquina.

Los típicos servicios de comunicaciones de este tipo son los ofrecidos por MSN Hotmail, MSN Yahoo y Skype.

4.3.3. Llamada de PC a teléfono y viceversa.

En este caso, uno de los usuarios dispone de un computador con el cual se conecta a Internet a través de una red de acceso y un ISP, en tanto que el otro usuario es un abonado normal a una red telefónica fija o móvil.



4.3.3.1. Llamada de PC a teléfono.

Cuando el usuario con computador desea llamar al aparato telefónico de un corresponsal, debe empezar conectándose a Internet en la forma tradicional a través de la red de su ISP. Una vez conectado, emplea los servicios de un proveedor de servicio de telefonía Internet (ITSP) que dispone de una pasarela que garantiza el acceso al punto más cercano a la central telefónica del abonado llamado. Dicha pasarela será la que se encargue de la llamada de la parte llamante y de toda la señalización relacionada con la llamada telefónica en el extremo de la parte llamada.

Cabe observar que el ITSP presta un servicio unidireccional de PC a teléfono y no gestiona a los abonados como tales; de hecho, el abonado con PC emplea los servicios del ITSP únicamente para las llamadas salientes. Cabe notar además que el ITSP dispone de una red IP gestionada y en consecuencia garantiza una determinada calidad de servicio vocal hasta la pasarela más cercana al abonado llamado, y que asimismo gestiona la interconexión con el operador telefónico de este último. Pese a que los ITSP utilizan tecnología VoIP, se consideran a sí mismos como proveedores de servicio telefónico y por lo general prestan sus servicios a individuos de la manera convencional, es decir, con tasación por minuto.

Ejemplos de comunicaciones de este tipo son los ofrecidos por Net2phone y Skype Out.

4.3.3.2. Llamada de Teléfono a PC.

En este caso, la parte llamante es el usuario telefónico y la parte llamada es el usuario con un PC. Como un usuario telefónico puede marcar esencialmente un número E.164 para establecer

comunicación con la parte llamada, el usuario con un PC debería disponer de alguna manera de un número E.164:

- indirectamente: en el caso de su interconexión a la red como abonado de una centralita privada automática (PABX) con tecnología IP conectada a la red pública (en realidad, en este caso cabría hablar más apropiadamente de un "teléfono IP" en lugar de un PC conectado a la red LAN gestionada por la PABX IP);
- o directamente: en este caso, se trata del abonado del lado IP que tiene una dirección E.164 atribuida por un operador de ToIP.

Técnicamente este último caso, funcionará dependiendo de la disponibilidad de un mecanismo de traducción intermediario implantado por el lado IP que pueda traducir el número E.164 público a la dirección IP de la parte llamada. Este mecanismo estará disponible sólo en función de la aplicación de una tecnología como ENUM.

La norma **ENUM (Electronic NUMbering)**, descrita en la RFC2916 del IETF, define un protocolo y una arquitectura basada en el sistema de nombres de dominio (DNS o Domain Name System) de Internet, que permite obtener una correspondencia entre los números de teléfono E.164 y los identificadores de servicio de llamada. De modo que a través de un número E.164 (que es único para cada usuario) como alias, se pueda localizar cualquier usuario final, con independencia de que se encuentre disponible a través de uno o varios terminales H.323, SIP, RTC o RDSI.

La utilidad de ENUM en un entorno VoIP (H.323 y SIP) se fundamenta en la existencia de una entidad. En el modelo H.323, esta entidad se corresponde con el "gatekeeper". En el modelo SIP, se corresponde con el "proxy".

Estas entidades (gatekeeper y proxy) procesan las respuestas del DNS y obtienen la URI necesaria para contactar con el usuario asociado al número E.164 marcado. Además, si fuera necesario, se encargan de desviar la llamada hacia la pasarela adecuada para que la llamada siga su curso. Por tanto, será necesaria la incorporación de nuevas funcionalidades para que dichas entidades sean capaces de interaccionar con el DNS.

Para encontrar el nombre DNS a partir de un número de teléfono E.164, la norma RFC2916 requiere ejecutar los siguientes pasos:

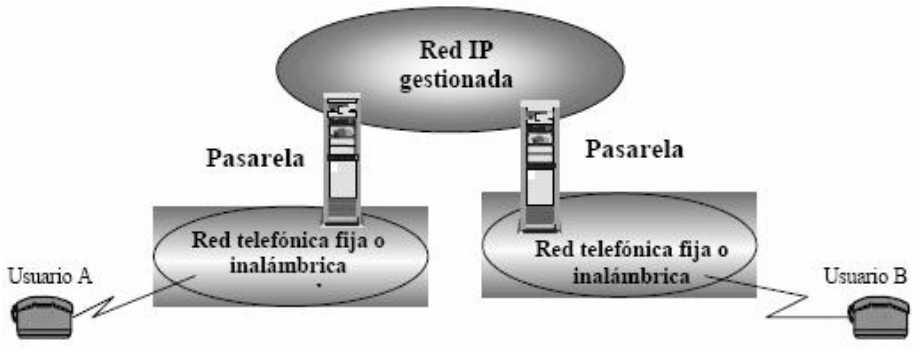
	Paso	Ejemplo
1	Escribir el número E.164 entero, incluido el indicativo de país (IDDD)	+46-8-9761234
2	Suprimir todos los caracteres no numéricos, salvo el signo «+»	+4689761234
3	Suprimir todos lo caracteres no numéricos	4689761234
4	Insertar un punto («.») entre cada cifra del número	4.6.8.9.7.6.1.2.3.4
5	Invertir el orden de las cifras del número	4.3.2.1.6.7.9.8.6.4
6	Añadir la cadena de caracteres «.e164.arpa» al final del número obtenido en el paso 5	4.3.2.1.6.7.9.8.6.4.e164.arpa

Utilizando el nombre de dominio obtenido en el último paso del procedimiento anterior, se aplica el algoritmo ENUM para obtener el orden de prioridad de los identificadores del servicio de llamada.

4.3.4. Llamada de teléfono a teléfono por IP.

En esta alternativa, las partes llamante y llamada están abonadas a la red telefónica pública (fija o móvil) y utilizan su aparato telefónico para comunicación vocal en la forma normal. Hay dos métodos para comunicarse mediante dos aparatos telefónicos ordinarios a través de una red IP o Internet.

4.3.4.1. Utilización de pasarelas.

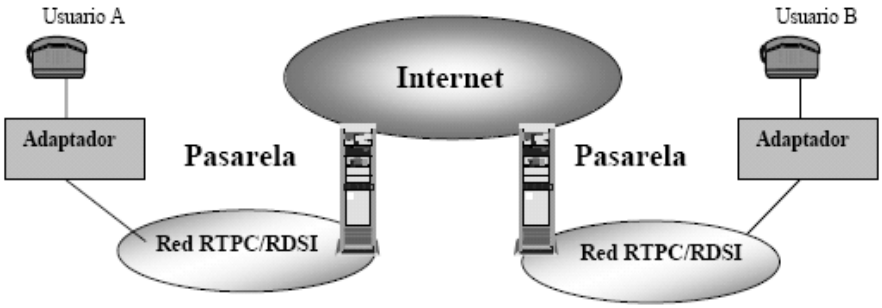


Esto significa que uno o varios actores de telecomunicaciones han establecido pasarelas que posibilitan la transmisión de voz a través de una red IP de un modo que es transparente para los usuarios telefónicos. En este caso no se trata de la red Internet sino de una red IP "gestionada", es decir, una red dimensionada de tal manera que permite el transporte de la voz con una calidad de servicio aceptable. Estas pueden pertenecer a distintos actores dependiendo si se trata de: a) la utilización puramente interna de VoIP dentro de la red de un solo operador telefónico que posee y gestiona toda la operación, encargándose de ambos usuarios A y B; o b) la prestación de un servicio vocal de larga distancia a través de un operador de larga distancia que utiliza tecnología VoIP (en este caso, los usuarios A y B pertenecen a distintas redes), en cuyo caso toda la operación pertenece al operador de larga distancia y es gestionada por el mismo.

4.3.4.2. Utilización de dispositivos adaptadores.

Muchas empresas ofrecen dispositivos parecidos a un módem que se instalan entre el aparato telefónico del usuario y su conexión a la RTPC.

Para que este tipo de configuración funcione adecuadamente, cada uno de los dos usuarios debe disponer de un abono con un ISP cuyos parámetros de acceso hayan sido programados en el dispositivo.



La parte llamante inicia la llamada de la misma manera que en una red de telecomunicaciones convencional, y la primera fase es en realidad el establecimiento de la comunicación en esa red; no obstante, inmediatamente después del establecimiento, los dispositivos intercambian la información necesaria para la segunda fase. A continuación, se disocia la llamada convencional y los dispositivos, en función de los datos que se han intercambiado y los parámetros preestablecidos, se establece una conexión entre cada uno de los corresponsales y su respectivo ISP. Una vez establecida la llamada,

los dispositivos convierten localmente las señales vocales a paquetes IP para transportarlos por Internet. En principio, este caso es muy similar al caso 1, salvo que los dos usuarios no requieren un PC y la necesidad de una «cita» Internet se facilita mediante el procedimiento iniciado en forma de una llamada telefónica. Sin embargo, este tipo configuración ha tenido éxito sólo marginalmente ya que requiere, como en el caso de PC a PC, que los dos corresponsales dispongan del mismo tipo de dispositivo.

En todos los casos, existe la necesidad de transmisión en tiempo real, con lo que es necesario garantizar aspectos de Qos (retardo, ancho de banda, etc.) bien mediante el sobredimensionado o bien implementando técnicas basadas en los modelos de DiffServ (Servicios Diferenciados), IntServ (Servicios Integrados) u MPLS (protocolo de conmutación por etiquetas multiprotocolo), sobre los que se esta trabajando actualmente. (los cuales serán analizados en detalle en el capitulo VI)

4.4. ESCENARIOS DE IMPLEMENTACIÓN.

4.4.1. Aplicaciones en el ámbito privado.

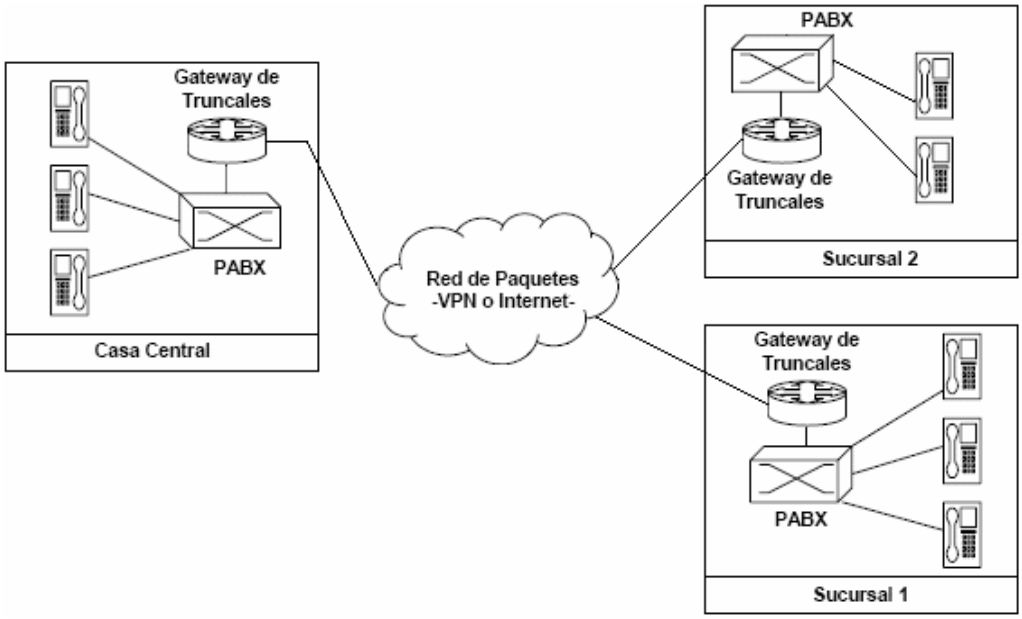
Muchas empresas han implementado redes de voz sobre paquetes para integrar en sus redes corporativas el tráfico de voz y datos. Estas redes son de tecnologías variadas, pero aquellas basadas en el protocolo IP son las más numerosas y nos concentraremos, entonces, en ellas.

Las aplicaciones más comunes son las empresariales y entre estas se destacan:

- La interconexión PABX tradicionales mediante la red IP.
- La utilización de PABX-IP, es decir aquellas que nativamente utilizan protocolos de transporte y señalización de voz sobre IP.

Podemos encontrar diversos escenarios de los que los más comunes son: las redes privadas totalmente IP, es decir, que tanto los dispositivos extremos como la red trocal es IP, y las redes privadas donde uno o varios dispositivos extremos son analógicos o digitales no IP y la red troncal es IP.

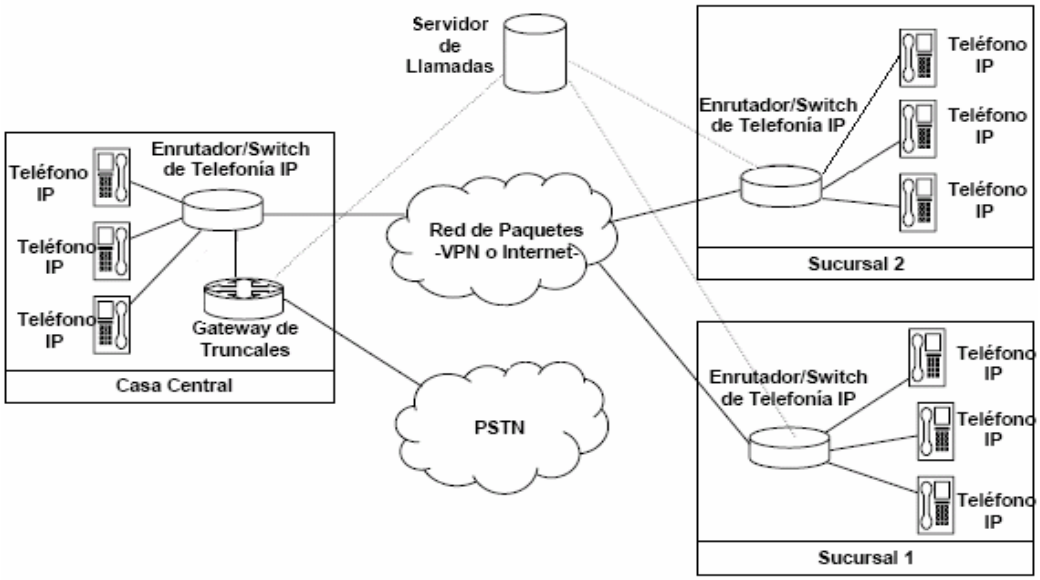
En la siguiente figura se muestra cómo es una interconexión de PABX tradicionales a través de la red IP:



Interconexión de troncales PABX y extensión de líneas mediante redes IP

En este caso el cliente dispone de equipos tradicionales (centralitas y teléfonos analógicos o RDSI, etc.). Las PABX se conectan a través de un gateways de voz, que transporta punto a punto tanto la señalización interna de las PABX como los canales vocales, y además conecta las redes de datos que pudieran existir en cada sucursal. El transporte de estas informaciones puede hacerse utilizando la red IP que se utilizaba para la interconexión de las redes de datos. Este puede ser una red privada de la empresa en cuestión (empresas grandes), una VPN contratada a un operador público o una red privada virtual a través de Internet (pequeñas empresas). En este último caso la empresa debe tomar las precauciones de seguridad requeridas para el intercambio de información por Internet, por ejemplo encriptando la información mediante el uso del protocolo IPSec (IP Security).

En la figura que se muestra a continuación se representa una solución de PABX IP:



Solución PBX-IP

El Servidor de Llamadas (creado por el ISC - International SoftSwuitch Consortium) se encarga del control de llamada y los dispositivos involucrados, y es el encargado de encaminar los mensajes de señalización entre los Routers/Switches de ToIP y de procesar los servicios. El router/switch de ToIP es un conmutador de paquetes o tramas Ethernet al que se conectan los usuarios a través de una red LAN. Tienen la capacidad de manejar mensajes de señalización y de priorizar el tráfico de voz. En caso de perder conectividad con el servidor central estos dispositivos suelen tener la capacidad de manejar el tráfico local de la sucursal.

El Teléfono IP es un dispositivo que cuenta con inteligencia propia para procesar la interacción con el usuario y solicitar los servicios al servidor de llamadas en nombre del usuario. Puede existir otros servidores centralizados, no mostrados en la figura como el Servidor de Tasación que se ocupa de contabilizar el uso de recursos por parte de los usuarios y el servidor de aplicación es el que ofrece una serie de servicios avanzados para las llamadas de los usuarios.

El inicio de la llamada lo efectúa un usuario de un teléfono IP hacia otro usuario con teléfono IP, ya sea que reside dentro del ámbito de un Router/Switch de ToIP o en otro. Los router/switches de ToIP están conectados a una red IP, que realiza la función de transporte de la llamada, y es en esta misma donde está conectado el Servidor de Llamadas que analizará en su base de datos la autentificación del llamante y ubicación del usuario llamado. La red de datos nuevamente podría ser una red privada, una VPN contratada a un operador o una VPN por Internet utilizando IPSec.

4.4.2. Aplicaciones en el ámbito público.

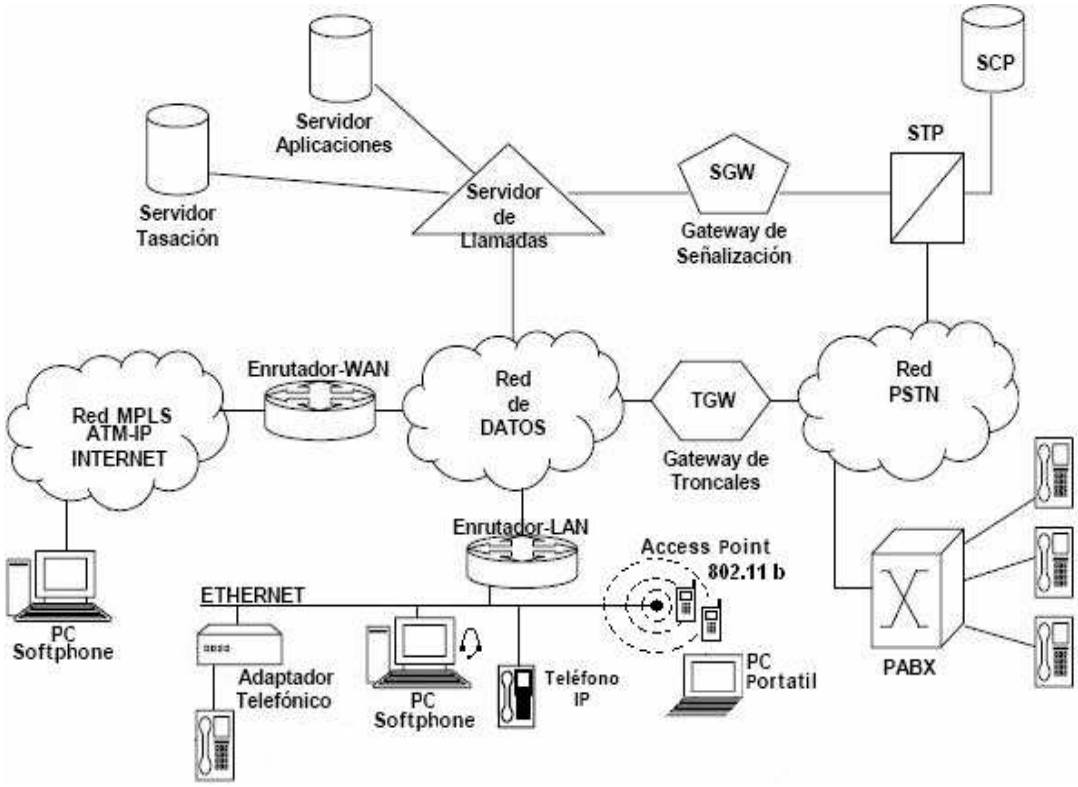
En el caso anterior existe la limitación que solo se pueden realizar llamadas entre las sucursales. Ahora de lo que se trata es el realizar llamadas al exterior utilizando la red IP interna.

El elemento esencial para poder interconectar la red IP a la PSTN es el "gateways", que hace de interfaz entre la red IP y la red telefónica. El escenario más común es la combinación del acceso a la red pública, para poder acceder a terminales externos y la red privada para poder acceder a terminales de la propia red, es decir de la misma empresa.

La siguiente figura esquematiza la arquitectura de las **"redes de nueva generación"** (NGN - Next Generation Networks).

Según la ITU, la NGN se define como una red basada en paquetes capaz de ofrecer servicios de telecomunicaciones y hacer uso de múltiples tecnologías de transporte de banda ancha y QoS (Quality of Service/Calidad de Servicio), en la cual las funciones relacionadas con el servicio son independientes de las tecnologías subyacentes de transporte.

Estas redes NGN proporcionan servicios de ToIP privada, como también servicios de ToIP local pública.



Arquitectura de redes publicas de nueva generación.

Esta arquitectura permite la operación con la red de conmutación de circuitos. El Servidor de Llamadas es el corazón del sistema y su función es la de procesar los mensajes de señalización de ambas redes y hacer el interfuncionamiento necesario. Este bloque que se esquematiza como una única caja en realidad es un conjunto de componentes tales como Media Gateway Controllers que son los encargados de interactuar al nivel de señalización con la PSTN y servidores de VoIP, como por ejemplo "SIP Servers" o "Gatekeeper" (SIP o H.323), que encaminan los mensajes de señalización y procesan las llamadas dentro de la red IP. La conversión de la voz de circuitos a paquetes y viceversa es realizada por los Media Gateways (Trunking Gateways) controlados por los Media Gateway Controllers del Servidor de Llamadas. El Signalling Gateway realiza las adaptaciones necesarias para transportar los mensajes de señalización número 7 sobre la red IP.

La red de ToIP irá avanzando hacia el abonado a través de Access Gateways que son dispositivos que controlan un gran número de líneas de telefonía tradicional y las convierten a VoIP controlados por los Servidores de Llamadas de clase 5 (Media Gateway Controllers de clase 5). Más cerca del cliente, e incluso en sus domicilios se ubican los IAD (Integrated Access Devices) estos realizan la conversión de la voz y la señalización de abonado a los protocolos de VoIP. También puede haber usuarios que directamente se conecten a la red IP a través de teléfonos IP (fijos-móviles).

A diferencia de los terminales IP **"fijos"**, los terminales **"móviles"**, se basan en el estándar para Redes Locales Inalámbricas (WLAN) 802.11b que permite entregar una solución práctica para redes inalámbricas de múltiples proveedores, y para igual número de aplicaciones. Disfrutando de las mismas facilidades y funcionalidad que el resto de los usuarios con terminales fijas. Para garantizar la seguridad de estas redes inalámbricas, existen varias alternativas, por ejemplo, los protocolos WEP (Wired Equivalency Protocol), o "Privacidad Equivalente al Alámbrico" y el WPA (Wi-Fi Application Protocol), o "Acceso Protegido Wi-Fi", que se encargan de autenticación, integridad y confidencialidad, proporcionados por los propios dispositivos inalámbricos, o IPsec (túneles).

Los servicios de voz (y multimedia) avanzados se dan a través de plataformas de servicio generalmente dedicadas a un determinado servicio que presentarán interfaces de programación estándar de manera que pueda utilizarse un entorno de creación de servicios también estándar que permita a terceras partes desarrollar servicios independientes de la plataforma "hardware" y sus fabricantes.

El advenimiento de las NGN, es una realidad en el desarrollo de las telecomunicaciones, condicionada por un grupo de circunstancias tecnológicas y de mercado. Las características de esta

red, de hacer converger las redes de datos, voz y video, llaman la atención a operadores, fabricantes y usuarios por las ventajas que introduce desde el punto de vista tecnológico, social y económico.

Por ejemplo, la infraestructura de ToIP de Cisco Systems permite ofrecer multitud de servicios sobre una única plataforma, como: ToIP, VoIP, acceso a Internet, VPNs que permitan la interconexión entre las sedes de una empresa o el acceso a la LAN corporativa a teletrabajadores remotos, etc.

5. CAPITULO V. FACTORES QUE AFECTAN LA CALIDAD DE SERVICIO (QOS).

Son muchos los términos manejados en el estudio de la QoS (Quality of Service), que, a su vez, son aplicables no sólo a éste área, sino a otros ámbitos de las telecomunicaciones y de la informática, por lo que en este apartado se explicarán aquellos considerados clave para el completo entendimiento de este tema. Para conseguirlo, inicialmente se presenta una introducción al término QoS estableciendo una visión inicial de lo que implica su aplicación en las tecnologías de redes existentes. Posteriormente se analizan todos aquellos parámetros implicados en su obtención, permitiendo, a su vez, realizar una clasificación, comprender las ventajas de su implementación y observar las diversas técnicas propuestas por las empresas al respecto.

5.1. INTRODUCCIÓN.

La provisión de QoS garantizada por parte de las redes de comunicación en un ámbito global es actualmente uno de los campos de investigación en activo, principalmente debido a la creciente importancia de aplicaciones telemáticas (destacando entre ellas a la ToIP), que precisan de esa garantía para su correcto funcionamiento.

El auge de la ToIP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el costo de llamadas a través de Internet. Sin embargo, si de algo adolece todavía la ToIP es de la calidad de los sistemas telefónicos tradicionales. Los problemas de esta calidad son muchas veces inherentes a la utilización de la red (Internet y su velocidad y ancho de banda) y podrán irse solventando en el futuro. Mientras tanto, cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

Los principales factores que influyen en la QoS de la ToIP, son: el delay (latencia o retardo), el jitter, la pérdida de paquetes, y el eco. Una calidad satisfactoria depende de un buen canal, baja latencia y buen control del eco; un buen canal se caracteriza por baja pérdida de paquetes, un codec de alta calidad y un buen algoritmo de Voice Activity Detection (VAD, detección de la actividad de la voz), cuyo objeto es eliminar los momentos de silencio de una conversación (que suelen llegar hasta un 60% del tiempo total de una llamada telefónica). La baja latencia es necesaria para una comunicación de voz interactiva. El control del eco hace que quien habla no interprete el eco como el principio de la respuesta de la otra persona.

Para una red ToIP de alta calidad, uno de los factores básicos es la capacidad para reducir y controlar el delay. La latencia de las comunicaciones de voz se define normalmente como el retraso

en una dirección entre la boca de quien habla y el oído de quien escucha. El delay, o latencia, de una llamada telefónica tradicional normalmente es de 50 ms; el GSM (Sistema Global para las Comunicaciones Móviles) tiene un delay superior a 200 ms; las comunicaciones por satélite llegan medianamente a más de 500 ms. La latencia máxima aceptada en una red de datos para una calidad de la voz tipo "carrier class" (alta disponibilidad), a saber comparable con la de las gestoras tradicionales de telefonía, es de 150/200 ms. Entre los elementos que contribuyen a la latencia, están las compresiones codec (que varían de 1 ms del G.711 a los 20 ms del G.729), la paquetización y el framing, que suponen aproximadamente 10 ms; el buffer necesario para compensar las variaciones de delay (jitter) puede añadir otros 50 ms, pero normalmente el 80% de la calidad en ToIP depende de cómo está diseñada la red IP. El retraso introducido por una infraestructura de red puede normalmente segmentarse entre conexión de **acceso up-link** (enlace ascendente), backbone y conexión de **acceso down-link** (enlace descendente), y depende tanto del "retardo de propagación" debido a las características físicas de los medios (cobre, fibra, inalámbrico), como del "retardo de red" producido por los equipos de red que procesan los paquetes de voz a lo largo de su camino. El delay puede producir interrupciones en el ritmo o en la cadencia de una llamada telefónica y si el retraso es alto puede convertir la llamada en algo similar a una transmisión CB, obligando a los interlocutores a adoptar una estructura formal "hablo yo/hablas tú" para asegurar que no empiecen ambos a hablar al mismo momento aprovechando una pausa aparente debido al delay. Al ser la red IP un factor crucial en la calidad de ToIP, es fácil darse cuenta de la importancia de disponer de un buen diseño de red y de instrumentos tecnológicos que puedan garantizar una efectiva continuidad en la OoS.

Dados estos requerimientos de QoS impuestos por el tráfico con características de tiempo real, como es voz y vídeo, se necesitan mecanismos que propicien el control de dichos parámetros de calidad, y dar garantía de QoS.

5.2. GENERALIDADES.

5.2.1. Concepto de QoS.

Se entiende por "Calidad de Servicio", a la capacidad de una red para sostener un comportamiento adecuado de tráfico que transita por ella, cumpliendo a su vez con los requerimientos de ciertos parámetros relevantes para el usuario final. Esto puede entenderse también como el cumplimiento de un conjunto de requisitos estipulados en un contrato (SLA: Service Level Agreement, acuerdo de nivel de servicio) entre un ISP y sus clientes.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de la red con otras aplicaciones no críticas.

5.2.2. Clasificación de QoS.

Es posible realizar una clasificación de QoS bajo distintas especificaciones, así podríamos diferenciarla según el tipo de tráfico, dónde aplicarla, la reserva de recursos de la red y otros parámetros, tal y como se indica a continuación.

5.2.2.1. Según la sensibilidad del tráfico.

Teniendo en cuenta la variedad de tráfico existente y los requerimientos de retardo, latencia y ancho de banda para cada tipo, nos encontramos con:

a) **QoS muy sensible al retardo:** Un ejemplo de este tipo es para el tráfico de vídeo comprimido. Para este caso es necesario garantizar la disponibilidad de una determinada y gran cantidad de ancho de banda reservado para este tráfico y un valor de retardo mínimo que asegure la correcta transmisión del mismo. Para conseguirlo será necesario utilizar mecanismos de prioridad, así como encolar adecuadamente los flujos de datos.
b) **QoS algo sensible al retardo:** Como la resultante de la aplicación de la emulación de circuito. Al igual que en el caso anterior se garantiza hasta un cierto nivel de ancho de banda, aunque en menor valor. De la misma manera, será necesario asignar prioridades para la transmisión de los datos.
c) **QoS muy sensible a pérdidas:** Como sucede con el tráfico tradicional. Si se garantiza un nivel de pérdidas de valor cero entonces nunca se descartarán paquetes ni se desbordarán los buffers de almacenamiento del flujo, lo que facilitará el control de transmisión, por otra parte, esta garantía se hace a nivel de acceso al medio (MAC) o en capas superiores, pero nunca a nivel físico.
d) **QoS nada sensible:** Por ejemplo el tráfico de servicios de noticias. La filosofía de este tipo de QoS es usar cualquier oportunidad de transmisión restante y asumir que la capacidad de los buffers posteriores es suficiente para llevarla a cabo, asignándole a este tipo de tráfico la prioridad más baja. A este tipo responden los algoritmos “Best Effort”(o al mejor esfuerzo), utilizado en Internet.

5.2.2.2. Según quién solicite el nivel de QoS.

Teniendo en cuenta que la petición de QoS puede ser realizada por el usuario final o por los conmutadores de la red, nos encontramos con:

a) **QoS Implícita:** En este tipo el router o conmutador asigna automáticamente los niveles de calidad servicio en función del criterio especificado por el administrador, como el tipo de aplicación, protocolo o dirección de origen.

Hoy en día todos los routers, y algunos conmutadores, ofrecen este tipo de QoS. El proceso es el siguiente:

Estaciones finales: Las estaciones finales transmiten los paquetes.

Conmutador o router: Le llegan los paquetes, realiza un estudio de los datos entrantes y los prioriza, repartiéndolos en diferentes colas según la prioridad asignada. Estos datos vuelven a ser transmitidos hacia el siguiente conmutador o router, donde se repite el proceso.

Las funciones son:

- Control de red: Lo tiene el administrador
- Lugar: Centralmente
- Técnicas: Se realiza según unos patrones de tráfico

b) **QoS Explicita:** Este tipo de QoS permite al usuario o aplicación solicitar directamente un determinado nivel de servicio que han de respetar los conmutadores y routers. Así, el proceso es:

Estaciones finales: En este caso las estaciones finales transmiten una petición RSVP, si ésta es aceptada, los paquetes son transmitidos.

Conmutador o router: Los datos entrantes son priorizados de acuerdo a instrucciones del nodo de destino, pasando al próximo conmutador o router, donde se repetirá el proceso

Las funciones son:

- Control de red: Lo tiene el usuario o la aplicación. Es por lo tanto, más difícil de gestionar
- Técnicas: IP Type of Service (ToS), RSVP.

5.2.2.3. Según las garantías.

En esta clasificación se va a tener en cuenta la reserva de recursos del sistema para proporcionar los servicios y son:

a) **QoS Garantizada / Hard QoS:** También conocida como "hard QoS" la calidad de servicio garantizada es aquella en la que se produce una reserva absoluta de los recursos de la red para un tráfico determinado, asegurándose así unos niveles máximos de garantías para este tráfico.
b) **QoS No Garantizada / Lack of QoS:** En una calidad de servicio sin garantías. El tráfico es transmitido por la red a expensas de lo que en ella pueda sucederle. Es el tipo de QoS correspondiente a los servicios Best Effort.
c) **QoS Servicios Diferenciados/ Soft QoS:** También conocida como "Soft QoS" es el punto medio entre los dos tipos anteriores. Para este tipo se realiza una diferenciación de tráfico, siendo tratados algunos mejor que el resto (expedición más rápida, más ancho de banda promedio, menos tasa de error promedio). Es el utilizado por DiffServ.

5.2.2.4. Según el lugar de aplicación.

Es posible aplicar calidad de servicio en los extremos y en los bordes de la red, por lo tanto tenemos:

a) **QoS Extremo a Extremo (End to End):** Es la aplicación de las políticas de calidad de servicio entre los extremos de la red. Es viable gracias a productos como el software Dynamic Access de 3Com, pero está menos extendida que la QoS entre dos bordes de la red (edge-to-edge). También se la conoce comúnmente como la QoS absoluta.

Con este tipo de QoS se simplifican, sin embargo, los puentes, cuya función se reduce a observar la marca de los paquetes (en el caso de 802.1p), sin tener que calcular la clase de servicio de cada paquete reducido.

Otra ventaja es que las aplicaciones podrían seleccionar dinámicamente el nivel de QoS, almacenándose temporalmente en los directorios de red o en los puentes una información estática de clases de servicio.

Actualmente, la política de las empresas dedicadas al networking es conseguir una calidad de servicio extremo a extremo, por lo que se están estudiando y aplicando diferentes técnicas para conseguirlo. A lo largo de los capítulos posteriores este tipo de QoS será referenciada en multitud de ocasiones, especificando cómo conseguirla.

b) **QoS Borde a Borde (edge to edge):** Es la aplicación de las políticas de calidad de servicio entre dos puntos cualesquiera de la red. Por ejemplo en los puentes. Esto tiene varias ventajas: en primer lugar no requiere que los administradores de red toquen ninguno de los extremos,

esto es una ventaja para el caso de las empresas en las que la organización responsable de la infraestructura de red está separada del grupo de los servidores y del resto de los puestos de trabajo. Otra ventaja es que son menos los dispositivos que tienen que ser manejados para la obtención de la QoS. Además, la accesibilidad por parte de un usuario cualquiera de la red o de un hacker para cambiar las especificaciones de QoS es mucho menor. Por último, utilizando edge-to-edge QoS no es necesario conocer cómo poner en práctica las reglas de QoS de cada uno de los posibles sistemas operativos que podrían tener los servidores en el caso de aplicar QoS extremo a extremo.

A este tipo también se le conoce como calidad de servicio relativa

5.2.3. Requerimientos para garantizar Qos.

Para garantizar la QoS se requiere de la participación de un conjunto de elementos, los cuales los podemos dividir en tres grupos generales:

- **Aplicaciones.** Aquí la aplicación debe de manejar la señalización necesaria para hacer la negociación de parámetros con la red.
- **Acceso LAN.** Que tipo de arquitectura de red se usará, protocolos, mecanismos de calendarización y control de tráfico, así como control de admisión.
- **Acceso WAN.** Es la arquitectura de transporte de información que ofrece la capacidad de mantener el mínimo de retardo y pérdidas de información, por medio de mecanismos de diferenciación y control de tráfico.

5.2.4. Parámetros de QoS.

Los problemas de QoS en ToIP vienen derivados de dos factores principalmente: a) Internet es un sistema basado en conmutación de paquetes y por tanto la información no viaja siempre por el mismo camino. Esto produce efectos como la pérdida de paquetes o el jitter. b) Las comunicaciones ToIP son en tiempo real lo que produce que efectos como el eco, la pérdida de paquetes y el retardo o latencia sean muy molestos y perjudiciales y deban ser evitados.

5.2.5. Como medir la QoS.

- Es necesario establecer un testbed en el cual se pueda medir el desempeño al nivel de aplicación y de red y así establecer los puntos de medición.

- Desarrollo e implementación de herramientas que permitan medir parámetros de QoS en forma pasiva y activa.

5.2.6. Beneficios al aplicar QoS.

Se centrará este punto, en el estudio de los beneficios para las aplicaciones, para las empresas y para los proveedores de servicio.

- **Ventajas para las aplicaciones.**

Hoy en día, todas las empresas están considerando Internet como una nueva vía para incrementar su negocio y, en consecuencia, las expectativas que se tienen para garantizar una calidad son las mismas que si se tratase de una red privada o controlada. Internet está siendo utilizada para la formación y el crecimiento de intranets dentro de la empresa y extranets que permiten el comercio electrónico con los socios del negocio. Es evidente, por tanto, que se está incrementando el acercamiento de los negocios hacia la Web, siendo cada vez más importante que los administradores de las redes aseguren que éstas entreguen unos niveles apropiados de calidad. Es aquí donde las tecnologías de QoS cobran especial importancia, proporcionando a los administradores las utilidades para la entrega de datos críticos del negocio en los periodos y con unas garantías determinadas.

- **Beneficios para las empresas.**

Las aplicaciones están consiguiendo ser cada vez más exigentes. Las denominadas críticas requieren cada vez más calidad, confiabilidad, y asegurar la puntualidad en la entrega. Un ejemplo claro son las aplicaciones de voz o vídeo, éstas deben ser manejadas cuidadosamente dentro de una red del IP para preservar su integridad. Además es necesario tener en cuenta que el tráfico no es predecible, ni constante, si no que funciona a ráfagas, produciéndose en ocasiones picos máximos de tráfico que son los causantes, en parte, de la saturación de la red. Ejemplos clarificadores de este tipo de tráfico es el producido por el mundo Web, el correo electrónico y las transferencias de ficheros, que son virtualmente imposibles de predecir.

Las tecnologías de QoS permiten a los administradores de red:

- Manejar las aplicaciones sensibles al jitter, como las que manejan audio y vídeo.
- Manejar el tráfico sensible al retardo, como la voz en tiempo real.
- El control de pérdidas en los momentos en los que la congestión sea inevitable.

- **Beneficios para los proveedores de servicio.**

Claramente, las empresas y las corporaciones se están convirtiendo en negocios con requerimientos de "misión crítica" sobre la red pública. Están delegando los servicios de sus redes a proveedores de servicio (outsourcing), lo que les permite centrarse más en el negocio interno y así reducir costosos capitales. Esto significa que los proveedores de servicio son quienes podrán ofrecer las garantías de calidad para el tráfico extremo a extremo (end to end) de la empresa. Las tecnologías de QoS permitirán a los proveedores de servicio ofrecer muchas más prestaciones, como el soporte del tráfico en tiempo real, o como la asignación específica de ancho de banda, que se suele especificar en los acuerdos de nivel de servicio (SLAs).

5.3. QOS EN LA RED.

5.3.1. Redes de datos.

Las redes de datos fueron concebidas a fin de posibilitar la comunicación entre las aplicaciones que se ejecutan en los computadores. Originalmente, se trataba de grandes computadores centralizados. La creación de los minicomputadores y a continuación de los microcomputadores, aunada a la concepción de las aplicaciones de computador orientadas al modelo cliente/servidor, han contribuido de manera importante al despliegue e interconexión de las redes de datos. Por tanto, el equipo conectado a una red de datos adopta la identidad de computadores altamente distribuidos con complejidad variable y que ejecutan diversas aplicaciones.

Desde el principio, el problema de Qos en las redes de datos fue diferente que en las redes telefónicas, debido al hecho de que la calidad de servicio prevista por los usuarios de la red de datos no está asociada con una aplicación particular ofrecida por la red, sino con las propiedades relativas a sus puntos de acceso a la red. El conjunto de estas propiedades define lo que comúnmente se denomina acuerdo de nivel de servicio (SLA).

El punto de acceso del usuario a una red de datos, pública o privada, posibilita establecer la comunicación entre una o varias máquinas y todas las demás conectadas a la red. Los requisitos de calidad de servicio en este punto de acceso forman parte del SLA se expresan por lo general como velocidad autorizada (promedio y de cresta), tiempo de transmisión (promedio y residual) o prioridad relativa de los datos en el caso de congestión. Cabe observar que se trata de propiedades con las que debería contar la red para el transporte de los datos a fin de sustentar una o varias aplicaciones de las cuales la red, a priori, no tiene conocimiento.

De manera similar a los puntos de acceso de usuario, los puntos de interconexión entre redes se rigen también por SLA independientes de las aplicaciones cuyas SLS expresan sólo propiedades de transporte.

Por consiguiente, el modo de transporte empleado por las redes de datos más a menudo es el modo paquetes, fundamentado en el carácter esporádico de los datos transmitidos por las aplicaciones informáticas. Los datos entregados en un punto de acceso de red son ensamblados en paquetes de tamaño fijo o variable según la naturaleza de la red. En cada caso, la cabecera del paquete incluye la dirección de destino, para que los componentes de la red puedan encaminar los paquetes hacia su destino final, o al punto más cercano, sin tener en cuenta el contenido del paquete, que será tratado por la aplicación apropiada en la máquina de destino. Mediante circuitos virtuales (por ejemplo, en las redes ATM) puede potenciarse un modo de transporte de paquetes, garantizando en mayor grado la QoS. No obstante, las redes de transporte, en el nivel básico, no prevén el modo de circuitos virtuales. Algunos protocolos, como DiffServ, IntServ, o MPLS, permiten ese tipo de ampliación en el nivel superior de una red IP, pero aún no se prevé su despliegue en todas las redes IP.

Por consiguiente, cuando una aplicación recurre a una o varias redes de datos, la calidad de servicio resultante de extremo a extremo entre las dos máquinas que ejecutan la aplicación en cuestión dependerá de la calidad de servicio garantizada por todas las redes que intervienen. Por este motivo, la calidad de servicio es criticada muy a menudo. Basta con que una sola red ofrezca una calidad de servicio inferior a la aceptable para que se vea afectada la calidad de extremo a extremo.

Por este motivo, cuando las empresas emplean la red Internet para interconectar máquinas distantes para sus aplicaciones estratégicas, con frecuencia eligen los servicios de proveedores de red privada virtual (VPN). Este tipo de proveedor establece, mediante ingeniería especializada, la configuración de señalización por encima de la red Internet, mediante una red virtual que garantiza propiedades de calidad de servicios aceptables entre todos los puntos de acceso de la empresa, con inclusión de algunos puntos de acceso dinámicos para los usuarios distantes. Por supuesto que una VPN sólo podrá establecerse mediante la reservación de recursos en todas las redes fijas que la apoyen; por consiguiente, un servicio de este tipo tendrá un costo más elevado y está previsto actualmente sólo para clientes empresariales.

5.3.2. Servicio best-effort.

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la QoS requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no pérdida de

contenido y ni secuencialidad de los mismos. En este sentido IP fue concebido, es decir, para "mover" por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real.

Para esto el servicio que brinda IPv4 es del tipo "Best Effort", es decir, cuando la red hace todo lo posible para intentar entregar el paquete a su destino, no existiendo garantía de que esto ocurra. Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma íntegra, sino que además requiere ser transferido en el tiempo adecuado, al "ritmo" adecuado, en correspondencia con la cadencia que es generado.

El nacimiento de IPv6 viene a resolver las limitaciones de IPv4, además de integrar nuevas características que permitan entregar seguridad y confiabilidad en la transmisión de la información.

5.3.2.1. Soporte de QoS que incorporan los protocolos IPv4 e IPv6.

Los protocolos IPv4 e IPv6 siguen la estrategia de asignación de prioridades definiendo campos incluidos en las cabeceras que permiten diferenciar tráfico. Estos protocolos, sin embargo, no pueden ofrecer por sí solos una QoS extremo a extremo. Para que esto sea posible necesitan apoyarse en alguno de los modelos y mecanismos propuestos por la IETF como:

- **Servicios Integrados** (IntServ) y **RSVP** (Resource ReserVation Protocol). Sigue una estrategia de reserva de recursos. Antes de que se transmitan los datos, las aplicaciones deben primero establecer caminos y reservar recursos. RSVP es el protocolo que usa IntServ para establecer los caminos y reservar los recursos necesarios.
- **Servicios Diferenciados** (DiffServ ó DS). Sigue una estrategia de asignación de prioridades. Los paquetes se marcan de distintas formas para crear varias clases de paquetes. Los paquetes de diferente clase recibirán servicios distintos.
- **MPLS** (MultiProtocol Label Switching). Es un nuevo esquema de encaminamiento y conmutación que integra los niveles de red y enlace sin discontinuidades. Se presenta como sustituto de IP sobre ATM ó IP/ATM. A los paquetes se les asignan etiquetas al ingresar en un dominio con capacidad de MPLS. La posterior clasificación, encaminado, y servicios aplicados a los paquetes se basarán en las etiquetas.

5.3.2.2. QoS en las diferentes redes IP.

Es posible contar con tres tipos de redes IP:

- **Internet.** El estado actual no permite un uso profesional para el tráfico de voz.
- **Red IP publica.** Los operadores ofrecen a las empresas la conectividad necesaria para interactuar sus redes de área local en lo que al tráfico IP se refiere. Considerándose como algo similar a Internet, pero con una mayor QoS, y con importantes mejoras en seguridad.
- **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 escenario se tiene bajo control prácticamente todos los parámetros de la red, resultando ideal para el transporte de la red.

5.3.3. Problemas de QoS en las fronteras.

El tráfico intercambiado entre redes ISP se convierte en el denominado tráfico "fuera de red", el cual plantea una serie de problemas de QoS.

Los principales problemas de QoS existentes fuera de la red pueden resumirse del siguiente modo:

- Cuando las redes de interconexión utilizan equipos de distintos vendedores y esos equipos no incluyen productos industriales plenamente normalizados, suelen surgir ciertos problemas que inciden en la QoS. Así, por ejemplo, se pierden estructuras del diseño de redes que mejoran la calidad de servicio, y no se utilizan sistemas de gestión normalizados.
- Cada uno de los acuerdos de nivel de servicio (SLA) ofrecidos por los proveedores de tránsito es específico. Las propiedades estadísticas de las redes ISP son distintas y, además, no son fácilmente comparables, ya que existen diferencias en cuanto al modo de recopilar los datos.
- Algunas veces, las especificaciones del servicio de VBR del ATM (empleado para el tráfico de Internet) varían de una red a otra, por lo que la QoS no se mantiene cuando el tráfico cruza las fronteras.
- Los equipos con dos o más años de antigüedad no suelen proporcionar las mismas capacidades de QoS que las ofrecidas por equipos más nuevos.

De lo anterior se desprende que la degradación de la calidad de servicio es muy frecuente en los extremos.

Por otra parte, existen motivos para sospechar que las posibles soluciones a estos problemas de QoS pueden verse aplazadas debido a un problema de coordinación. Todas las redes que manejan los datagramas enviados entre anfitriones comunicantes ("equipos terminales", en términos de RTPC) deben ser capaces de conservar los parámetros de QoS que proporciona la red de origen para que dichos parámetros puedan ser actualizados entre los anfitriones o las partes que establecen la comunicación. En otras palabras, si una de las redes del ISP encargadas de proporcionar la comunicación confiere a su parte de la red una calidad de servicio inferior a la ofrecida por otras redes, la QoS del flujo se verá reducida en consecuencia.

En este contexto, las redes individuales pueden mostrarse renuentes a invertir en una QoS superior si no existe alguna forma de coordinar esta mejora con las demás partes de la cadena.

5.3.4. QoS en la transmisión de paquetes de VoIP sobre LAN.

Una de las principales desventajas para cualquier tráfico crítico respecto del tiempo y en particular los paquetes de VoIP en una LAN, es que los protocolos más utilizados en el nivel de enlace, Ethernet y Token Ring, trabajan con un tamaño de paquete variable. El equipamiento desarrollado para VoIP brinda sólo conectividad Ethernet, con un ancho de banda de transmisión (BW) de 10 Mbps. El tamaño de la carga útil del paquete varía entre 46 y 1500 bytes y el encabezado ocupa entre 14 y 20 bytes. Por ejemplo, si tenemos un paquete con una carga útil de 64 bytes, y un encabezado de 20 bytes, la tasa de paquetes Ethernet es de 14880 pps (10000000 bps/ [(64 bytes +20 bytes) x 8 bits/Bytes]).

Por lo tanto, la utilización del ancho de banda y la tasa de paquetes pueden o no coincidir debido a la variación del tamaño de los paquetes. La utilización se incrementa debido a la variación de dos factores, aumento de la cantidad de paquetes y/o el tamaño de la carga útil de los mismos.
En Ethernet la disponibilidad de ancho de banda es dependiente del número de colisiones, en forma exponencial debido a la forma de trabajo del mecanismo CSMA/CD de la norma Ethernet 802.3

Para cumplir con los requerimientos de QoS para ToIP la utilización del ancho de banda no debe superar el 25 % o su equivalencia en porcentaje de colisiones que no debe superar el 45 %.
El estándar 802.1p provee el método para especificar los requerimientos de retardo y prioridades sobre una red LAN Ethernet y Token Ring.

Normalmente la QoS de LAN va asociada a la QoS a nivel de red, haciendo una equivalencia de prioridades 802.1p a tipos de servicio IntServ o DiffServ (más fácil con Diffserv).

5.3.5. QoS en la transmisión de paquetes de VoIP sobre WAN.

De acuerdo a resultados empíricos, la calidad de la voz comienza a degradarse en un enlace WAN, cuando el retardo supera los 150 ms. Debemos considerar no solo el ancho de banda que ocupa el tráfico de VoIP sino también el tráfico de datos propiamente dicho. En enlaces de baja capacidad, es decir menores a 512 Kbps se puede llegar a degradar la voz en forma notable cuando se transmiten los paquetes de VoIP que compiten con paquetes de datos o con otros paquetes de VoIP. Esto ocurre cuando no hay una política correctamente aplicada de QoS. Hay soluciones propietarias, como LFI (Link Fragmentation Interleave) utilizadas en enlaces de baja velocidad. Funcionan segmentando y entrelazando todos los paquetes para evitar la competencia con los pequeños paquetes de VoIP.

5.4. DIFICULTADES TÉCNICAS, PARÁMETROS DE QOS.

El elemento que más afecta a la calidad de las llamadas de ToIP es el diseño, implementación y uso de la red en la que tienen lugar estas llamadas. Una llamada típicamente se originará en un CPE (Customer Pre-mises Equipment) o "equipo en las premisas del cliente", circulará primero a través de la LAN del cliente, circulará posteriormente a través de un enlace WAN, la red del proveedor de servicios y vuelta a otra red LAN y, por último, el CPE del extremo remoto. Los equipos CPE y los enlaces WAN son los más vulnerables a factores degradantes.

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:

5.4.1. Retardo.

El retardo de extremo a extremo (a veces denominado "latencia") es el tiempo entre la generación de un sonido en un extremo de una llamada y su recepción en el otro extremo. El retardo incluye el tiempo que toma codificar el sonido como señal digital, la travesía de la señala por la red, y la regeneración de la señal como sonido en el extremo de recepción. El retardo causa dos deterioros diferentes. Primero, al aumentar el retardo, el eco se vuelve más evidente. Segundo, cuando el retardo es lo suficientemente prolongado, perturba la dinámica de la conversación, dificultando la comunicación.

Se ha determinado que el retardo máximo que la voz puede sufrir en una conversación es de 250 mseg, y que un retardo mayor de este valor se torna sumamente desagradable, ocasionando que

los integrantes de la conversación traten de hablar simultáneamente. De esta manera, cuando uno de los usuarios escucha que el otro no está hablando, entonces comienza a hablar, pero debido al retardo, el otro usuario no lo escucha de manera inmediata, por lo que puede comenzar a hablar también, lo cual ocasiona que las voces de los usuarios se solapen constantemente, haciendo muy difícil que la conversación se desarrolle normalmente. El solapamiento de las voces es detectado por los integrantes de la conversación un tiempo después de que comenzaron a hablar, siendo este tiempo igual al retardo sufrido por la voz. Cuanto mayor sea este retardo, mayor será el tiempo que se tarde en detectar que se está hablando simultáneamente, resultando las colisiones de las voces más desagradables y difíciles de controlar. Cuando el retardo es menor a 250 mseg, el efecto causado por las colisiones es tolerable y la conversación se puede desarrollar normalmente. A continuación se muestran los valores (véase la Recomendación UIT-T G.114) que indican las clases de calidad e interactividad de acuerdo con el retardo de transmisión en una conversación telefónica.

Clase N°	Retardo por cada sentido	Observaciones
1	De 0 a 150 ms	Aceptable para la mayoría de las conversaciones; sólo algunas funciones altamente interactivas pueden experimentar degradación.
2	De 150 a 300 ms	Aceptable para las llamadas de baja interactividad (satélite con 250 ms por salto).
3	De 300 a 700 ms	Prácticamente una llamada semidúplex.
4	Más de 700 ms	Inútil, a menos que los llamantes estén habituados a conversar en semidúplex (como en el ejército).

Clases de calidad del UIT-T según el retardo de transmisión

Para las transmisiones de vídeo, el retardo debe también mantenerse dentro de un límite tolerable de alrededor de 3 segundos. Para lograr retardos no mayores de un límite superior se emplean métodos de segmentación y de asignación de prioridades.

A los paquetes de voz y vídeo se le asignan prioridades mayores que a los paquetes de datos. Con este esquema, los paquetes de datos son almacenados hasta que los paquetes de mayor prioridad (voz y vídeo) son transmitidos.

Con la segmentación, los paquetes de gran tamaño son divididos para formar varios paquetes más pequeños. Con paquetes de menor tamaño se logra que el tiempo de serialización sea menor, logrando un menor retardo. Adicionalmente, si el equipo de usuario se encuentra transmitiendo un paquete de datos y llega un paquete de voz ó vídeo, entonces este último paquete deberá esperar

menos tiempo por la transmisión del paquete de datos cuanto más pequeño sea éste. Adicionalmente, el hecho que los paquetes sean de menor tamaño contribuye a que, en caso de pérdidas de paquetes por errores de transmisión o por congestión, la información que se pierde sea menor.

Cuando el retardo entre la emisión de la voz y el eco de retorno es significativo (45 ms o más), el eco se hace sumamente molesto no permitiendo en algunos casos la conversación. Los equipos de usuario deben poseer canceladores de eco para disminuir este efecto. Los canceladores de eco comparan la voz recibida de la red de paquetes con la voz que está siendo transmitida, eliminando los patrones semejantes y con esto eliminando el eco.

Por su filosofía de funcionamiento, las redes de paquetes tienen mayores retardos y variaciones de retardo que las tecnologías TDM y las de conmutación de circuitos.

En la RTPC convencional, la mayor parte del retardo de extremo a extremo corresponde al tiempo de propagación del medio de transporte. El procesamiento causa cierto retardo, pero generalmente no supera unos pocos milisegundos. En cambio, la voz paquetizada sufre una considerable demora por el procesamiento, y otros retrasos debidos a que comparte el circuito y el ancho de banda con los datos y así los paquetes pueden atravesar muchos nodos antes de llegar a su destino, lo que puede dar la posibilidad de deficiencias en la transmisión de paquetes de voz por las memorias intermedias de colas y fluctuaciones. A fin de minimizar dichos retardos de colas y propagación, el procesamiento de la red debe agilizarse, y a los paquetes que portan comunicaciones vocales interactivas se les debe dar la ruta más directa a través de la red. A continuación se describen los componentes que contribuyen al retardo de extremo a extremo.

5.4.1.1. Retardo de compresión.

Al comprimir la voz y el vídeo se tiene un retardo que puede ser significativo y que depende del algoritmo de compresión escogido. El retardo de compresión puede ser dividido en dos categorías: el retardo del algoritmo y el retardo por procesamiento. El **retardo del algoritmo** no depende de la circuitería utilizada (capacidad ó velocidad del microprocesador, tipo de memoria utilizada, etc.), sino que depende de la manera en que el algoritmo maneja la información a ser comprimida.

Como se vio en el capítulo 4, existen diferentes algoritmos para compresión de voz, cada uno de estos algoritmos involucra diferentes retardos. Con PCM, ADPCM y EADPCM tenemos que el

retardo del algoritmo es de 0,125 mseg (tiempo entre muestras PCM) Con G.729, G711, G723, etc. tenemos diferentes retardos de algoritmo.

Para comprimir la voz, G.729 utiliza segmentos de voz de 10 mseg (correspondientes a recolectar 80 muestras PCM) a los cuales les aplica el algoritmo respectivo para lograr la compresión. Adicionalmente, para comprimir esos 10 mseg. de voz, el algoritmo analiza un segmento de voz de 5 mseg. posterior al segmento de 10 mseg de voz que está comprimiendo. De esta manera se tiene que el retardo de algoritmo de G.729 es de 15 mseg.

Por otro lado, G.711 opera con segmentos de voz de 0,125 mseg. (correspondiente a recolectar 1 muestra PCM) y no analiza segmentos de voz posteriores al que está comprimiendo.

En el caso de G.723, utiliza segmentos de voz mucho mayor al algoritmo anterior: 30 mseg. (correspondientes a 240 muestras PCM). Para la compresión de los segmentos de 30 mseg el algoritmo tiene que analizar un segmento de voz de 7,5 mseg. adicionales al segmento de voz que está comprimiendo, con lo cual el retardo del algoritmo es de 37,5 mseg.

Por otro lado tenemos los retardos de algoritmo de los compresores de vídeo. Si se utiliza la información del cuadro siguiente para codificar el cuadro actual (facilidad disponible con H.261) y se utilizan 10 cuadros por segundo, se tiene que el retardo del algoritmo es de 100 mseg. Se hace necesario esperar 100 mseg. para obtener el cuadro siguiente para poder procesar el cuadro actual.

Adicional al retardo del algoritmo, tenemos el retardo ocasionado por el **procesamiento del algoritmo**. Este retardo depende directamente de la circuitería utilizada y cuanto mayor es la velocidad y capacidad del procesador y mayor la velocidad de acceso a las memorias, menor será el tiempo de procesamiento. Este retardo también depende de la complejidad del algoritmo utilizado, que cuanto más complejo, mayor número de instrucciones requiere y mayor retardo presenta.

Como se vio, existen varios métodos de compresión, donde cada uno de ellos posee diferentes retardos, los menores retardos se logran con PCM y ADPCM (pero también son los que requieren mayor ancho de banda) y el mayor retardo es el que se obtiene utilizando G.723 (pero es el que utiliza un menor ancho de banda).

En definitiva, la elección del protocolo de compresión, determinará el retardo causado por la compresión. Siendo importante que la elección de este conjunto de parámetros se haga tomando como base las características del sistema.

5.4.1.2. Retardo de empaquetamiento de la información.

Como se vio anteriormente, la duración de los segmentos de voz que procesa el algoritmo de compresión depende del algoritmo que se está utilizando.

G.728 utiliza segmentos de voz de 0,625 mseg. y la velocidad del algoritmo es de 16 Kbps. De esta manera se tiene que el segmento de voz es representado por 10 bits (0625mseg. x 16 Kbps). Si solo estos 10 bits se empaquetan en una trama IP se tiene un overhead (sobre carga) muy grande, y por lo tanto un desperdicio importante de ancho de banda.

Usualmente, se reúnen varios segmentos de voz en un solo paquete de información, con la finalidad de disminuir el overhead en la comunicación. Esto tiene como contraparte un mayor retardo. Así, si se reúnen 40 segmentos G.728 de voz, el overhead pasa a ser 11% pero el retardo de empaquetamiento pasa a ser de 25 mseg. (0,625 mseg x 40).

Si la voz comparte un mismo canal lógico que los datos, entonces se puede reunir tanto datos como voz en un solo paquete. De esta manera, la voz y los datos comparten el mismo paquete pero diferentes subpaquetes, cada uno de ellos con la identificación adecuada que permite al receptor diferenciar los dos tipos de información recibida. Con esto se logra utilizar el ancho de banda de una manera mucho más eficiente, disminuyendo el overhead en la comunicación.

De igual manera, se puede combinar diferentes conversaciones en un solo paquete de información, diferenciando cada una de ellas por un identificador.

Al reunir en un solo paquete diferentes segmentos de la misma conversación ó de diferentes conversaciones, y/o segmentos de datos, se logra una mejor utilización del ancho de banda, pero a consta de mayores retardos.

Lo importante es configurar los equipos de usuario de forma tal de que la combinación de segmentos de información en un solo paquete no traiga como consecuencia retardos excesivos que afecten la comunicación. Para lograr comunicaciones de voz similares a las obtenidas a través de las líneas telefónicas, se trata de que el retardo total ida y vuelta no supere el medio segundo.

Cuando se transmite vídeo, los segmentos de voz se combinan con los segmentos de vídeo, lográndose con esto una utilización adecuada del ancho de banda.

5.4.1.3. Retardos por serialización.

Este retardo es el tiempo que tarda el paquete en ser transmitido en su totalidad hacia la WAN cuando el mismo ya se encuentra de primero en la “cola” de transmisión del CPE. Cuanto más grande es el paquete mayor será el tiempo para que este sea transmitido en su totalidad hacia la WAN y

cuanto menor sea la velocidad del enlace también será mayor el retardo de serialización (retardo de serialización = tamaño del paquete / velocidad del enlace).

Así, por ejemplo, si tenemos un paquete de 2100 bytes y la línea es de 64 Kbps, el tiempo que tarda este paquete en ser recibido en su totalidad por la WAN es de 262,5 mseg ([2100 bytes x 8 bits/byte] / 64000 bits/seg]). Si el paquete es de 255 bytes, el retardo de serialización será de 31,875 mseg.

De esta manera se logra observar que el limitar el tamaño de los paquetes es muy importante no sólo para disminuir los retardos de espera en cola, sino que también para disminuir los retardos de serialización.

5.4.1.4. Retardo de espera en cola.

Cuando se requiere transmitir un paquete de información, pero otro paquete se está transmitiendo en ese momento, hay que esperar a que termine la transmisión del mismo antes de proceder a transmitir el otro paquete. El tiempo que transcurre debido a esta espera de que el otro paquete se transmita se denomina retardo de espera en cola.

Si el tamaño del paquete que se está transmitiendo es de, digamos, 1500 bytes (tamaño de paquete común en redes Ethernet) y el enlace del equipo a la WAN es de 64 Kbps, entonces si el paquete se está comenzando a transmitir, el tiempo de espera en cola será de 187.5 mseg. ([1500 bytes x 8 bits/byte] / [64000 bits/seg]). Como se aprecia, cuanto mayor sea el tamaño del paquete, mayor será el tiempo de espera (tiempo de espera = tamaño del paquete / velocidad del enlace de transmisión). Para redes Token Ring el tamaño del paquete es usualmente de 2100 bytes, en estos casos el tiempo de espera sería de 262 mseg.

Si bien, cuando se requiera transmitir un paquete de voz, y supongamos que ya existan tres paquetes de datos con las características anteriores, en espera de ser transmitidos; si no se realiza ningún procedimiento adicional, el paquete de voz comenzará a ser transmitido después de esperar 562 mseg (3paquetes x 1500 bytes x 8 bits/Byte / 64000bits/seg). Como podemos ver, este retardo es excesivo y no permite que se obtenga una buena calidad en la conversación.

Sin embargo, si se a cada tipo tráfico se le asigna una prioridad diferente, se podría reducir dicho tiempo de manera significativa. Esto significaría, dado el ejemplo, que cuando se genera el paquete de voz, el mismo no se coloca detrás de los tres paquetes de datos que se generaron previamente, sino que se coloca en otra cola de mayor prioridad.

Pero aun no resulta suficiente, el hecho de asignar prioridades a la información a transmitir para minimizar los retardos de espera en cola a valores adecuados. Volviendo al ejemplo, supongamos que uno de los paquetes de datos ya se estaba transmitiendo cuando se generó el paquete de voz, entonces, el paquete de voz se transmitirá antes de los dos últimos paquetes de datos, sin embargo, deberá esperar porque se termine de transmitir el primer paquete de datos que ya estaba en proceso de transmisión. Dicha espera pudiera ser de hasta de 187,5 mseg ([1500 bytes x 8 bits/byte] / 64000 bits/seg]). Como podemos ver, dicho retardo sigue siendo excesivo.

La forma de minimizar este retardo, consiste en segmentar los paquetes de datos. Así, un paquete de 1500 bytes puede ser segmentado en, digamos, 15 paquetes de 100 bytes. De esta manera, y volviendo al supuesto anterior, ya no tendríamos 3 paquetes de 1500 bytes en cola, sino que tendríamos 45 paquetes de 100 bytes en cola. Ahora bien, dado que el paquete de voz tiene prioridad sobre los de datos, éste deberá esperar a lo sumo, a que un solo paquete de datos se transmita. Siendo ahora los paquetes de datos de solamente 100 bytes, la espera será a lo sumo de 12,5 mseg (100 bytes x 8 bits / 64000 bits /seg).

De esta manera podemos ver como mediante el uso de prioridades bajamos el tiempo de espera de 562 mseg a 187.5 mseg y combinando este procedimiento con el de segmentación se logró bajar el tiempo de espera a tan sólo 12,5 mseg.

Así que, los retardos de espera en cola pueden ser de una magnitud considerable, por lo tanto deben ser cuidadosamente tratados. Para minimizar los impactos de los retardos de espera en cola, se deben segmentar los paquetes de información y asignar prioridades a los mismos.

5.4.1.5. Retardo de propagación.

El retardo de propagación está relacionado con la transmisión de una señal a una distancia considerable. Por ejemplo, una línea de fibras ópticas a larga distancia impone un retardo de propagación de unos 5 μseg. por kilómetro. A medida que las innovaciones técnicas reducen el número de repetidores necesarios para redes de fibras ópticas, las velocidades de transmisión por dichas redes aumentan, pero las limitaciones físicas impiden una gran reducción en el retardo de propagación de extremo a extremo. Sin embargo, la topología de la red puede controlarse para mantener el retardo de propagación a un mínimo, haciendo que los paquetes tomen las rutas más directas.

5.4.1.6. Retardo en el buffer.

Como se ha dicho con anterioridad, la voz y el vídeo requieren que los paquetes de información sean reproducidos de manera constante. Dado que el manejo del ancho de banda de las redes de paquetes es bajo demanda, entonces, en diferentes instantes de tiempo, la red experimentará diferentes cargas y por lo tanto, la llegada de los paquetes al equipo destino no se realizará de manera constante.

Para que los paquetes de información puedan ser reproducidos de manera constante, se hace necesario almacenar una determinada cantidad de los mismos, y luego reproducirlos de manera constante.

Dicho almacenamiento implica un retardo, ya que una cierta cantidad de paquetes debe ser almacenada antes de ser enviada a su usuario final. La idea básica es que este tiempo de almacenamiento de un paquete sea tal que, en los momentos en que la red experimente una carga pesada, los paquetes almacenados en buffer no se agoten y se pueda seguir suministrando los mismos de una manera relativamente constante.

Supongamos que el tiempo promedio entre los paquetes es de 25 mseg, y que existe una probabilidad considerable, de digamos 10% de que, en picos de carga alta de la red, lleguen dos cadenas de paquetes separadas por un tiempo de 100 mseg. Entonces, para que no se agote la memoria, se deberá almacenar al menos cuatro paquetes de información antes de enviarlos a su destino final. Dado a las características de la red de paquetes, siempre existirá la probabilidad de que ocurran retardos más considerables, pero si la probabilidad de dichos retardos es muy baja, digamos de menos del 0,1%, se aceptará la pequeña degradación de la voz ocasionada por la variación de retardos, y no se considerará para el diseño del tiempo de almacenamiento en memoria.

5.4.1.7. Retardos de descompresión.

Hace refieren al tiempo que se tarda en descomprimir la voz (o video). Estos tiempos dependen de la complejidad de descomprimir el algoritmo utilizado y del hardware utilizado para ello. Para descomprimir la voz usualmente no se toma tiempos mayores a 4 mseg. Por lo que no resultan tan significativos como los anteriores, por lo que no se analizaran detalladamente.

5.4.2. Variación del retardo (Jitter).

Otro factor de importancia en la transmisión de voz, es el ocasionado por las variaciones de retardos existente entre los paquetes. Por su filosofía de funcionamiento, la información que viaja a

través de las redes de paquetes experimenta retardos variables de tiempo para llegar a su destino. Estas variaciones de retardo se deben a que el ancho de banda se utiliza bajo demanda y de manera compartida, por lo que cuando se requiere mayor uso de ancho de banda, los retardos de transmisión son mayores que cuando se requiere menor ancho de banda.

La calidad de la voz transmitida (así como también, el vídeo) depende en gran parte de que a la(s) persona(s) que está(n) viendo y/o escuchando este tipo de información les llegue la misma de manera relativamente constante. Variaciones bruscas de los retardos provocan que la voz se escuche de una manera muy diferente a la original, y hasta pudiendo ocasionar que se haga totalmente ininteligible. En lo que respecta al vídeo, las variaciones bruscas de retardo ocasionan que los movimientos de las personas, objetos, etc. sean reproducidos de una manera totalmente artificial, muy alejados de sus características originales, y provocando por tanto una degradación en la calidad de la información.

Las variaciones de los retardos entre paquetes viene dada por los retardos de espera en cola. Dado que el número de los paquetes en cola y el tamaño de los mismos depende de las condiciones de tráfico específicas en cada momento dentro de la red IP.

El jitter entre el punto inicial y final de la comunicación debiera ser inferior a 50 mseg. Si el valor es menor a 50 mseg el jitter puede ser compensado de manera apropiada. En caso contrario debiera ser minimizado.

Por ejemplo, si el equipo que transmite el paquete posee una línea de 64 Kbps con la WAN y en el momento que se quiere transmitir el paquete hay otro transmitiéndose de, digamos 1500 bytes, el paquete deberá esperar 187 mseg ([1500 bytes x 8 bits/byte] / [64000 bits/seg]). Si, el paquete en cuestión llega al nodo pero existen, digamos 40 paquetes antes de él de 1550 bytes que se requieren transmitir por la misma troncal, siendo esta de 34 Mbps, el paquete en cuestión deberá esperar 14,6 mseg ([40 paquetes x 1550 bytes x 8 bits/byte] / [34000000 bits/seg]). Si el paquete en cuestión debe atravesar por tres troncales con situaciones de carga similares, la espera por espera en cola de dicho paquete, a lo largo de toda la red será de 43,8 mseg. De igual manera, cuando al puerto destino de, digamos, 2 Mbps existen 4 paquetes de 1500 bytes en cola, cuando llega el paquete al que estamos haciendo referencia, dicho paquete deberá esperar 24 mseg. antes de que comience a ser transmitido. Sumando todos estos tiempos, se tendría un retardo total por espera en cola de 269 mseg. Si otro paquete que se transmite a la red no consigue ningún paquete en cola antes que él, el tiempo de espera en cola bajaría de 269 mseg (caso anterior) a 0 mseg.

El retardo variable depende de la cantidad de paquetes que se encuentren en las diferentes colas de espera, del tamaño de dichos paquetes y de la velocidad de las líneas. Dado que la carga en la red varía a cada instante y los paquetes poseen tamaños diferentes, los retardos varían constantemente.

De esta manera observamos, como en las redes de conmutación de paquetes, la variación de retardos es algo intrínseco en su filosofía de funcionamiento, y por tanto, se requieren técnicas adicionales que permitan la transmisión de voz y vídeo a través de las mismas, ya que, como vimos, este tipo de tráfico se debe entregar al usuario de una manera relativamente constante.

Además, como se dijo anteriormente, con la finalidad de obtener una calidad para el tráfico de voz similar a la que se obtiene con las redes telefónicas tradicionales, el retardo total en un sentido debe mantenerse por debajo de 250 mseg, por lo que hay que buscar las técnicas adecuadas para que un gran porcentaje de los paquetes (digamos el 98%) se mantenga por debajo de este umbral.

Para controlar este fenómeno, la solución más ampliamente adoptada es la utilización del **"jitter buffer"**. El jitter buffer consiste básicamente en asignar una pequeña cola o almacén para ir recibiendo los paquetes y sirviéndolos con un pequeño retraso, permitiendo así a las tramas más lentas arrivar a tiempo para ser ubicadas en la secuencia correcta. Si algún paquete no está en el buffer (se perdió o no ha llegado todavía) cuando sea necesario se decarta. Normalmente en los teléfonos IP (hardware y software) se pueden modificar los buffers. Un aumento del buffer implica menos perdida de paquetes pero más retraso. Una disminución implica menos retardo pero más pérdida de paquetes.

Dada estas condiciones, se debe encontrar un tamaño óptimo del buffer que permita controlar el jitter sin aumentar el retardo a niveles excesivos. Algunos equipos comerciales lo ajustan dinámicamente de acuerdo con la variabilidad de la red.

Si la red de datos está bien construida y se toman las precauciones apropiadas, la variabilidad del retardo es normalmente un problema menor y el buffer de jitter no contribuye significativamente al retraso total de extremo a extremo.

Es aquí, donde las **timestamps** de RTP juegan un papel importante, al ayudar a determinar qué el jitter, si lo hubiera, existe dentro de la red.

5.4.3. Deterioro por el eco y su control.

El eco en la red es el resultado del acoplamiento entre el trayecto de transmisión y el de recepción, que hace que el habla saliente vuelva a la persona que la originó. Por lo general, este

problema aparece en el contexto de las comunicaciones de PC a teléfono, de teléfono a PC o de teléfono a teléfono, y es causado por los componentes electrónicos de las partes analógicas del sistema que reflejan una parte de la señal procesada. Este eco es problema cuando el retardo completo (ida y vuelta) en la red es mayor que 50 mseg.

Este umbral es subjetivo y varía persona a persona. Un valor de retardo mas allá de 65 mseg será percibido como un verdadero eco (el hablante oirá su propia voz después de haber hablado), entre 30 y 65 mseg el retardo le añadirá a la voz un sonido que se conoce como "túnel" y un valor de retardo por debajo de 30 mseg el efecto es imperceptible.

En las comunicaciones telefónicas, existen dos tipos de eco. Uno tiene alto nivel y poco retardo y se produce en el circuito híbrido de 2 a 4 hilos local; mientras que otro es de bajo nivel y gran retardo y se produce en el circuito separador híbrido remoto.

La intensidad de un eco depende de dos factores: la **amplitud de la señal** que produce el eco y el **tiempo** que le toma para volver a la persona que habla. La amplitud es una función de la intensidad del acoplamiento entre los canales de transmisión y de recepción. Es caracterizada como "pérdida del trayecto del eco", que es la diferencia en nivel (en dB) entre el habla de entrada original y la señal que hace eco. Para una pérdida del trayecto del eco determinada (es decir, un nivel constante), cuanto más prolongado sea el período entre el habla original y el eco que vuelve, más fuerte o perceptible, parecerá el eco

Un eco que es inaudible en una red de conmutación de circuitos puede ser audible con la transmisión por paquetes debido al mayor retardo. Las interconexiones entre redes de paquetes y redes con conmutación de circuitos son particularmente susceptibles al deterioro causado por el eco. Las reflexiones de dispositivos híbridos bifilares a tetrafilares usados en líneas analógicas en redes con conmutación de circuitos crean un eco intenso; la planificación de pérdidas en la RTPC y las reglas para redes privadas conectadas a la RTPC tienen mayormente el objeto de mantener los ecos de híbridos y otros ecos por debajo del umbral de audibilidad. El retardo relacionado con la transmisión por paquetes viola las suposiciones técnicas de la red con conmutación de circuitos. Por lo tanto, el control del eco en la interfaz entre las redes es esencial para proteger a los usuarios de ambos extremos contra el eco.

Si bien las redes totalmente digitales no tienen trayectos de eco, pueden aun así estar sujetas al eco producido por el acoplamiento en los dispositivos de los extremos. El acoplamiento acústico, en el que el micrófono capta la salida del receptor, es una fuente posible. La captación eléctrica entre

circuitos analógicos (diafonía) es otra. Ese eco es por lo general menos intenso que el del híbrido, pero puede llegar a ser audible con un retardo prolongado.

Utilizando redes ATM, este retardo suele ser menor de 50 mseg, por lo que no se requiere de técnicas especiales para hacer frente a sus consecuencias. Sin embargo, en las redes IP, el retardo es usualmente mayor a este valor, por lo que se requiere el empleo de técnicas especiales que eliminen ó minimicen estos efectos negativos. En este caso hay dos posibles soluciones para evitar este efecto tan molesto.

- **Canceladores de eco.** Es el sistema por el cual el dispostivo emisor guarda la información que envía en memoria y es capaz de detectar en la señal de vuelta la misma información (tal vez atenuada y con ruido). El dispostivo filtra esa información y cancela esas componentes de la voz. Requiere mayor tiempo de procesamiento.
- **Supresores de eco.** Consiste en evitar la señal emitida sea devuelta convirtiendo por momentos la linea full-duplex en una linea half-duplex de tal manera que si se detecta comunicación en un sentido se impide la comunicación en sentido contrario. El tiempo de conmutación de los supresores de eco es muy pequeño. Impide una comunicación full-duplex plena.

5.4.3.1. Canceladores de eco.

El control del eco es necesario en la interfaz entre una red de paquetes y una red con conmutación de circuitos en donde pueda haber híbridos. Para ello, se establece la recomendación G.168 de la ITU-T, que define el desempeño de los canceladores de eco.

Los canceladores de eco aprenden como el circuito que tienen conectado refleja la señal proveniente de la WAN. Estos equipos observan y ajustan el filtro adaptable para reproducir esta reflexión, mejorando así la perdida del trayecto del eco hasta en 26 – 30 dB. Los ajustes se realizan en menos de medio segundo después de comenzada la conexión.

Los ajustes realizados por el cancelador de eco incluyen el cálculo tanto del retardo de la reflexión como de su amplitud proveniente de los diferentes puntos del circuito: del híbrido del CPE, del teléfono y de cualquier otro punto que genere reflexiones (cambio de calibre de cables, “bridged taps”, etc.).

De esta manera, el cancelador de eco aprende las características del circuito que tiene conectado y como ocurre el retorno del eco: la relación amplitud, frecuencia y retardo. Entonces almacena una copia de la señal transmitida, le aplica la respuesta que aprendió, y le substrae a la señal

que recibe la señal almacenada, cancelando con esto el eco. Cualquier residuo del eco es removido usando un procesador no lineal, que elimina todas las señales por debajo de cierto umbral.

5.4.3.2. Supresores de eco.

Para ofrecer un servicio de ToIP, las pasarelas tendrán que procesar el eco generado por la transferencia de dos a cuatro hilos (desadaptación de impedancias), de lo contrario, no será posible utilizar el servicio con equipos analógicos clásicos. Como solución, se están instalando compensadores de eco de alta calidad en la pasarela de la red.

Conocido también como conmutador vocal (ITU-T G.165/168), detecta una señal en el trayecto entrante o saliente, y conmuta la atenuación en el otro trayecto para reducir el nivel de cualquier señal de retorno. Esta técnica de supresión puede usarse en teléfonos con parlantes, audífonos, y microteléfonos inalámbricos, en los que es común el acoplamiento acústico. La conmutación vocal es una función más simple que la compensación de eco, pero es menos transparente a la dinámica de la conversación, y puede sumar sus propios deterioros a la señal de habla.

5.4.4. Supresión de silencio y ruidos.

Es una gran ventaja del empaquetamiento de la voz ya que no se generan paquetes a trasmitir durante pausas en medio de las frases, o silencio de una persona mientras la otra está hablando. Se debe establecer diferencia entre habla y silencio, el no transmitir paquetes de silencio y la generación de los silencios correspondiente al otro extremo. Con este parámetro activado, se consigue que la transmisión de paquetes (uso de ancho de banda) se reduzca a las situaciones en que los agentes están hablando. El resto del tiempo, cuando no existe voz a transmitir, se libera el ancho de banda. Considerando este aspecto, se puede afirmar que el tamaño medio de un paquete de voz durante una conversación es de 8 Kbps.

De esta forma, aunque realmente el caudal en datos de la voz codificada no requiere grandes anchos de banda, se puede decir que una conversación full-duplex consume máximo 22kbps. Durante una conversación normal por teléfono, sólo en pequeños intervalos ambos locutores hablan simultáneamente, la tecnología actual provee un sistema conocido como supresión de datos en silencio, el cual no envía datos si no hay sonido.

Para la Supresión de Ruidos, se usa el VAD (Vocee Activity Detection) que detecta la diferencia entre la existencia de voz y los silencios, de esta forma no transmite los paquetes de

silencio y se genera el llamado ruido de confort al otro extremo del enlace. Tanto la supresión de datos como la conversión de la voz en datos se realiza de dos modos, por hardware y por software.

5.4.5. Perdidas de paquetes.

En la red telefónica tradicional con conmutación de circuitos, a una llamada se le asigna una conexión física entre puntos extremos, y el circuito permanece dedicado a ese canal mientras dure la llamada. En cambio, las redes de paquetes dividen las transmisiones de voz, video, fax y datos en pequeñas muestras o paquetes de información. Cada paquete tiene un encabezamiento que determina adónde va el paquete y suministra información para el rearmado cuando el paquete llega a destino. Los paquetes se desplazan independientemente, y son intermezclados con paquetes de otro tráfico de la red a lo largo del trayecto. El tiempo de desplazamiento a través de la red varía según el paquete.

A menos que la red esté precisamente adaptada a la carga de tráfico de pico, existe una cantidad de paquetes que a veces no llegan a su destino. Esos paquetes perdidos producen lagunas en las comunicaciones vocales, que pueden causar chasquidos, silenciamiento, o un habla ininteligible. En la transmisión de datos, el remedio para la pérdida de paquetes (al no ser sensibles a los retardos) consiste en volver a enviar los paquetes perdidos, pero eso no da resultado en el caso de conversaciones habladas sensibles al tiempo, en las cuales es mejor perder un paquete que transmitirlo con demasiado retardo.

Generalmente, hay dos maneras de perder paquetes. Pueden perderse en nodos de la red a causa de un desborde en la memoria intermedia, o porque un encaminador congestionado los descarta deliberadamente para reducir la congestión. Estos paquetes realmente se pierden, y nunca llegarán a destino. Las interrupciones en la red debidas a dispositivos fuera de servicio o a cortes de las fibras ópticas también pueden causar la pérdida de paquetes. Esos eventos pueden causar grandes pérdidas de paquetes, que se distribuirán entre los diferentes canales virtuales que la red esté cursando en ese momento.

Segundo, los paquetes pueden retrasarse si toman una ruta más larga o pasan tiempo en la cola de un dispositivo, causando una variabilidad en la hora de llegada al extremo receptor. La memoria intermedia de fluctuaciones (jitter buffer) se usa para reducir la variabilidad, reteniendo los paquetes para la entrada al descodificador. La demora introducida por dicha memoria intermedia se sintoniza con la variación prevista del retardo de la red. Esa demora determina el tiempo máximo que un paquete puede tomar para llegar todavía a tiempo para ser descodificado. Los paquetes que lleguen

después del retardo prescrito pierden su turno, y prácticamente se pierden, ya que la operación de la voz no puede aguardar a que aparezcan los paquetes tardíos.

La tasa de pérdida de paquetes dependerá de la calidad de las líneas utilizadas y del dimensionamiento de la red. Para que la calidad vocal sea aceptable, dicha tasa de pérdida de paquetes ha de ser menor que el 5 % en WAN y el 2 % en LAN.

El fax no incorpora procedimientos de recuperación de errores, sin embargo muchos errores no son notorios ante el ojo humano y la degradación no molesta.

En el caso del habla, si la voz es comprimida, la pérdida de información se convierte en un gran problema, ya que puede ocurrir que varios fonemas se pierdan y de ocurrir varias perdidas puede resultar en la degradación de la calidad de la voz. Cada paquete IP contiene entre 40 y 80 ms. de voz, que corresponde a la duración de unidades fundamentales de voz, como son los fonemas: cuando se pierde un paquete, se pierde un fonema. Aunque el cerebro humano es capaz de reconstruir algunos fonemas perdidos, demasiadas pérdidas pueden generar una señal ininteligible.

En una red que funcione sin control de admisión de llamadas, y sin un protocolo de QoS habilitado, la pérdida de paquetes es incontrolable ante la congestión. Las consecuencias de la congestión dependen del tipo de red, de la proporción de tráfico de voz y de datos, del número de saltos, y de la duración del evento. El número de paquetes tardíos puede minimizarse aumentando el tamaño de la memoria intermedia de fluctuaciones, pero una memoria más larga aumenta el retardo de extremo a extremo. Entonces es necesario tener otra manera de hacer frente a las pérdidas de paquetes.

Una solución posible para reducir la pérdida de paquetes consiste en utilizar sistemas de corrección de errores que tengan codificación redundante y adaptable, es decir, variable de acuerdo con las pérdidas de paquete estadísticamente observadas en la red en determinado momento. Es posible obtener, cuando se utilizan dichos sistemas, unos niveles muy altos de calidad sonora, incluso por Internet. No obstante, esta solución genera otras dificultades relacionadas con el retardo total de transmisión, que, como ya se ha indicado, ha de controlarse si se ha de usar la red para telefonía.

También, como posible solución se podría interpolar el paquete perdido haciendo uso de los paquetes recibidos con anterioridad, transmitiendo al usuario el resultado de esta interpolación. Este método trabaja bien cuando la pérdida de paquetes es infrecuente, pero no es de utilidad cuando existen ráfagas de paquetes perdidos.

Otro método que se puede utilizar para hacer frente a la pérdida de paquetes, es el envío de información redundante. De esta manera, cuando existen pérdidas de paquetes se puede utilizar la

información redundante de los paquetes recibidos para reconstruirlos. La desventaja de este método es la mayor utilización de ancho de banda y de mayores retardos.

Todo esto debe ser tomado en cuenta cuando se utiliza la red IP, como medio para aplicaciones de telefonía, que por su objetivo de diseño y prestaciones, tienen distintas características.

5.4. 5.1. Para evitar paquetes perdidos y datos faltantes.

La mejor manera de evitar paquetes tardíos y perdidos es proyectar la red de manera de excluir o minimizar las demoras y otros factores que contribuyan a éstas. Esto significa que el control de la congestión (llamado control de admisión de llamadas) debe estar en servicio para evitar que se llenen las colas de los encaminadores, lo cual causa variaciones en el retardo, y posiblemente un desborde. A continuación se describen estrategias para minimizar los paquetes perdidos. Algunas requieren su ejecución en toda la red, y otras pueden usarse en un solo canal para mejorar la calidad de una llamada individual.

5.4.5.1.1. Protocolos QoS.

La ejecución de protocolos de QoS en la red facilita la transmisión de paquetes vocales en las diversas pasarelas y encaminadores, reduciendo las fluctuaciones y la pérdida resultante de paquetes. La eficacia de esto es mayor si la red está cursando una proporción considerable de tráfico de datos. Si la red cursa una proporción elevada de tráfico vocal, podrá todavía haber demoras de colas en los encaminadores, con el consiguiente aumento de las fluctuaciones y las pérdidas de paquetes.

5.4.5.1.2. Control de admisión de llamadas.

En las redes con una alta proporción de tráfico vocal, el control de admisión de llamadas puede prevenir la congestión limitando el número de llamadas activas a través de diversos nodos de la red. Esto es análogo a la “señal rápida de ocupado” en la red con conmutación de circuitos. Cuando no hay control de admisión de llamadas y el número de llamadas aumenta por encima de la utilización recomendada, la calidad de las llamadas en la red declina a medida que aumentan el retardo, la fluctuación y la pérdida de paquetes.

5.4.5.1.3. Memoria intermedia adaptable de fluctuaciones.

Cuando un paquete vocal llega a destino, es retenido en la memoria intermedia de fluctuaciones hasta que el descodificador está listo para el paquete. Los paquetes tardíos son

descartados. Un aumento en la tasa de pérdida de paquetes en el descodificador puede significar que hay más paquetes que llegan tarde. Se puede usar un algoritmo adaptable para ajustar el retardo de la memoria intermedia de fluctuaciones según aumenta y disminuye la tasa de pérdida de paquetes. Dicho ajuste ayuda a minimizar el número de paquetes tardíos cuando el sistema está congestionado, y evita agregar demoras innecesarias cuando se alivia la congestión. La memoria intermedia es ajustada durante los períodos de silencio, de manera que el desplazamiento temporal de la señal es transparente para los usuarios.

5.4.5.1.4. Envío de datos duplicados.

El envío de datos redundantes también corrige la pérdida de paquetes vocales. Para emplear esta solución, la información de un paquete es copiada al paquete siguiente de la secuencia, y se usa si el paquete original se pierde o se retrasa. Con algunos codecs, tales como el G.729, incluso los datos incompletos pueden ser útiles para reparar la laguna. Como la descodificación de los datos duplicados debe aguardar la llegada de otro paquete si se pierde el original, este método de supresión de pérdidas agrega un retraso más.

5.4.5.1.5. Tasa de pérdida de paquetes.

Esta variable mide el comportamiento del enlace para detectar congestión. Como se ha mencionado inicialmente, IP es un protocolo de transporte basado en el paradigma del mejor esfuerzo "Best Effort", que no garantiza que un paquete que es transportado por una red IP llegue finalmente a su destino. Es estos términos, la tasa de pérdida de paquetes mide cuantitativamente este factor. Usualmente en un enlace usado como subred de interconexión no deben observarse pérdidas mayores al 1% salvo que el circuito este congestionado o que existan problemas a nivel de transmisión Física, o que los nodos (routers) extremos estén sobrecargados.

Para medir la pérdida de paquetes se usa también ICMP (Internet Control Message Protocol), enviando un número finito de paquetes, y contabilizando el número de paquetes recibidos desde la interfase remota. Estos resultados son posteriormente presentados en forma gráfica. Al igual que la latencia, la tasa de pérdida de paquetes es una variable muy importante a considerar en el análisis de aplicaciones de VoIP, y en las aplicaciones relacionadas con la distribución de audio y video en tiempo real, sobre redes de datos.

5.4.6. Requerimientos de ancho de banda.

Una llamada telefónica ocupa un ancho de banda de unos 32 Kb. Este ancho de banda debe estar disponible para que la comunicación sea fluida. Si la línea de datos se satura repentinamente, puede deteriorarse la calidad o incluso cortarse la llamada. Además puede ser determinante el tiempo de latencia, para evitar el efecto de retardo en la conversación, este efecto no será perceptible si la latencia es inferior a 50 ms, pero si es superior, puede hacerse molesto. Un remedio a estos problemas consiste en contratar con nuestro proveedor de comunicaciones lo que se denomina "calidad de servicio, QoS", que garantiza que siempre hay un determinado ancho de banda disponible para la telefonía.

Cabe recordar que conforme el ancho de banda disminuye, la calidad de sonido se degrada en mayor grado. Es por ello que la elección de la codificación que vaya a implementarse en la red deberá tomar en cuenta esta consideración.

Codec de Audio	Ancho de banda comprimido	Ancho de banda paquetizado	Ancho de banda en Ethernet
G723	6,3 Kbps	17 Kbps	27,2 Kbps
G729	8 Kbps	24 Kbps	28,8 Kbps
G711	64 Kbps	74,6 Kbps	84,7 Kbps
FAX	4,8 Kbps	12,8 Kbps	20,4 Kbps

Habitualmente en un entorno LAN, donde se utiliza tecnología Switch a 10 o 100Mbps, se elige la compresión G711 con un ancho de banda de 84,7Kbps. ya que se obtiene mayor calidad y se dispone suficiente ancho de banda. En cambio en el entorno WAN donde el ancho de banda sea más escaso y costoso, se elige la compresión G723 con un ancho de banda de 27,2Kbps.

El ancho de banda puede reducirse 30 a 40% cuando se utiliza detección de silencios (VAD). Y en las líneas WAN, los Routers pueden utilizar la compresión de cabeceras IP (cRTP) para reducir las cabeceras de 40 a 24 bytes, pudiendo reducir hasta 16,41kbps en el caso del G723.

Por lo tanto, el ampliar el ancho de banda debe utilizarse como una solución puntual para resolver determinadas situaciones de congestión en determinados puntos de la red y para determinados tipos de redes. Es medianamente factible para redes LAN y prácticamente imposible

para redes WAN, mientras los precios sigan siendo tan elevados. Es por tanto, una solución costosa, con durabilidad mínima debido al crecimiento del tráfico de la red y de las necesidades de ancho de banda de determinados tipos de tráfico.

La QoS sin embargo, conlleva, entre otras cosas, una correcta gestión del ancho de banda. Presentándose como la forma más eficiente, hoy en día, para la mejora de toda red que se precie. Es, en definitiva, la solución por la que deberían apostar todas las empresas para mejorar su red y, en consecuencia, su negocio.

5.5. MÉTODOS, HERRAMIENTAS Y SOFTWARE, QUE PERMITEN MEDIR PARÁMETROS DE QOS.

5.5.1. Como medir la Qos.

En las comunicaciones de ToIP, así como en otros tipos de aplicaciones, se debe constatar una medida de calidad fiable, para ofrecer un servicio rentable a la vez que sea satisfactorio al cliente. Con este fin, se ha demostrado que la audición de la voz depende directamente de las características más comunes de una red de paquetes IP.

Existen distintos valores en los que se puede estar interesado a la hora de evaluar la calidad de funcionamiento de la red: retardo de paquetes, ancho de banda, pérdidas, etc. También tiene importancia en que punto o puntos de la red se mide. Para un determinado tráfico, se puede medir el retardo que se produce extremo a extremo entre origen y destino, o el retardo en uno de los trayectos por los que atraviesa el tráfico. También es distinto medir a partir del instante en que se entrega un paquete al sistema operativo de un sistema final, que medir a partir del momento en que el primer bit sale por el medio físico.

Para ello se distinguen dos tipos de técnicas de medidas: medidas activas y medidas pasivas. Las técnicas activas o intrusivas son aquellas en las que se inyecta tráfico en la red con el objetivo de realizar las medidas, mientras que las técnicas pasivas o no intrusivas se limitan a observar el tráfico existente en la red.

5.5.2. Mediciones activas y pasivas.

5.5.2.1. Medidas activas.

La monitorización activa consiste en probar directamente las propiedades de la red generando el tráfico necesario para realizar la medida. Esto permite utilizar métodos de análisis mucho más

directos, pero también presenta el problema de que el tráfico introducido puede tener un impacto negativo en las prestaciones recibidas por otros tipos de tráfico.

Existen varios métodos activos para medir prestaciones de red tales como el ancho de banda disponible, el retardo, las pérdidas y para estimar las características enlace por enlace. Monitorizan la QoS del flujo de paquetes prueba para determinar la QoS de los usuarios indirectamente. Esto implica que asumimos implícitamente que la QoS de un usuario es la misma que los valores medidos con los paquetes de prueba.

Analicemos un poco más las desventajas:

- Si usamos un flujo de paquetes de prueba que simula el tráfico actual del usuario:
  - El flujo de paquetes de prueba produce una no despreciable cantidad de tráfico extra en la red y esto afecta a la QoS/prestaciones del tráfico de usuarios.
  - La QoS/prestaciones obtenidas de los paquetes de pruebas no es igual a la obtenida sin la influencia del flujo de paquetes de prueba.

- Si usamos paquetes pequeños de prueba y los enviamos en ciertos intervalos, como ping:
  - El tráfico extra puede ser despreciable, pero la QoS/prestaciones obtenidas desde el paquete de prueba no es igual a las experimentadas por los usuarios, en general.
  - Puede ser catalogado como tráfico hostil o intento de ataque. Por ejemplo, algunos routers rechazan tráfico ICMP o limitan su tasa, por si se trata de un intento de spoofing, etc.

5.5.2.2. Medidas pasivas

Llamamos medidas pasivas a las medidas realizadas a parámetros de la red normalmente vinculados al tráfico cursado de una forma transparente para la red, con el fin de que la medida en sí no perturbe ni influencie el comportamiento de la red. Esto se consigue con algún método no intrusivo para la red, haciendo una escucha o sniffing del tráfico cursado en determinados puntos de interés de la red, para su posterior procesado off-line o bien de forma dinámica. Introduciendo algún tipo de inteligencia (aplicación) a los elementos de red, como los routers, podemos no solo la posibilidad de identificar y cuantificar la cantidad de paquetes que transcurren por él sino que también podemos las características específicas de dichos paquetes. Realizando medidas pasivas se puede llegar a conocer la velocidad de transferencia de bits o paquetes, tasas de pérdida de los mismos, tiempo entre llegadas, niveles de encolamiento en los routers, etc.

La monitorización pasiva se puede clasificar en dos tipos: monitorización en dos puntos y monitorización en un punto.

La **monitorización en dos puntos** requiere dos dispositivos de medida desplegados en los puntos de acceso y salida de la red. Estos dispositivos, toman paquetes de datos de forma secuencial y los parámetros de prestaciones de la red como el retardo o las pérdidas pueden ser calculadas comparando los datos de los correspondientes paquetes tomados en cada punto. Si aplicamos la monitorización de dos puntos como medida de QoS/prestaciones:

- Todos los dispositivos deberían estar sincronizados en el tiempo.
- Requiere identificar cada paquete en los dos dispositivos por su cabecera y/o contenido. Este proceso de identificación puede ser tremendamente difícil cuando el volumen de paquetes es enorme, como en redes de gran escala, y este tipo de monitorización no es escalable.
- Para identificar los paquetes monitorizados, debemos recoger todos los paquetes de datos. Este proceso requiere un no despreciable ancho de banda.

La **monitorización de un punto** usa el mecanismo de asentimiento de TCP. Cuando se recibe un segmento TCP desde una fuente, se transmite un paquete de asentimiento para ese segmento. Entonces, monitorizando este par de paquetes en un punto de la red, podemos medir el retardo Round Trip Time entre ambos puntos. Los paquetes perdidos también pueden ser detectados de esta forma. Sin embargo, si aplicamos este tipo de monitorización, las medidas están restringidas a flujos TCP.

Si conseguimos extraer la información de interés de las medidas realizadas, entonces esa información es “libre”, en el sentido de que no hemos necesitado introducir ningún tipo de tráfico para conseguirla, siendo además, más cercanas a las prestaciones que el usuario realmente recibe de la red, pues se trata de tráfico real.

5.5.3. Herramientas y softwares.

5.5.3.1. PING.

El ping es la más sencilla de todas las aplicaciones TCP/IP. Envía uno o más datagramas (método activo, por lo tanto) a un host de destino determinado solicitando una respuesta y mide el tiempo que tarda en retornarla. Utiliza los mensajes Eco y Respuesta al Eco ("Echo Request", "Echo Reply") de ICMP. Ya que se requiere ICMP en cada implementación de TCP/IP, a los hosts no les hace falta un servidor separado para responder a los pings.

El RTT (Round Trip Time, Tiempo de Viaje Redondo, o de Ida y Vuelta) es calculado como la diferencia entre el tiempo en el que el echo request es enviado y el tiempo de la correspondiente respuesta es recibida por la aplicación ping. Una variación de este método es construir un paquete request ICMP con la marca de tiempo. Este paquete contiene tres marcas de tiempo: origen, recibida y transmitida. Si los hosts implicados tienen en el intercambio de marcas de tiempo tienen los relojes sincronizados, el retardo del camino directo puede ser calculado usando las marcas de tiempo origen y recibida. El retardo del camino de retorno puede ser calculado usando la marca de tiempo transmitida contenida en el paquete respuesta y el tiempo en el que el paquete respuesta llega al transmisor.

En la figura a continuación se muestra una salida mostrada por ping, observando como también se proporcionan los RTT mínimos, medios y máximos.

```
pythagoras: ~ > ping  - s betz . ericsson . se 100  5
PING  betz . ericsson . se : 100 data bytes
108 bytes from betz . ericsson . se (147 . 214 . 173 . 118) : icmp_seq=0. time=96 . ms
108 bytes from betz . ericsson . se (147 . 214 . 173 . 118) : icmp_seq=1. time=91 . ms
108 bytes from betz . ericsson . se (147 . 214 . 173 . 118) : icmp_seq=2. time=79 . ms
108 bytes from betz . ericsson . se (147 . 214 . 173 . 118) : icmp_seq=3. time=147 . ms
108 bytes from betz . ericsson . se (147 . 214 . 173 . 118) : icmp_seq=4. time=81 . ms

----betz . ericsson . se PING Statistics----
5 packets transmited, 5 packets received, 0 % packets loss
round-trip (ms)  min / avg / max = 79 / 98 / 147
```

Una herramienta equivalente a ping en la capa de transporte es **echoping**, utilidad que prueba los host remotos conectándose al servicio echo. Es capaz de probar conexiones UDP y TCP y además puede emitir una petición HTTP para probar la disponibilidad de un servidor Web. Al ser una implementación del nivel de aplicación el "servicio echo", algunos retardos extra se introducen en los tiempos de respuesta.

5.5.3.2. Traceroute.

Es una herramienta que combina muy inteligentemente, dos características de los protocolos que hacen posible Internet: TTL o expiración de los paquetes e ICMP

Para proteger a Internet del efecto de paquetes atrapados en ciclos de enrutamiento (retardos), los diseñadores de TCP/IP dotaron a cada datagrama IP de un contador al que llamaron TTL por las siglas de “Time To Live”. Esto es un número que limita cuántos saltos puede dar un datagrama, antes de ser descartado por la red. Cuando se introduce un datagrama IP a la red, el campo TTL es poblado con el número máximo de saltos que define la vida de ese datagrama. Cada enrutador por el que ese datagrama transita, resta uno a ese número. Cuando éste llega a cero, el datagrama es descartado.

Los paquetes ICMP sirven para muchas cosas: avisar que un enlace o que un dispositivo están congestionados, que se escogió un camino sub-óptimo para enviar un paquete, que no se puede acceder a un sitio en particular, etc. Uno de esos avisos es particularmente útil para “traceroute”: el aviso de que se excedió la vida útil del paquete.

Combinando estas dos herramientas, traceroute permite construir un mapa de la red de acuerdo como es vista desde un nodo en particular.

Una herramienta que usa el mismo mecanismo que traceroute es **pathchar**, sin embargo fue diseñada para un propósito diferente. Estima las prestaciones de cada host a lo largo de un camino desde una fuente a un destino. Envía una serie de paquetes UDP de varios tamaños a cada router (incrementando el TTL) y recoge información de cada salto de forma incremental. Usando el conocimiento de los anteriores saltos y la distribución del RTT en este salto, pathchar estima el ancho de banda, la latencia, pérdidas y las características de la cola en este salto.

Sin embargo, como pathchar hace mucho esfuerzo para caracterizar el camino de forma muy precisa, tiene una serie de desventajas, por lo que no es muy popular. Primero, porque tarda mucho en ejecutarse, y segundo porque altera mucho el estado de la red al introducir muchos paquetes de prueba.

5.5.3.3. Netflow e IPFIX.

Netflow (Networks-Flow o Flujo de Red), tecnología desarrollada por CISCO Systems en 1996, permite mejorar la capacidad de encaminamiento de sus routers. Siguiendo la filosofía “encaminar una vez, conmutar muchas veces”, identifica los flujos establecidos entre máquinas con el fin de agilizar el encaminamiento de futuros paquetes IP. Este software soporta ambientes basados en LINUX y/o Windows.

Para un router, un flujo de datos está constituido por un conjunto de paquetes IP con una misma combinación de atributos (direcciones y puertos origen y destino, tipo de protocolo de transporte, tipo de servicio e interfaz de entrada) en un intervalo de tiempo. Cuando se detecta un

nuevo flujo, Netflow guarda en la memoria interna la correspondencia entre el flujo y su interfaz de salida, de forma que para posteriores paquetes a consultas en sus tablas de encaminamiento, ahorrando de este modo, valiosos ciclos de CPU.

Precisamente, esta capacidad de los dispositivos de encaminamiento de obtener información referente a los flujos cursados puede ser aprovechada para medir y caracterizar el tráfico que atraviesa el router prácticamente en tiempo real, y ello de una manera convenientemente agregada facilita el análisis de la calidad de servicio.

Con el fin de ocupar el vacío existente en la definición de métricas que especifiquen de una manera formal el rendimiento de redes IP, el IETF organizó, en el año 1998, un grupo de trabajo denominado IP Performance Metrics (IPPM), encargado de formalizar parámetros que permitieran tanto a usuarios como proveedores de red cuantificar el estado de sus servicios de red. Si bien el grupo de trabajo IPPM define claramente aquellas métricas útiles en la caracterización de calidad de servicio QoS, no precisa el modo de obtención de dichas métricas.

Mediante el empleo de técnicas pasivas de análisis como **IPFIX (Internet Protocol Flow Information Export)** se puede disponer de una arquitectura no intrusiva e interoperable para calcular métricas de calidad de servicio. El hecho de ser un método pasivo permite disponer de numerosos puntos de medida sin que el tráfico de datos se vea afectado, mientras que el hecho de ser interoperable contribuye a que diversos operadores puedan colaborar entre sí para recabar información relacionada con sus enlaces y el tráfico intercambiado entre ellas.

Las métricas de OWD (One way delay, o retardo unidireccional) pueden ser útiles para determinar si la infraestructura de red se encuentra dentro de los márgenes de tolerancia impuestos por los servicios denominados de tiempo real como la VoIP o la videoconferencia. Asimismo el retardo unidireccional resulta crítico en el ancho de banda máximo alcanzable en las actuales redes Gigabit.

Un posible método de estimación del OWD consiste en disponer de dos o más dispositivos IPFIX, normalmente routers, con la misma base de tiempos, siendo el primero capaz de asegurar precisiones del orden de nanosegundos y del orden de milisegundos el último. De este modo es posible inferir el tiempo transcurrido entre el primer punto de medida y el último, definiendo de este modo un estimador directo del retardo unidireccional. Mediante técnicas de análisis de flujos también es factible definir estimadores aproximados que permitan cuantificar la variación en el retardo unidireccional (o jitter).

5.5.3.4. Netperf.

Netperf es una herramienta que puede ser usada para medir varios aspectos de las prestaciones de las redes. Realiza tests para obtener el throughput unidireccional y la latencia extremo a extremo.

Usa tanto TCP como UDP sobre el ampliamente aceptado interfaz socket de Berkeley. Netperf consiste en dos partes ejecutables: netserver es la parte servidora que puede actuar manualmente o vía inetd, y netperf es la parte cliente. Ejecutando netperf, una conexión TCP de control es establecida entre los dos host para negociar los parámetros de configuración del test. Durante el test, el canal de control está activo, pero no se usa. La medida de prestaciones del flujo suele ser determinar la máxima tasa de transferencia de un flujo TCP o UDP dados. Esta medida puede ser fácilmente calculada dividiendo los bytes transmitidos con el tiempo transcurrido. La prestación de la transacción está de cierta manera relacionada con la medida de la latencia. Durante este test, los paquetes de usuario con carga útil (1 byte por defecto) son transmitidos dentro de la red y una respuesta es generada por el receptor. La tasa de transacción se expresa entonces como el cociente entre el número de transacciones entre el tiempo transcurrido.

5.5.3.5. MGen.

El Multi Generator (MGen) es un software Open Source desarrollado por el Naval Research Laboratory (NRL) en su grupo de trabajo PROTocol Advanced Networking (PROTEAN) Research Group. MGEN proporciona la capacidad de desarrollar pruebas o tests de prestaciones en redes basadas en IP mediante el uso de tráfico UDP/IP.

La aplicación MGen, como “método activo”, genera patrones de tráfico IP en tiempo real para cargar a la red en distintas formas. El tráfico generado puede utilizarse para calcular estadísticas de como se está comportando la red ante una determinada carga analizando distintos parámetros de calidad de servicio, como el troughput, la cantidad de paquetes perdidos, el retardo experimentado por los paquetes. MGen es una aplicación que actualmente sólo corre sobre un sistema operativo basado en UNIX y/o WIN32 (la versión 3.3 para analizar IPv4 y la versión 3.1 para analizar IPv6).

El conjunto de herramientas MGen viene acompañado a su vez de otro complemento de software llamado Dynamic-receiver (Drec). Que sirve a su vez para recoger y volcar en disco la captura de los paquetes recibidos desde el nodo emisor que es el que está utilizando la aplicación MGen.

El tipo de paquetes que MGen genera son del tipo UDP. Esta es una de las razones principales por la que se opta por esta aplicación, dado que el envió de pequeños paquetes IP/UDP nos permitirá

emular y examinar el comportamiento de la voz sobre IP. MGen puede resultar ineficiente en según que casos muy puntuales de hosts sobrecargados por procesos con alto uso de recursos.

5.5.3.6. NetMeter.

Dentro de las variadas herramientas que permiten evaluar el rendimiento de cualquier red de forma activa, encontramos NetMeter. Ésta es una aplicación Open-Source (públicada bajo licencia GNU/GPL) que está desarrollada por el Centro de Conmutaciones Avanzadas de Banda Ancha (CCABA), cuyo objetivo es la automatización de tareas de generación/recepción y monitorización de tráfico IP, así como la representación gráfica de los resultados obtenidos. Incluyendo parámetros que caracterizan la Qos en redes IP (IPv4 e IPv6).

A partir de una automatización de las herramientas y tareas que actúan a más bajo nivel y que son utilizados por NetMeter se obtiene una metodología estructurada para la realización de experimentos, así como la base sólida para planificar cualquier conjunto de pruebas involucradas en proyectos de análisis de tráfico.

Las medidas que soporta esta aplicación son las especificadas por el IP Performance Metrics Group (IPPM) de la IETF.

Según el IPPM existen el siguiente tipo de medidas posibles para una red:

- **Connectivity:** Realizar medidas con el objetivo de verificar la conectividad entre puntos de la red.
- **One-way delay and loss:** Medidas del retardo extremo a extremo y de las pérdidas de paquetes sufridas en la transmisión. El One-Way Delay es uno de los parámetros que se consideran y se calculan en este proyecto.
- **Round-trip delay:** El Round-Trip delay es el retardo sufrido por un paquete desde que sale de un host origen hacia un destino determinado y vuelve. (Ejemplificado en la aplicación ping).
- **Delay Variaton:** Medidas de la variación del retardo (jitter). El objetivo de estas medidas es modelar la variación de las muestras obtenidas de un experimento respecto la media obtenida. Este parámetro es tenido también en cuenta en las medidas de este proyecto.
- **Loss patterns:** Medidas para modelar los posibles de patrones de pérdidas.

- **Packet reordering:** Modelización de la cantidad de paquetes que llegan desordenados a su destino.
- **Bulk transport capcity:** Medidas del ancho de banda consumido por ráfagas de tráfico consumidas.
- **Link bandwith capacity:** Medidas del ancho de banda del enlace, calculables con Netmeter.

Una de las características atractivas que presenta esta aplicación, es que permite salvar la configuración de las pruebas a realizar y repetirlas en un futuro manteniendo las mismas condiciones a nivel de aplicación pero realizando los cambios que se consideren oportunos a nivel de red

6. CAPITULO VI. SOLUCIONES TÉCNICAS PARA EL APROVISIONAMIENTO DE QOS EN LAS REDES IP.

En este Capitulo se da una descripción amplia y detallada de las diferentes tipos de herramientas que se disponen para asegurar una QoS dentro de una red IP. Se trata de mecanismos que previenen o manejan una congestión, distribuyen el tráfico o incrementan la eficiencia de la red, cuando de tráfico con requerimientos de tiempo real se trata (por ejemplo, voz).

6.1. INTRODUCCIÓN.

Las redes IP fueron diseñadas para el transporte óptimo del tráfico de datos, por lo que la QoS requerida en las mismas se basó únicamente en la integridad de los datos, esto es, no pérdida de contenido y ni secuencialidad de los mismos. En este sentido IP fue concebido, es decir, para "mover" por la red, de forma óptima y segura, tráfico sin requerimientos de tiempo real.

Como se a dicho anteriormente, el servicio que brinda IPv4 es del tipo "Best Effort". Por otra parte, el tráfico de audio y vídeo no solo requiere ser transferido por las redes IP de forma íntegra, sino que además requiere ser transferido en el tiempo adecuado, al "ritmo" adecuado, en correspondencia con la cadencia que es generado. En consecuencia, la QoS en relación con el tráfico que tiene requerimientos de tiempo real necesita considerar otros parámetros de calidad, tales como la latencia (retardo y jitter) y el ancho de banda.

Garantizar QoS en base a retardos y ancho de banda disponible en una red IP no es nada fácil. Una vez digitalizada la voz y paquetizada, se envía al canal de transmisión y aquí no existen soluciones que nos garanticen o permitan establecer anchos de banda, orden de paquetes y retrasos asumibles en su transmisión. Las posibles soluciones pasan por diferenciar los paquetes de voz de los paquetes de datos, priorizar la transmisión de los paquetes de voz y hacer que los retrasos añadidos a la transmisión de los paquetes no superen en ningún caso los 150 milisegundos (recomendación de la ITU).

Las líneas de trabajo actuales de cara a conseguir "QoS" en una transmisión IP, están basadas en:

- Supresión de silencios y VAD (voice activity detection).
- Compresión de cabeceras.
- Reserva de Ancho de Banda: implantación del estándar **RSVP** (Protocolo de Reserva de Recursos) de la IETF.

- Priorizar: existen diferentes tendencias tales como:
    a) **CQ** (Custom Queuing): asignación de un porcentaje del ancho de banda disponible.
    b) **PQ** (Priority Queuing): establecer prioridad en las colas.
    c) **WFQ** (Weight Fair Queuing): asignar prioridad al tráfico de menos carga.
    d) **DiffServ:** definido en borrador por la IETF, evita tablas en routers intermedios y establece decisiones globales de rutas por paquete.
- Control de Congestión: uso del protocolo **RED** (Random Early Discard), técnica que fuerza descartes aleatorios.
- La implantación de **IPv6** que proporciona mayor espacio de direccionamiento y la posibilidad de Tunneling.

Al contar con QoS, es posible asegurar una correcta entrega de la información necesaria o crítica, para ámbitos empresariales o institucionales, dando preferencia a aplicaciones de desempeño crítico, donde se comparten simultáneamente los recursos de red con otras aplicaciones no críticas. QoS hace la diferencia, al prometer un uso eficiente de los recursos ante la situación de congestión, seleccionando un tráfico específico de la red, priorizándolo según su importancia relativa, y utilizando métodos de control y evasión de congestión para darles un tratamiento preferencial. Implementando QoS en una red, hace al rendimiento de la red más predecible, y a la utilización de ancho de banda más eficiente.

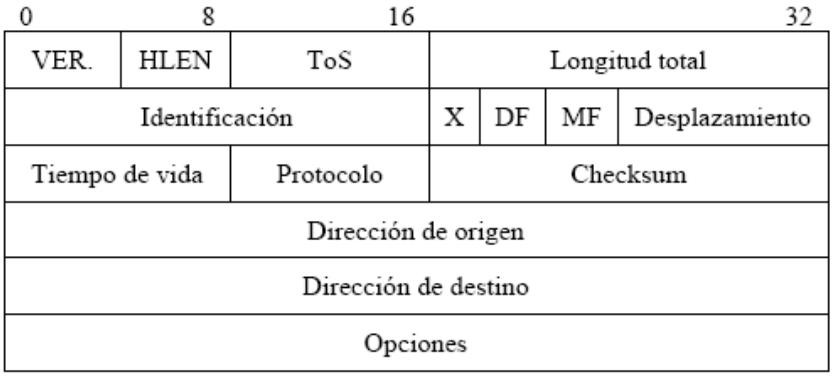
Dados estos requerimientos de QoS impuestos por el tráfico con características de tiempo real, como es audio y el vídeo, se necesitan mecanismos de señalización que propicien tener bajo control dichos parámetros de calidad, y dar garantía de QoS.

6.2. QOS DE INTERNET.

6.2.1. QoS de IPV4.

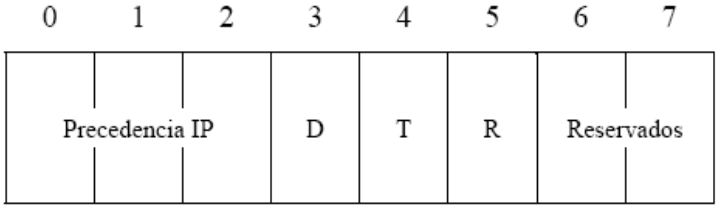
IPv4 es el protocolo de Internet usado en la actualidad y provee los mecanismos básicos de comunicación de la norma TCP/IP e Internet.

La calidad de Servicio en IPv4 se lleva a cabo a través del campo **ToS** (Type of Service), que es el segundo byte de la cabecera de IPv4.



Cabecera IPv4 con byte ToS

Los tres primeros bits de este campo son los bits de Precedencia IP, los tres siguientes se llaman D (Delay), T (Troughput) y R (Reability) ó bits DTR, mientras que los 2 últimos se dejaron para futuros usos. En la figura siguiente se puede observar la distribución de estos bits dentro del campo ToS.



Byte ToS de IPv4

La función del byte ToS es la de indicar a los distintos nodos por los que pasa el paquete el tratamiento de encolado y encaminado que debe recibir. De esta manera, los paquetes con distintos valores de campo ToS pueden ser gestionados con distintos niveles de servicio en la red.

Los 3 bits de precedencia se usan principalmente para clasificar los paquetes en la frontera de la red en una de las 8 posibles categorías. Los paquetes con menor precedencia (menores valores) pueden ser descartados a favor de los de mayor precedencia cuando haya congestión en la red.

Bits (0-2) del byte ToS	Precedencia IP	Bits (3-6) del byte ToS	Tipo de Servicio
111	Control de red	0000	Todo Normal
110	Encaminamiento	1000	Minimizar Retardo
101	Crítico	0100	Maximizar Troughput
100	Muy Urgente	0010	Maximizar Fiabilidad
011	Urgente	0001	Minimizar costes
101	Inmediato		
001	Prioridad		
000	Normal		

Clases de Servicio ToS

Además, según se configuren los bits DTR se puede especificar respectivamente si el paquete debe ser tratado con retardo normal ó bajo si se activa el bit D, con Troughput normal ó alto activando el bit T, y con fiabilidad normal o alta si se activa el bit R.

Posteriormente los bits DTR fueron redefinidos (por la RFC1349), de modo que el nuevo campo Tipo de Servicio estaría formado por 4 bits, los 3 del DTR y el bit 6 ó C (Cost). Si éste último está activado, indica que el tratamiento que debe recibir el paquete debe ser de mínimo costo.

Podría parecer que este simple esquema tiene todo lo necesario para ofrecer QoS IP en la red. Sin embargo, esto no es así por una serie de importantes limitaciones, como son:

- Solo permite la especificación de prioridad relativa de un paquete. No implementa ningún mecanismo que controle si realmente un paquete marcado por el usuario como de máxima precedencia pertenece a un flujo que realmente necesita ser tratado con máxima prioridad debido a la carencia de función de vigilancia.
- Los 3 bits restringen el número posible de clases de prioridad a 8. Además, dos de las clases (Control de red y Encaminamiento) se reservan para los paquetes que generan los nodos tales como actualización de rutas ó mensajes ICMP. Esto se hace para proteger los paquetes necesarios para el buen funcionamiento de la red, pero como contrapartida limita el número de clases que los usuarios pueden usar a 6.

Muy pocas arquitecturas han decidido dar soporte a clases de servicio diferenciado basadas en los bits de Precedencia IP ó en los DTR tal y como se definieron originalmente.

6.2.2 QoS de IPV6.

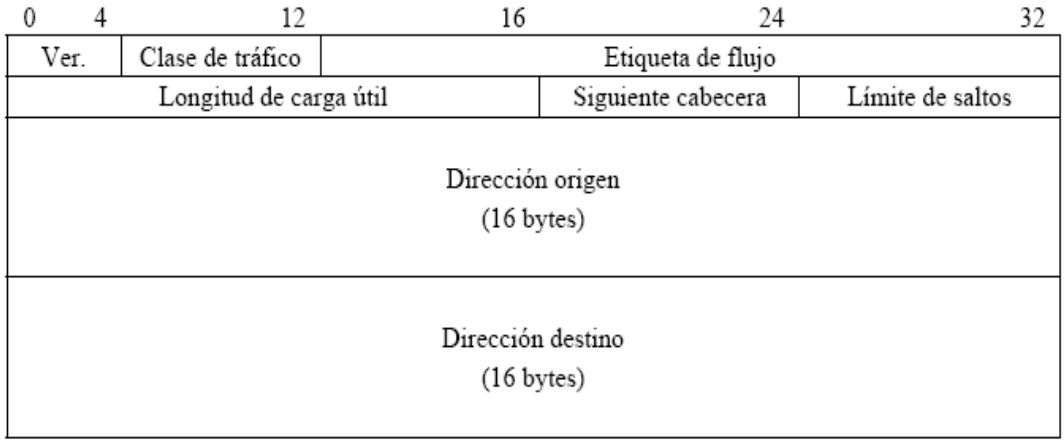
6.2.2.1. Introducción.

IPv6 ó IPng (IP next generation) es la nueva versión del Protocolo Internet (IP) diseñado para suceder a IPv4 manteniendo las partes que funcionaban bien, quitando ó mejorando las que no lo hacían y añadiendo nuevas capacidades, como las de QoS. En el diseño del nuevo protocolo se han tenido en cuenta las siguientes consideraciones:

- **Direccionamiento**: IPv6 utiliza direcciones de 128 bit para solucionar el agotamiento de direcciones que sufre IPv4.
- **Prestaciones**: IPv6 se ha diseñado para que los encaminadores puedan hacer su trabajo lo más rápido posible. En este sentido, se define una cabecera de tamaño fijo, que será la consultada en todos los nodos para el encaminamiento y una serie de cabeceras opcionales ó cabeceras de extensión que solo se consultarán cuando sea necesario. Si a esto se suma que el número de campos de cabecera en IPv6 es menor que en IPv4 y que no se permite la fragmentación, se consigue simplificar el tratamiento necesario a la hora de encaminar y por tanto mayor rapidez de encaminamiento.
- **Servicio de red**: Soporta servicios en tiempo real y permite especificar niveles de prioridad para determinar estrategias de eliminación en el caso de congestión. IPv6 permite el etiquetado de paquetes que pertenezcan a un flujo particular.
- **Flexibilidad en el direccionamiento**: IPv6 incluye el concepto de dirección anycast, en el que el paquete se entrega a solo uno de los conjuntos de nodos. Además se incluyen esquemas de direccionamiento multicast.
- **Seguridad**: Incluye el soporte para la autentificación y la privacidad. Paralelamente a IPv6 se está desarrollando un nuevo protocolo ICMP (ICMPv6) que será más ligero y conciso.

6.2.2.2. Formato de los paquetes.

El paquete IPv6 está formado por una cabecera fija de 40 bytes y opcionalmente por unas cabeceras de extensión.



Cabecera IPv6 con byte Clase de Tráfico

El significado de cada uno de los campos es el siguiente:

Versión: (4 bits), contiene el valor 6.

Clase de tráfico ó Prioridad: (8 bits), indica a los encaminadores el nivel de servicio requerido por el paquete. Se distingue dos tipos de tráfico: con control de congestión y sin control de congestión.

Etiqueta de flujo: (20 bits), **s**e asigna un número de identificación para cada comunicación entre ordenadores. Los encaminadores usan esta identificación para almacenar información relevante asociada a la conexión.

Longitud de carga útil: (16 bits), longitud del paquete menos la cabecera.

Próxima cabecera: (8 bits), tipo de cabecera después de la cabecera IPv6.

Límite de saltos: (8 bits), se decrementa en uno por cada nodo por el que pasa el paquete. Cuando el valor llega a cero se elimina el paquete.

Dirección origen: (128 bits), dirección desde donde se envía el mensaje

Dirección destino: (128 bits), dirección de destino. Esta dirección puede que no sea la dirección final si existe una cabecera de enrutamiento.

Se definen además las siguientes cabeceras de extensión:

Opciones de salto: Define opciones especiales que requieran un procesamiento por salto.

Opciones de destino: Contiene información opcional a examinar por el nodo de destino.

Encaminamiento: Proporciona encaminamiento extendido, similar al encaminamiento IPv4.

Fragmentación: Contiene información sobre la fragmentación y recomposición

Autentificación: Proporciona integridad a los paquetes y autentificación. Seguridad encapsulada usando el protocolo IPSec. Este protocolo ya se podía usar en IPv4 como un añadido (add-on), aunque en IPv6 ya viene integrado. Además, proporciona privacidad.

6.2.2.3. Gestión de la fragmentación.

Los encaminadores IPv6 no fragmentan los paquetes a diferencia que en IPv4. Cuando IPv6 envía su mensaje de conexión al receptor, se graba el máximo tamaño de paquete de cada subred en la ruta. Cuando la respuesta a la conexión llega, estableciendo la conexión, el origen sabe cual es el tamaño mayor de paquete que puede enviar. Es en el origen donde se fragmenta en paquetes de modo que no se supere este tamaño.

Dado que los paquetes no se fragmentan existe menos probabilidad de pérdida de paquetes y de reenvío de paquetes.

6.2.2.4. Direcciones IPV6.

Las direcciones de IPv6 son de 128 bits. La forma más aceptada de representar las direcciones IPv6 es x:x:x:x:x:x:x:x, donde cada x es un valor hexadecimal de una porción de 16 bit de la dirección. Se permiten tres tipos de direcciones:

- **Unicast:** Identifica un único destino. Actualmente se han partido las direcciones en distintos campos pero sin una longitud fija. Las direcciones IPv4 se encapsulan en IPv6 poniendo los 12 octetos más significativos a cero.
- **Anycast:** Una dirección anycast permite al origen especificar que quiere contactar con cualquier nodo de un grupo de nodos por medio de una única dirección. Una utilidad de este tipo de direcciones podría ser la de llegar al encaminador más cercano (según el cálculo de distancia de un determinado protocolo de encaminamiento) de varios conectados a una misma red local.
- **Multicast:** La dirección multicast permite definir grupos de 112 bits. El resto identifica el tipo de multicast, si va a ser local, de organización o global, lo que se conoce también como campo “alcance”.

Además permite la auto-configuración de direcciones para dar soporte al protocolo móvil de IPv6 (Mobile IPv6). Por medio de la cabecera de extensión de encaminamiento se puede indicar una

ruta parcial o completa por donde irá el paquete. En ese sentido cuando se llegue a la dirección de destino indicada en la cabecera se leerá esta cabecera y se enviará a la próxima dirección de la lista.

6.2.2.5. Tunneling.

Los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone. Los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente determinados usando direcciones IPv6 IPv4-compatible.

6.2.2.6. Seguridad.

IPv6 establece seguridad en el propio protocolo (IPsec), con lo que una organización puede asegurar que tendrá seguridad no sólo en las aplicaciones que tienen mecanismos de seguridad sino para todas las aplicaciones. La seguridad en IPv6 incluye tanto autentificación como privacidad.

El mecanismo de autentificación asegura que el paquete recibido es el mismo que el enviado por el emisor. Se asegura que el paquete no ha sido alterado durante la transmisión. La privacidad imposibilita que el contenido del paquete se pueda examinar. Para ello se emplean distintas técnicas de cifrado y claves públicas.

IPSec es considerado el mejor protocolo de seguridad en la actualidad, representa un gran esfuerzo del grupo de trabajo de la IETF. Inicialmente fue desarrollado para usarse con el nuevo estándar IPv6, aunque posteriormente se adaptó a IPv4.

6.2.2.7. Capacidades de QoS.

Los campos Etiqueta de flujo y Clase de Tráfico pueden ser usados por un emisor para identificar aquellos paquetes para los que quiere un tratamiento prioritario en los encaminadores intermedios, tales como los datos de tiempo real. Sin embargo, al igual que ocurre con IPv4, IPv6 por sí solo no es suficiente para dar QoS extremo a extremo, ya que mantiene el problema de IPv4 de que sólo puede definir prioridades relativas. Por tanto, sólo será capaz de proporcionar QoS de extremo a extremo cuando se combina con mecanismos de QoS implementados en los nodos encaminadores de la red como los que se proponen en “IntServ”, “DiffServ” ó “MPLS”.

A la hora de combinarse con dichas tecnologías, IPv6 ofrece algunas mejoras respecto de IPv4, como la disponibilidad de la Etiqueta de Flujo además de la etiqueta de Clase de Tráfico, gracias a las cuales, se puede identificar flujos concretos de paquetes a los que se le quiere dar un tratamiento especial para Servicios Integrados o para Servicios Diferenciados. Se ha propuesto además el uso de estos campos o etiquetas para MPLS.

6.2.2.7 1. Etiquetas de flujo.

La etiqueta de flujo es un campo de 24 bits de la cabecera de paquete IPv6 que permite el etiquetado de diferentes tipos de datos para conseguir diferente tratamiento en los nodos de la red.

Se entiende por flujo una secuencia de paquetes enviados desde un origen a un destino para el cual el origen quiere un tratamiento especial. La naturaleza de dicho tratamiento especial puede ser transmitida a los encaminadores por un protocolo de reserva de recursos (RSVP), o mediante información transmitida en los mismos paquetes del flujo. Un emisor puede generar un único flujo, varios ó tráfico que no pertenezca a ningún flujo en concreto.

Un flujo está identificado de forma única por la combinación de una dirección origen y una etiqueta de flujo distinta de cero. Los paquetes que no pertenecen a ningún flujo llevan una etiqueta de flujo igual a cero. Una etiqueta de flujo es asignada a un flujo por el nodo origen del mismo.

Todos los paquetes de un mismo origen con una misma etiqueta deben tener la misma dirección de destino, prioridad, opciones de salto y de encaminamiento en el caso de que las tengan activas.

6.2.2.7.2. Clase de tráfico.

El campo de Clase de tráfico de 8 bits de la cabecera de IPv6 permite a una fuente identificar la prioridad deseada para sus paquetes, relativa a otros paquetes de la misma fuente. Los valores de prioridad están divididos en dos rangos: Los valores de 0 a 7 y los valores de 8 a 16.

Los **valores de 0 a 7** se usan para especificar la prioridad del tráfico en el caso de que la fuente esté proporcionando control de congestión, es decir, que se adapta a la congestión, por ejemplo tráfico TCP.

Los **valores de 8 a 15** se usan para especificar la prioridad del tráfico que no se adaptan a la congestión, por ejemplo los paquetes de tiempo-real que son enviados a una velocidad constante.

6.3. CONTROL DE CONGESTIÓN.

Existen varios niveles en los cuales se puede proveer de calidad de servicio en una red IP. Uno de ellos es el de contar con una estrategia de manejo de los paquetes en caso de congestión, o el evitar que la red alcance este estado, descartando paquetes a medida que estos ingresan a la red.

El "manejo de congestión" es un término general usado para nombrar los distintos tipos de estrategia de encolamiento que se utilizan para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red, para que ciertos flujos tengan prioridad sobre otros.

6.3.1. Mecanismos de previsión de la congestión.

6.3.1.1. RED (Random Early Detection).

RED es un mecanismo de gestión activa de cola que trata de evitar la congestión eliminando paquetes aleatoriamente. El descarte de un simple paquete es suficiente para indicar que existe congestión a los protocolos de nivel de transporte del cliente, ya que cuando se descarta un paquete, el nodo envía un aviso implícito a la fuente TCP que lo envió indicándole que el paquete descartado sufrió congestión en algún punto del camino hacia el destino TCP. Como respuesta a este aviso implícito, la fuente TCP reducirá su ritmo de transmisión (volviendo a un comienzo lento ó recuperación rápida cuando desaparezca la congestión) de modo que la cola del nodo no se sature.

Las ventajas que aporta la gestión activa de cola RED son entre otras:

- Identifica los estados tempranos de congestión y responde descartando aleatoriamente paquetes. Si la congestión continua creciendo, RED descarta paquetes de forma más agresiva para prevenir que la cola alcance el 100 por ciento de su capacidad, lo cual resultaría en una pérdida total de servicio. Esto permite a RED mantener un cierto nivel máximo de tamaño medio de cola incluso con los protocolos de transporte no cooperativos.
- Gracias a que RED no espera hasta que la cola esté completamente llena para comenzar a descartar paquetes, la cola puede aceptar ráfagas de tráfico y no descartar todos los paquetes de la ráfaga. Así, RED es apropiado para TCP porque no descarta grupos de paquetes de una única sesión TCP ayudando así a evitar la sincronización global de TCP.
- Permite mantener la cantidad de tráfico en la cola a nivel moderado. Ni demasiado bajo, lo que causaría que el ancho de banda estuviese infrautilizado, ni con valores cercanos a la capacidad máxima, donde el excesivo descarte de paquetes provocaría que una gran cantidad de sesiones TCP redujera sus tasas de transmisión, llevando a una pobre utilización del ancho

de banda. Así, RED permite mantener el nivel de tráfico en cola de modo que se pueda obtener la mejor utilización del ancho de banda.

Las limitaciones de la gestión activa RED son:

- Puede ser muy difícil de configurar para obtener un funcionamiento predecible.
- RED no es apropiado para flujos no TCP tales como ICMP (Internet Control Message Protocol) ó UDP (User Datagram Protocol), ya que estos no detectan el descarte de paquetes y continuarían transmitiendo al mismo ritmo, perdiendo gran cantidad de paquetes debido a la congestión de la red.
- Existen algunos problemas en el uso e implementación de RED. Uno de ellos es que no tiene en cuenta las prioridades de los flujos a la hora de descartar, de modo que puede darse el caso de que se descarten paquetes de más prioridad mientras se estén sirviendo los de baja prioridad.

Este sistema podría utilizarse para gestionar una cola para tráfico Best Effort, ya que todos los flujos tendrán igual prioridad y el problema de RED de no distinguir prioridades no sería un inconveniente en este caso.

6.3.1.2. WRED (Weighted Random Early Detection).

Es una extensión de RED en la que se permite mantener un algoritmo RED diferente para cada tipo de tráfico dentro de la cola, teniendo en cuenta la prioridad de éstos.

Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma random si la congestión aumenta. Está diseñada para aplicaciones TCP debido a la posibilidad de retransmisión. Esta pérdida en la red obliga a TCP a un control de flujo reduciendo la ventana e incrementándola luego en forma paulatina. Un proceso de descarte generalizado, en cambio, produce la retransmisión en "olas" y reduce la eficiencia de la red.

La versión ponderada WRED realiza el drop de paquetes de forma que no afecta al tráfico de tipo RSVP. Una versión superior debería considerar el tráfico de aplicación.

6.3.2. Mecanismos de gestión de la congestión.

6.3.2.1. FIFO (First In First Out).

Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Es adecuado para interfaces de alta velocidad, sin embargo no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes, tratando a todos los flujos por igual, ya que el retardo medio de cola aumenta para todos los flujos a medida que la cogestión aumenta. Esto hace es especialmente perjudicial para las aplicaciones de tiempo real que sufrirán mayores retardos, jitters y pérdidas.

Otra característica, durante los periodos de congestión, el encolamiento FIFO beneficia a los flujos UDP sobre los TCP. Cuando se produce una pérdida de paquete debido a la congestión, las aplicaciones basadas en TCP reducen su tasa de transmisión, pero las aplicaciones basadas en UDP continúan transmitiendo paquetes al mismo ritmo que antes sin percatarse de la pérdida de paquetes.

6.3.2.2. FQ (Fair Queuing).

Generalmente conocida como WFQ (Weighted Fair Queueing), es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red, utilizado habitualmente para enlaces de velocidades menores a 2048 [Mbps]. WFQ ordena el tráfico en flujos, utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto de origen, etc. Una vez distinguidos estos flujos, el enrutador determina cuáles son de uso intensivo o sensibles al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola. WFQ es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generen altas y bajas cargas en la red, ya que WFQ se adapta a las condiciones cambiantes del tráfico en la red.

Sin embargo, la carga que significa para el procesador en los equipos de enrutamiento, hace de esta metodología poco escalable, al requerir recursos adicionales en la clasificación y manipulación dinámica de las colas.

6.3.2.3. PQ (Priority Queuing).

El Encolamiento de Prioridad (PQ), consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. Cada paquete es asignado a una de estas colas, las cuales son servidas en estricto

orden de prioridad. Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad, y así. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad (starvation).

6.3.2.4. CQ (Custom Queuing).

Para evadir la rigidez de PQ, se opta por utilizar Encolamiento Personalizado (CQ). Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round-Robin. CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles.

6.3.2.5. CBWFQ (Class Based WFQ).

WFQ tiene algunas limitaciones de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta; colapsa debido a la cantidad numerosa de flujos que analizar. CBWFQ fue desarrollada para evitar estas limitaciones, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la creación de clases definidas por el usuario, que permiten un mayor control sobre las colas tráfico y asignación del ancho de banda.

Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ, pero si con CBWFQ. Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo, ACL, valor DSCP, o interfaz de ingreso. Cada clase posee una cola separada, y todos los paquetes que cumplen el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se puede configurar específicamente el ancho de banda y límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase.

6.3.2.6. LLQ (Low Latency Queuing).

El Encolamiento de Baja Latencia (LLQ) es una mezcla entre PQ y CBWFQ. Es actualmente el método de encolamiento recomendado para ToIP, que también trabajará apropiadamente con tráfico de videoconferencias. LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad. Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido por la velocidad de enlace.

6.4. MECANISMOS DE SEÑALIZACIÓN CON QOS.

6.4.1. Servicios Integrados (IntServ).

6.4.1.1. Concepto de reserva en IntServ.

La arquitectura de Internet de IntServ, parte de las premisas de seguir utilizando el protocolo IP y de ofrecer servicio tanto "mejor esfuerzo" como servicios de tiempo real. La idea fundamental de esta arquitectura radica en que las aplicaciones se ven como un flujo dentro de la Internet y por cada flujo se deberá crear un estado (soft state) en cada uno de los enrutadores. En estos estados se realiza la reserva de los recursos necesarios para ofrecer QoS a las aplicaciones.

IntServ, se basa en el protocolo RSVP (Resource ReSerVation Protocol, RFC 1633), que implica una reserva de recursos en la red para cada flujo de información de usuario, así como el mantenimiento en la red (en los routers) de un estado para cada flujo, esto es, mantenimiento de la "reserva" (tablas de estados de reserva). Esto conduce a un considerable tráfico de señalización y ocupación de recursos en cada router para cada flujo, con la consiguiente complejidad en el hardware, al margen del aporte que esta señalización hace a la congestión de la red. No es una solución escalable, no es una solución adecuada para grandes entornos como Internet, aunque si lo es para entornos más limitados y también para redes de acceso al backbone.

El modelo de Servicios Integrados esta implementado por 4 componentes:

a) **Control de admisión:** El control de admisión implementa el algoritmo de decisión para determinar si se puede admitir un nuevo flujo sin afectar a los que ya estaban asignados. Se invoca en cada nodo para hacer una decisión de aceptación/rechazo local para cada terminal

que solicita un servicio de tiempo real a lo largo de un camino de la red. El algoritmo de admisión tiene que ser consistente con el modelo de servicio, y forma parte lógicamente del control de tráfico. El control de admisión se confunde a menudo con la política de admisión, que es una función que se realiza paquete a paquete en los "bordes" de la red para asegurar que un terminal no viola las características de tráfico comprometidas. La política de admisión se considerada como parte del organizador de paquetes.

b) **Clasificador:** Clasifica los paquetes dentro de alguna clase. La elección de una determinada clase puede estar basada en los contenidos de la cabecera y/o en algún número de clasificación adicional añadido en cada paquete. Una clase puede corresponder a una amplia gama de flujos, por ejemplo, todos los flujos de vídeo o todos los flujos provenientes de una determinada organización. Por otro lado, una clase puede contener un solo flujo. Una clase es una abstracción que puede ser local a cada uno de los encaminadores; el mismo paquete puede ser clasificado de forma diferente en diferentes encaminadores a lo largo del camino.
c) **Organizador de paquetes:** El organizador de paquetes gestiona el envío de diferentes secuencias de paquetes usando un conjunto de colas y otros mecanismos como temporizadores. Uno de los organizadores más utilizados en el modelo de Servicios Integrados es el WFQ, aunque para las partes de la red que se sabe que están siempre poco cargadas se usan mecanismos más sencillos como las colas FIFO.
d) **Protocolo de reserva de recursos:** Se utiliza para crear y mantener estados específicos de flujo en los terminales y en los encaminadores presentes en el camino de un flujo y debe estar implementado en todos ellos. Aunque en las especificaciones del protocolo no se cierra la posibilidad de usar otros protocolos, el recomendado por la comunidad internacional es el RSVP.

6.4.1.2. Tipos de servicios definidos en IntServ.

Los tres tipos de servicios que se han aprobado hasta ahora en el Modelo de Servicios Integrados son:

- **Servicio de mejor esfuerzo ó Best Effort:** Es el servicio que se le suele asignar al tráfico de las aplicaciones elásticas. La red no promete nada, pero trata de entregar los paquetes tan pronto como sea posible. En cada momento, la velocidad de transferencia depende del ancho de banda disponible en la red. Todos los flujos de tiempo-real que no hayan hecho una reserva de recursos también se transmiten con el servicio de mejor-esfuerzo.

- **Servicio Garantizado (GS):** Es usado por las aplicaciones rígidas intolerantes. Proporciona un límite firme en el retardo y la ausencia de pérdida de paquetes para un flujo que se ajuste a sus especificaciones de tráfico. El servicio garantizado no intenta minimizar el jitter, tan solo controla el retardo máximo de las colas de espera. Las aplicaciones de tiempo real, una vez conocido este retardo máximo, fijan su punto de reproducción de forma que todos los paquetes lleguen a tiempo. El retardo instantáneo para la mayoría de los paquetes será mucho menor que el retardo garantizado, por lo que los paquetes deben almacenarse en el receptor antes de ser reproducidos.
- **Servicio de Carga Controlada (CL):** diseñado para las aplicaciones adaptativas y tolerantes. No se dan garantías cuantitativas, simplemente se asegura que el servicio en condiciones de sobrecarga es aproximadamente tan bueno como el servicio de "mejor esfuerzo" en redes ligeramente cargadas. Una fuente de datos proporciona a la red las especificaciones del tráfico que va a generar. La red asegura que habrá suficientes recursos disponibles para ese flujo, siempre y cuando el flujo siga ajustándose a las especificaciones dadas. El servicio dado a los paquetes que se ajustan a las especificaciones se caracteriza por retardos pequeños y escasas pérdidas de paquetes. Los retardos de colas no son significativamente más grandes que el tiempo que se tarda en vaciar una ráfaga de tamaño máximo a la velocidad demandada. Puede haber pérdidas de paquetes ocasionales debidas a efectos estadísticos, pero la tasa de pérdidas total no debe exceder demasiado la tasa de errores de paquetes básica del medio de transmisión.

6.4.1.3. RSVP (Resource ReSerVation Protocol).

RSVP es un protocolo que se desarrolla entre los usuarios y la red, y entre los diferentes nodos (routers) de la red que soportan este protocolo. Consiste en hacer "reservas" de recursos e n dichos nodos para cada flujo de información de usuario, con la consecuente ocupación de los mismos. Esto requiere, lógicamente, intercambio de mensajes RSVP entre dichos entes funcionales, así como "mantener" estados de reserva en cada nodo RSVP. De manera que tanto la solicitud de las reservas, como el mantenimiento de éstas durante la comunicación, y la posterior cancelación, implica el intercambio de mensajes de señalización, lo que representa un tráfico considerable cuando de entornos como Internet se trata.

Las características más importantes del RSVP son:

- El RSVP hace reservas para aplicaciones: unicast y multicast, adaptándose dinámicamente las alteraciones de los miembros de un grupo o de rutas.
- El RSVP es simplex, solo reserva recursos para flujos unidireccionales. Para tener reserva bidireccional se debe solicitar dos consultas RSVD de ambos sentidos.
- El que inicia y mantiene las reservas en RSVP son los receptores llamados (receiver-initiated).
- El estado de las reservas es "leve" (soft-sate), o sea después de un intervalo de tiempo la reserva se vence, para lo cual todos lo receptores constantemente deben actualizar la solicitud de reservas para mantener el canal de comunicación.
- El RSVP no es un protocolo de enrutamiento, sino que usa la ruta escogida por cualquier protocolo de enrutamiento de uso actual o de uso futuro.
- El RSVP transporta y mantiene información sobre el control de tráfico y control de políticas que son tratados por otros módulos.
- El RSVP ofrece varios estilos de reserva, para adaptarse a una gran variedad de aplicaciones y usos.
- Los routers que no implementan RSVP pueden funcionar perfectamente en las transmisiones de la red.
- El RSVP soporta IPv4 e IPv6.

RSVP se ha diseñado para permitir a los emisores, receptores y routers de las sesiones de comunicación (tanto multicast como unicast) comunicarse con el resto para establecer una ruta que pueda soportar la calidad de servicio requerida. La calidad de servicio viene especificado en un flowspec.

6.4.1.3.1. Clases de QoS.

Existen varias clases de QoS, definidas por la IETF, especificándose dos formalmente para RSVP. Servicio de Carga Controlada (Controlled Load Service) y Servicio Garantizado (Guaranted Service).

El **Servicio garantizado (SG)**, este servicio proporciona un nivel de ancho de banda y un límite en el retardo, garantizando la no existencia de pérdidas en colas. Está pensado para aplicaciones con requerimientos en tiempo real, tales como ciertas aplicaciones de audio y vídeo.

Cada router caracteriza el SG para un flujo específico asignando un ancho de banda y un espacio en buffer.

En cuanto al **Servicio de carga controlada**, a diferencia del SG, este servicio no ofrece garantías en la entrega de los paquetes. Así, será adecuado para aquellas aplicaciones que toleren una cierta cantidad de pérdidas y un retardo mantenidos en un nivel razonable. Los routers que implementen este servicio deben verificar que el tráfico recibido siga las especificaciones dadas por el Tspec (especificación de tráfico), y cualquier tráfico que no las cumpla será reenviado por la red, como tráfico Best Effort.

De los dos tipos de servicios que RSVP soporta, el más adecuado para aplicaciones con requerimientos de tiempo real, es el servicio garantizado, aunque es más complejo de implementar que el servicio de carga controlada.

RSVP define dos sentidos para la transferencia de sus mensajes de señalización, downstream y upstream. El flujo downstream se efectúa desde la fuente al receptor o receptores, y el flujo upstream en sentido contrario.

6.4.1.3.2. Mensajes de señalización.

PATH y RESV son dos mensajes básicos del protocolo RSVP, y son en definitiva los mensajes a través de los cuales se lleva a cabo la reserva de recursos en la red previo a la comunicación.

Una aplicación solicita participar en una sesión RSVP como emisor, enviando un mensaje "Path" en el mismo sentido que el flujo de datos, por las rutas uni/multicast proporcionadas por el protocolo de routing. A la recepción de este mensaje, el receptor transmite un mensaje "Resv", dirigido hacia el emisor de los datos, siguiendo exactamente el camino inverso al de los mismos, en el cual se especifica el tipo de reserva a realizar en todo el camino.

6.4.1.3.2.1. Mensajes PATH.

Los mensajes PATH´s son generados por la fuente de mensajes de usuario necesitados de garantía de QoS, e indica las características de éstos en cuanto a recursos que necesita. La ruta que deben seguir estos mensajes es la misma que siguen los datos de usuario, para lo cual se requiere previamente un "diálogo" entre el proceso RSVP y el proceso de routing, pues dicha ruta quien la determina es el protocolo de routing, de lo contrario para nada serviría RSVP.

En su paso por cada router RSVP los mensajes PATH´s se actualizan y se retransmiten, consistente esto en poner la dirección IP del router que lo actualiza y re-envía. Cada router RSVP también almacena la dirección del router anterior. Así, con los mensajes PATH´s se posibilita indicar al receptor, o receptores, no solo las características del tráfico de usuario, sino también la ruta por donde debe solicitar las correspondientes reservas de recursos. Los routers que no soporten RSVP transfieren transparentemente los mensajes PATH´s.

6.4.1.3.2.2. Mensajes RESV.

Los mensajes RESV´s son producidos por el receptor (o receptores) de los flujos de información de usuario, como "respuesta" a los mensajes PATH´s, y solicitan a la red (a los routers RSVP) las correspondientes reservas de recursos para soportar la comunicación con cierta QoS, fluyendo hasta la fuente del stream de datos de usuario, es decir, en sentido upstream. Con la información de ruta que suministran previamente los mensajes PATH´s, los mensajes RESV´s dirigen las solicitudes de reservas a los routers RSVP apropiados, esto es, por donde fluirán los streams de datos.

Los mensajes RESV´s especifican el ancho de banda mínimo que se requiere para obtener determinada demora en un stream de datos específico. Vale decir además, que es posible efectuar reservas compartidas, esto es, una misma reserva aplicable a varios streams de datos de usuario.

Estas reservas de recursos en los routers RSVP de la red se materializan mediante "soft-states" en dichos routers, estados que requieren para mantenerse de "refrescamientos" periódicos, por lo que durante toda la comunicación se necesita "señalizar" para mantener las reservas previamente efectuadas. En consecuencia, esto conlleva a cierta señalización "permanente" durante la fase de transferencia de información de usuario, con la consiguiente carga de tráfico que implica.

Vale decir también que la reserva de recursos extremo a extremo que posibilita RSVP será válida si, y solo si, la congestión y demora que introduzcan los routers no RSVP no es significativa.

Otros mensajes del protocolo RSVP son:

- **PATHTEAR:** son mensajes generados por la fuente de datos de usuario para eliminar los estados path´s en todos los routers RSVP. Siguen la misma ruta que los mensajes PATH´s. También pueden ser originados por cualquier nodo cuando se agota el timeout del estado path.

- **RESVTEAR:** son generados por los receptores para borrar los estados de reserva en los routers RSVP, por tanto viajan en el sentido upstream. Pueden ser también originados por nodos RSVP al agotarse el timeout del estado de reserva de los mismos.
- **PATHERR:** viajan en sentido upstream hacia el emisor siguiendo la misma ruta que los mensajes PATH´s, y notifican errores en el procesamiento de mensajes PATH´s, pero no modifican el estado del nodo por donde ellos pasan en su "viaje" hacia la aplicación emisora.
- **RESVERR:** notifican errores en el procesamiento de mensajes RESV, o notifican la interrupción de una reserva. Se transfieren en la dirección downstream hacia el receptor o receptores apropiados.

6.4.1.3.3. Modelos de reserva de recursos.

RSVP modela una reserva por medio de dos componentes, una asignación de recursos y un filtro de paquetes. La asignación de recursos especifica que cantidad de recursos son reservados mientras el filtro de paquete selecciona que paquetes pueden usar los recursos. Esta distinción y la posibilidad de cambiar el filtro de paquetes dinámicamente permite a RSVP ofrecer varios estilos de reserva. Un estilo de reserva captura los requerimientos de comunicaciones del nivel de aplicación.

Por ahora se han definido tres modelos de reserva:

- **Libre** (Wildcard): Este modo indica que cualquier paquete con destino al grupo multicast asociado puede utilizar los recursos reservados. Esto permite hacer una única asignación de recursos a través de todas las rutas de distribución del grupo.
- **Filtro Fijo** (Fixed Filter): Este modo indica que mientras dure la conexión el receptor solo recibirá paquetes de las fuentes indicadas en la petición de reserva original.
- **Filtro dinámico** (Dynamic Filter): Se permite durante la conexión modificar la función de filtro. Esto permite la posibilidad de dinámicamente seleccionar un canal entre las distintas fuentes. Esto requiere que se asignen los recursos suficientes para manejar el peor caso que es cuando todos los receptores pidan de diferentes fuentes.

6.4.1.3.4. Parámetros fundamentales de una reserva.

6.4.1.3.4.1. Sesión.

La sesión es la unidad para la cual se hace una reserva, y equivale a una identificación del receptor. Una sesión RSVP viene definida por los parámetros siguientes:

- **DestAddress:** Contiene la dirección IP del destino, ya sea unicast o multicast.
- **ProtocolId:** Identificador del protocolo IP utilizado (IPv4 o lPv6).
- **DstPort** (opcional)**:** Puerto de destino generalizado (por ejemplo, puertos TCP/UDP).

Como puede comprobarse, una sesión identifica inequívocamente a una aplicación receptora (identificada por el campo DstPort) en un host determinado (identificado por la pareja DstAddress + ProtocolId).

6.4.1.3.4.2. Descriptor de flujo.

Una petición de reserva RSVP para una sesión determinada siempre incorpora un descriptor de flujo, dado que es la unidad de información necesaria para definir la calidad de servicio para un conjunto de datos del emisor. Un descriptor de flujo se compone de dos conjuntos de parámetros:

- **FlowSpec** (Especificación del flujo) Define la calidad de servicio deseada, y recoge las especificaciones de tráfico del servicio del modelo de Servicios Integrados elegido. Se divide a su vez en dos grupos de parámetros:
  - → Rspec (Especificación de la Reserva), describe propiamente la calidad de servicio requerida.
  - → Tspec (Especificación del Tráfico), describe las características del flujo de datos.

- **FilterSpec** (Especificación de Filtro) Define el conjunto de paquetes de datos que deberá recibir la calidad de servicio definida por el FlowSpec y el estilo de reserva que se debe aplicar.

6.4.1.4. Problemas asociados a IntServ.

La cantidad de información de estado aumenta proporcionalmente con el número de flujos. Esto implica un gran almacenamiento y procesado en los encaminadores. Esta arquitectura es por tanto poco escalable dentro del núcleo de Internet (core de Internet).

Los encaminadores tienen que cumplir muchos requisitos. Todos los encaminadotes deben tener RSVP, control de admisión, clasificación MF, y administrador de paquetes (scheduling).

Se requiere de un despliegue generalizado para garantizar servicio, aunque es posible un despliegue incremental del servicio de carga controlada desplegando un servicio de carga controlada y la funcionalidad RSVP en los nodos cuellos de botella de un dominio y pasando usando tunnelling los mensajes RSVP sobre otras partes del dominio.

6.4.2. Servicios Diferenciados (DiffServ o DS).

6.4.2.1. Introducción.

A diferencia de la arquitectura de servicios integrados, en donde es necesario hacer una reservación del canal, de manera análoga al servicio telefónico, y en donde existe una señalización para mantener la reservación, en la arquitectura de servicios diferenciados, los paquetes son clasificados únicamente en el dispositivo de acceso a la red, y ya dentro de la red, el tipo de procesamiento que reciban los paquetes va a depender del contenido del encabezado.

Los servicios diferenciados (DS) proporcionan mecanismos de calidad de servicio para reducir la carga en dispositivos de la red a través de un mapeo entre flujos de tráfico y niveles de servicio. Los paquetes que pertenecen a una determinada clase se marcan con un código específico (DSCP – DiffServ CodePoint). Este código es todo lo que necesitamos para identificar una clase de tráfico. La diferenciación de servicios se logra mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, hecho conocido como PHB (Per Hop Behavior).

De esta manera a través de DS se asignan prioridades a los diferentes paquetes que son enviados a la red. Los nodos intermedios (routers) tendrán que analizar estos paquetes y tratarlos según sus necesidades. Esta es la razón principal por la que DS ofrece mejores características de escalabilidad que IntServ. Dentro del grupo de trabajo de DiffServ de la IETF, se define en el campo DS (Differentiated Services) donde se especificarán las prioridades de los paquetes. En el subcampo DSCP (Differentiated Service CodePoint) se especifica la prioridad de cada paquete. Estos campos son validos tanto para IPv4 como IPv6.

6.4.2.2. Arquitectura.

La arquitectura DiffServ es la propuesta del IETF para solucionar problemas asociados a IntServ. La solución consiste básicamente en agrupar los flujos de tráfico IP en agregados, dentro de los cuales, los paquetes de un agregado serán tratados de la misma forma en cada nodo.

Este tratamiento realizado salto a salto se denomina Per-hop behavior (PHB), que se corresponden con distintos niveles de:

Prioridad de servicio. Determina que paquete se atiende en primer lugar de todos los que están esperando a ser transmitidos por el enlace.

Prioridad de descarte. En el interior de los nodos los paquetes son almacenados en buffers de tamaño finito. Como consecuencia de esto, cuando se agota su capacidad hay que proceder al descarte de uno o más paquetes. La prioridad de descarte permite cuales son los paquetes que se van a descartar cuando se produzca esta situación.

Cada grupo PHB al que pertenecen paquetes se codifica en un campo de su cabecera llamado en DS y su valor determina el tratamiento que se le debe dar a ese paquete en cada tramo de la red

6.4.2.2.1. Per Hop Behaviors (PHB).

La RFC 2475 define PHB como el comportamiento de "fordwaring" observable externamente aplicado en un nodo DiffServ hacia un DiffServ Behavior Aggregate (BA).

Con la capacidad del sistema de marcar paquetes de acuerdo al parámetro DSCP, los conjuntos de paquetes con el mismo DSCP y enviados en una determinada dirección pueden agruparse en un BA. Paquetes provenientes de fuentes múltiples o diversas aplicaciones, por tanto, pueden pertenecer al mismo BA.

En otras palabras, un PHB se refiere a la planificación del paquete, el encolamiento, la política, de un nodo en cualquier paquete dado perteneciente a un BA.

Existen cuatro estándares disponibles de PHBs especificados para ser usados dentro de una red de servicios diferenciados:

- Default PHB (PHB por defecto o Best Effort, RFC 2474);
- Class-Selector PHB (PHB selector de clases, RFC 2474);
- Assured Forwarding PHB (PHB tránsito asegurado, RFC 2597);
- Expedited Forwarding PHB (PHB tránsito expedito, RFC 2598).

La IETF se ha centrado en la especificación de estos dos últimos tipos de PHBs, dadas sus características.

6.4.2.2.1.1. Default PHB.

El PHB por defecto en esencia específica que un paquete marcado con valor de DSCP 00000 (recomendado) recibe el servicio best-effort tradicional de un nodo DS-compliant (esto es, un nodo de red que cumple con todos los requisitos del corazón de DiffServ). Además, si un paquete llega a un nodo DS-Compliant, y el valor DSCP no se mapea a algún otro PHB, el paquete será mapeado al PHB por defecto.

6.4.2.2.1.2. Class Selector (SC) PHB.

Para preservar la compatibilidad hacia atrás con algún esquema de precedencia IP actualmente en uso en la red, DiffServ ha definido un valor DSCP del tipo xxx000, donde x es 0 á 1. Estos valores DSCP se llaman Class-Selector Code Points. (El valor DSCP de un paquete con PHB por defecto 000000 también se llama Class-Selector Code Point.)

El PHB asociado con un Class-Selector Code Point es un PHB Class-Selector.

Paquetes con un valor de DSCP de 11000 tienen preferencia en el envío hacia delante (para programación, encolado, y demás), sobre paquetes con valor DSCP de 100000.

6.4.2.2.1.3. Assured Forwarding (AF) PHB.

El PHB AF define un método por el cual los BAs pueden darse con diferentes garantías de envío hacia delante.

Además, este PHB define cuatro clases: AF1, AF2, AF3, y AF4. Cada clase se asigna a una cantidad específica del espacio del buffer y ancho de banda de la interfaz, de acuerdo con la política establecida. En cada clase AF, se pueden especificar tres valores de precedencia: 1, 2 y 3.

Así pues, el tratamiento ofrecido a los paquetes de un determinado flujo dependerá de la cantidad de recursos asignados para los flujos de su clase, de la carga de los mismos y de su probabilidad de descarte ante situaciones de congestión.

6.4.2.2.1.4. Expedited Forwarding (EF) PHB.

El componente de IntServ, RSVP, proporciona un servicio de ancho de banda garantizado. Aplicaciones como la voz sobre IP, video, y programas online requieren este servicio robusto. EF PHB, elemento clave de DiffServ, proporciona este servicio a través de una pérdida baja, una baja latencia y un bajo jitter, así como un servicio asegurado de ancho de banda.

EF puede implementarse usando PQ. Cuando se implementa en una red DiffServ, EF PHB proporciona una línea virtual, o un servicio premium. Sin embargo, para una eficiencia óptima, EF debe ser reservado para únicamente las aplicaciones más críticas, puesto que en situaciones de congestión de tráfico, no es factible tratar todo o gran parte del tráfico con alta prioridad.

El servicio **Expedited Forwarding** es aproximadamente equivalente al Servicio Garantizado de IntServ, mientras que el **Assured Forwarding** corresponde más o menos al Servicio de Carga Controlada de IntServ.

6.4.2.2.2. Clasificadores.

El clasificador tiene como función el clasificar el tráfico entrante de acuerdo con los perfiles de los clientes y reenviar los flujos al gestor correspondiente AF, EF ó BE.

Para ello, el clasificador toma un flujo de tráfico simple como entrada y le aplica una serie de filtros. Cada filtro representa un determinado perfil de cliente y tendrá un gestor de servicios asociado. A la salida de cada filtro tendremos un flujo de tráfico formado por los paquetes que hayan pasado el filtro. Este flujo se enviará al gestor de servicios que tenga asociado el filtro.

Un filtro consiste en un conjunto de condiciones sobre los valores que componen el paquete que se consideren claves para su clasificación.

Dos de los clasificadores más usados son el Clasificador BA (Behaviour Aggegate) para los nodos interiores y el Clasificador Multi-Field ó MF para los nodos frontera.

6.4.2.2.2.1. Clasificador BA.

Este tipo de clasificador, usa solamente los DSCP de la cabecera IP de los paquetes para determinar el flujo de salida lógico hacia el cual el paquete debería ser dirigido.

Cada filtro BA estará configurado con un valor DSCP y solo dejará pasar los paquetes marcados con este DSCP.

6.4.2.2.2.2. Clasificador MF.

Los clasificadores MF clasifican paquetes basándose en uno o más campos del paquete (entre los que puede estar el DSCP). Un tipo común de clasificador MF es el llamado **'6-tuple'** que clasifica basándose en 6 campos de las cabeceras IP y TCP o UDP (dirección destino, dirección origen, protocolo IP, puerto origen, puerto destino, y DSCP). Los clasificadores MF pueden clasificar

también basándose en otros campos como las direcciones MAC, etiquetas VLAN, campos de clases de tráfico de capa de enlace o campos de protocolos de capas más altas, pero el '6-tuple' es el más usado.

6.4.2.2.3. Nodos DS.

En la arquitectura definida por Diffserv aparecen nodos extremos DS de entrada y salida, así como nodos DS internos. Este conjunto de nodos definen el dominio Diffserv y presenta un tipo de políticas y grupos de comportamiento por salto (PHB) que determinarán el tratamiento de los paquetes en la red.

Veamos a continuación las diferentes funciones que deben realizar los nodos DS:

6.4.2.2.3.1. Nodos extremos DS.

Será necesario realizar diferentes funciones como el acondicionamiento de tráfico entre los dominios Diffserv interconectados. De esta manera debe clasificar y establecer las condiciones de ingreso de los flujos de tráfico en función de: dirección IP y puerto (origen y destino), protocolo de transporte y DSCP, este clasificador se conoce como MF (Multi-Field Classifier). Una vez que los paquetes han sido marcados adecuadamente, los nodos internos deberán seleccionar el PHB definido para cada flujo de datos.

Los nodos DS de entrada serán responsables de asegurar que el tráfico de entrada cumple los requisitos de algún TCA (Traffic Conditioning Agreement), que es un derivado del SLA, entre los dominios interconectados. Por otro lado los nodos DS de salida deberán realizar funciones de acondicionamiento de tráfico o TC (Traffic Conformation) sobre el tráfico transferido al otro dominio DS conectado.

6.4.2.2.3.2. Nodos internos DS.

Podrá realizar limitadas funciones de TC, tales como remarcado de DSCP. Los nodos DS internos solo se conectan a nodos internos o a nodos externos de su propio dominio. A diferencia de los nodos externos para la selección del PHB solo ser tendrá en cuenta el campo DSCP, conocido como clasificador BA (Behavior Aggregate Classifier).

6.4.2.3. Análisis de los routers DS.

Una red de Servicios Diferenciados es un dominio que comprende un conjunto de dispositivos. Este dominio puede tener acceso otros elementos de red fuera de él.

Los tipos de routers en redes DS se clasifican así:

- **First Hop Router:** es el router más próximo al host emisor de paquetes. Los flujos de paquetes son clasificados y marcados acorde a la etiqueta SLA (Service Level Agreement). Es responsable de que el tráfico esté acorde con el ancho de banda del perfil.
- **Ingrees Router:** se sitúan en los puntos de entrada al backbone DiffServ (dominio DS), efectuando la clasificación de los paquetes en base al campo DS o en base a múltiples campos de la cabecera de éstos.
- **Egress Router:** se ubican en los puntos de salida de redes DiffServ (dominio DS), controlando el tráfico. Efectúan la clasificación de paquetes en base solo al campo DS de las cabeceras.
- **Interior router:** tienen la misión de "sumar" flujos, realizar la clasificación DS y reenvío de paquetes. Se sitúan dentro del backbone DS (dominio DS).

6.4.2.4. Observaciones de la red Diffserv.

Al utilizar el modelo DiffServ se obtienen varias ventajas. Los enrutadores operan más rápido, ya que se limita la complejidad de la clasificación y el encolado. Se minimizan el tráfico de señalización y el almacenamiento. En DiffServ, se definen clases de servicio, cada flujo particular de datos es agrupado en un tipo de clase, donde son tratados idénticamente. Los enrutadores internos sólo están interesados del comportamiento por salto (PHB: Per Hop Behavior), marcado en la cabecera del paquete. Esta arquitectura permite a DiffServ rendir mucho mejor en ambientes de bajo ancho de banda, y provee de un mayor potencial que una arquitectura IntServ.

DiffServ se plantea como la solución más adecuada para ofrecer calidades diferenciadas en el seno de las futuras redes. Además es compatible y complementaría de MPLS.

6.4.3. MPLS (Multi Protocol Label Switching).

6.4.3.1. Introducción.

El protocolo de conmutación por etiquetas multiprotocolo (MPLS) surgió en los últimos años de la década de los 90 como una arquitectura que debiera permitir mejorar la performance de las redes

IP. Sin embargo, actualmente su interés radica en sus aplicaciones a redes privadas virtuales, a Ingeniería de Tráfico y a QoS sobre IP.

El principal objetivo que se persigue con MPLS es conseguir una red IP que trabaje directamente sobre tecnologías de transporte de datos (sin capas intermedias que reduzcan el rendimiento) y donde la calidad de servicio y la gestión de tráfico se proporcionen a través de tecnologías de capa IP, es decir, pretende tener las ventajas que ofrecía ATM evitando sus desventajas.

Gracias a ello, los usuarios empresariales pueden obtener el recorte de costos que ofrece una infraestructura de red compartida y beneficiarse simultáneamente de un tráfico con unos niveles garantizados de latencia, pérdidas de paquetes y fluctuación de fase (jitter), algo crucial para aplicaciones en tiempo real como la ToIP.

Cisco Systems ha sido una empresa pionera al proporcionar una solución pre-estandarizada MPLS a la conmutación por etiquetas. Así también respondiendo a esta necesidad de los clientes, Telmex (empresa de servicios IP) ofrece su servicio de Ancho de Banda por Demanda, que saca partido a las capacidades de administración de su plataforma de conectividad IP MPLS, para entregar a sus clientes de Redes Corporativas los anchos de banda diferenciados que se ajusten a la temporalidad de sus requerimientos específicos.

6.4.3.2. Nodos LSRs y LERs.

La arquitectura de una red MPLS está definida en el RFC 3031. Los dispositivos que participan en los mecanismos del protocolo MPLS pueden ser clasificados en enrutadores de etiqueta de borde o **Label Edge Routers (LERs)**, y en ruteadores de conmutación de etiquetas o **Label Switching Routers (LSRs)**.

- Un LSR es un dispositivo ruteador de alta velocidad, que dentro del núcleo de una red MPLS, participa en el establecimiento de las LSPs, usando el protocolo de señalización apropiado y una conmutación de alta velocidad aplicado al tráfico de datos, que se basa en las trayectorias establecidas.
- Un LER es un dispositivo que opera en el borde de una red de acceso hacia una red MPLS. Un LER soporta múltiples puertos conectados a diferentes tipos de redes (por ejemplo, frame relay, ATM, Ethernet); y se encarga, en el ingreso de establecer una LSP para el trafico en uso y de evitar este trafico hacia la red MPLS, usando el protocolo de señalización de etiquetas, y en egreso de distribuir de nuevo el trafico hacia la red de acceso que corresponda. El LER

juega un papel muy importante en la asignación y remoción de etiquetas que se aplica al tráfico que entra y sale de una red MPLS.

6.4.3.3. FEC.

Una clase de envío equivalente o **Forwarding Equivalence Class (FEC)**, es una representación de un grupo de paquetes que comparten los mismos requerimientos para su transporte; todos los paquetes de este gripo tienen el mismo trato en la ruta hacia su destino. Al contrario de lo que pasa en el tradicional envío de paquetes en IP, en MPLS, la asignación de un paquete a una FEC en particular se realiza solo una vez, en el momento en el que paquete entra a la red.

La definición de una FEC se basa en los requerimientos de servicio que posea un conjunto de paquetes dado, o simplemente por el prefijo de una dirección IP. Cada LSR construye una tabla para especificar que paquete debe ser enviado; esta tabla, llanada base de información de etiquetas (LIB), se construye con uniones FEC/etiqueta.

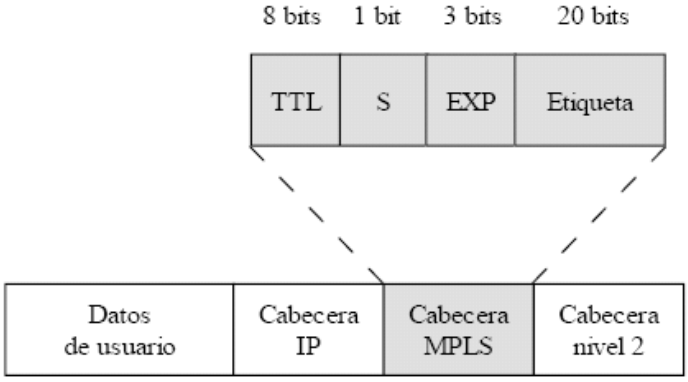
6.4.3.4. Funcionamiento básico de MPLS.

Una MPLS consiste de un conjunto de LSR que tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado FEC, así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es “orientada a conexión”. Cada FEC, además de la ruta de los paquetes contiene una serie de caracteres que define los requerimientos de QoS del flujo. Los routers de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tiene los routers MPLS sobre los routers IP, en donde el proceso de reenvió es más complejo.

En un router IP cada vez que se recibe un paquete se analiza su encabezado IP para compararlo con la tabla de enrutamiento (routing table) y ver cual es el siguiente salto (next hop). El hecho de examinar estos paquetes en cada uno de los puntos de tránsito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y por lo tanto, una mayor duración en el recorrido.

6.4.3.5. Formato cabecera MPLS.

La cabecera MPLS se compone de los campos Etiqueta MPLS, EXP ó experimental (antes conocido como CoS.), S ó Stack que se usa para apilar etiquetas de forma jerárquica y TTL (Time To Live), que sustenta la funcionalidad estándar TTL de las redes IP.



Cabecera MPLS

La cabecera MPLS está conformada por 32 bits, divididos como se muestra en la figura anterior, y contiene los siguientes elementos:

- **Valor de la etiqueta:** Etiqueta de 20 bits con valor local.
- **Experimental (EXP):** Son los 3 bits siguientes reservados para uso experimental. Se podría especificar en estos bits el PHB del salto.
- **Pila (S o Stack):** Es el bit de posición de pila:

  Cuando es "1"denota que es la entrada más antigua en la pila.

  Cuando es "0" denota que es cualquier otra entrada.
- **Tiempo de vida (TTL o Time To Live):** Es un campo de 8 bits, y se utilizan para codificar el valor del conteo de saltos (IPv6) o de tiempo de vida (IPv4).

Un aspecto interesante para comprender como se consigue que MPLS pueda funcionar sobre cualquier tipo de transporte es como se insertan las etiquetas dentro de los paquetes MPLS.

Si el protocolo de transporte de datos sobre el que trabaja MPLS contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativos para las etiquetas. Si por el contrario, la tecnología de nivel 2 que se emplea no soporta un campo para etiquetas (caso de los enlaces PPP o LAN), entonces se emplea una cabecera

genérica MPLS de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

6.4.3.6. Mecanismos de señalización.

- **Petición de Etiquetas (label request):** usando este mecanismo, un LSR hace una petición de etiqueta a su vecino downstream, de manera que la pueda unir a una FEC específica. Este mecanismo puede ser empleado por toda la cadena de LSRs hasta el LER de egreso.
- **Mapeo de Etiquetas (label mapping):** en respuesta a una petición de etiqueta, un LSR downstream entonces manda (mapea) una etiqueta el LSR upstream correspondiente, usando este mecanismo de mapeo.

6.4.3.7. Protocolo de selección de rutas.

Una de las funcionalidades que tiene MPLS, principalmente en la transmisión de video, es que asegura que siempre habrá recursos disponibles para mantener el canal de transferencia fluido; cuando se cumplen los requisitos de QoS. Esto es muy importante en videoconferencias multipunto, en donde se asegura ancho de banda suficiente para el video y se acota un retardo máximo para la voz. Para hacer esto se necesitan dos cosas:

- Ruteo con QoS para determinar la métrica, los mas recomendados son:
  - **Ruteo de Salto a Salto** (Hop by Hop routing).
  - **Ruteo Explicito** (Explicit routing).

- Algoritmo de Ruteo basado en restricciones (Constraint-based routing algorythm), que permita reservar recursos para cada petición, los tres principales recomendados por la IETF son:
  - **LDP** (Label Distribution Protocol, RFC 3036);
  - **RSVP–TE** (ReSource reserVation Protocol – Traffic Engineering, RFC 3473);
  - **y el CR–LDP** (Constraint-Based Routing – Label Distribution Protocol, RFC 3472).

Dependiendo de como se establezcan los LSP se pueden presentar diversas opciones: Si se utiliza la aproximación **"hop by hop"** (o "salto a salto") para el establecimiento de los LSP la IETF ha recomendado (no obligatorio) el uso del protocolo LDP para la asignación de etiquetas, en este caso también se pueden utilizar los protocolos RSVP–TE y CR–LDP. Si la estrategia utilizada es la

“downstream unsolicited” donde el LER de salida distribuye las etiquetas que deben ser utilizadas para alcanzar un determinado destino, la única opción disponible es LDP.

Cuando la estrategia es “downstream on demand” iniciada por el LER de entrada y no se desea seguir el camino calculado paso a paso, sino que se desea utilizar el que permita definir una ruta explicita, las opciones actualmente disponibles son CR–LDP y RSVP–TE.

6.4.3.7.1. Ruteo con QoS.

6.4.3.7.1.1. Ruteo de Salto a Salto.

En este ruteo cada LSR escoge el siguiente salto para cada FEC, independientemente de los demás LSRs. En esta opción de utiliza OSPF (Open Shortest Path First), siendo uno de los protocolos de ruteo mas sencillos, provee solo algunas de las ventajas de MPLS como son: conmutación y apilado de etiquetas, trato diferenciadle paquetes de diferentes FEC pero con la misma ruta. Sin embargo no provee Ingeniería de Tráfico ni Políticas de Ruteo para el manejo de QoS.

6.4.3.7.1.2. Ruteo Explicito.

En el ruteo explicito el LSR de entrada o de salida define todos o varios de los LSRs por los que va a pasar el LSP dentro de un FEC determinado. Cuando el LER define todos los LSR se cumple completamente el ruteo explicito, si define solo algunos el ruteo explicito es parcial. Con cualquiera de la técnicas de ruteo explicito se manejan todos los beneficios de MPLS, tanto de ingeniería en tráfico como de QoS.

6.4.3.7.2. Algoritmos de Ruteo basado en restricciones.

6.4.3.7.2.1. LDP (Label Distribution Protocol.

Es la opción recomendada, aunque no obligatoria del la IETF. Todo LSR que soporte el protocolo LDP debe mantener sesiones LDP con otros LSR o LER que hagan lo mismo. Durante una sesión LDP se generan diversos tipos de mensajes con la finalidad de dar a conocer a otros enrutadores que el enrutador está vivo, mantener vivo dicho conocimiento, comunicar las asociaciones que el LSR haga de etiquetas o FECs, solicitar etiquetas a otros LSR, comunicar cuando una asociación ya no es válida, entre otras. En resumen el protocolo LDP mantiene el dominio MPLS en coherencia, en cuanto a las etiquetas y las relaciones que puedan tener con otros FECs en la red.

Los mensajes LSP son de suma importancia y deben de ser fiables al 100% ya que gracia a ellos es que MPLS funciona. Cuando se utiliza IP como protocolo de red, los LSRs anuncian su

estado mediante UDP/IP; si utiliza IP lo hace mediante multicast a todos los routers suscritos al dominio MPLS. Cuando los routers suscritos reciben el mensaje, que se comporta como un “ping” tradicional, estos los reenvían también. En los mensajes “ping” o ”hello” vía UDP se transporta también la IP del servidor que se anuncia con el fin de que si alguno de los LSR desea establecer una sesión LDP, lo hará con el protocolo TCP y a la dirección IP anunciada. Si se da el caso, se establece la conexión y se inicia una sesión LDP entre los LSR interesados.

6.4.3.7.2.1.1. Mensajes LDP.

Los pares LDP se podrán intercambiar cuatro clases de mensajes:

Mensajes de descubrimiento (discovery messages): se usan para anunciar y mantener la presencia de un LSR en la red. Un LSR mandará periódicamente por la red mensajes “hello” a través de un puerto UDP con la dirección multicast "todos los encaminadores de esta subred".

Mensajes de sesión: se utilizan para establecer, mantener y terminar sesiones entre pares LDP. Cuando un LSR descubre a otro por medio de mensajes HELLO utilizará un procedimiento de iniciación LDP por medio de TCP.

Mensajes de anuncio (advertisement messages): se usan para crear, modificar y eliminar asociaciones de etiquetas a FECs. Se transportan vía TCP. Cuando se haya establecido la asociación los pares LDP podrán intercambiarse este tipo de mensajes.

Mensajes de notificación: Los mensajes de notificación también se transportan vía TCP. Hay dos tipos de mensajes de notificación: notificaciones de error y notificaciones de aviso. El primer tipo se utiliza para notificar errores fatales, en cuyo caso terminará la sesión y se descartarán todas las asociaciones de etiquetas aprendidas en dicha sesión. El segundo tipo se utiliza para pasarle a un LSR información de la sesión LDP o el estado de algún mensaje anterior.

6.4.3.7.2.1.2. Identificadores LDP.

Un identificador LDP se utiliza para identificar el espacio de etiquetas de un LSR. Se compone de seis octetos, de los cuales los cuatro primeros identifican al LSR y los dos últimos identifican el espacio de etiquetas de dicho LSR. El espacio de etiquetas puede ser por interfaz o por plataforma. Si los dos últimos octetos tienen un valor de cero el espacio de etiquetas será por plataforma.

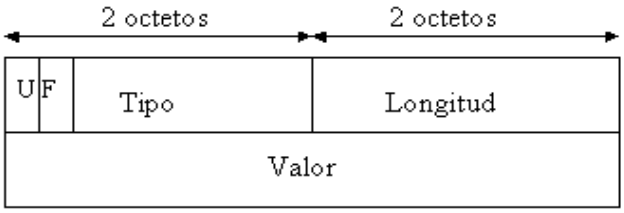
6.4.3.7.2.1.3. Sesión LDP.

Cuando un LSR utiliza LDP para anunciar más de un espacio de etiquetas a otro LSR, utilizará diferentes sesiones LDP para cada espacio de etiquetas. Como se comentó anteriormente, LDP utiliza TCP. Cuando dos LSRs requieren múltiples sesiones LDP, se establecerán sesiones TCP distintas para cada sesión LDP. En la especificación del protocolo RFC3036, se definen dos fases para el establecimiento de la sesión LDP:

- **Descubrimiento.** Existen dos modalidades, "básica" y "extendida". La básica, se utiliza si los LSRs están conectados directamente por medio de un enlace. Y la "extendida", es útil cuando se ha configurado un LSP entre dos LSRs.
- **Establecimiento y mantenimiento de sesiones LDP.** Una vez conocidos los vecinos se podrá establecer la sesión. Cada uno de los LSRs implicados puede jugar un papel activo o pasivo. El establecimiento de una sesión consta de dos fases: "conexión de transporte", que consiste en el establecimiento de una conexión TCP entre los LSRs implicados, para una nueva sesión LDP y el "Inicio de la sesión", basado en la negociación de los parámetros de la sesión.

6.4.3.7.2.1.4. Formato de los mensajes LDP.

Para el intercambio de mensajes entre LSRs se realiza mediante el envío de PDUs (Protocol Data Unit o Unidad de datos del protocolo) de LDP. Este envío se basa en la utilización se sesiones LDP que se establecen sobre conexiones TCP. Es importante destacar que cada LDP PDU puede transportar más de un mensaje LDP, sin que estos mensajes tengan que tener relación entre ellos. El protocolo LDP utiliza el esquema de codificación de mensajes conocido como **TLV** (Tipo, Longitud, Valor), cada mensaje LDP tiene la siguiente estructura:



U: campo de 1 bit que indica el comportamiento en caso de recibir un mensaje desconocido. U=0 hay que responder con un mensaje de notificación al LSR origen, U=1 se ignora el mensaje y se continua procesando el PDU.

F: campo de un bit. Este campo sólo se utiliza cuando el bit U esta en 1. Si se recibe un mensaje desconocido que debe propagarse y el bit F está en cero, este mensaje no progresa al siguiente LSR, en caso contrario si se hace.

Tipo: campo de 14 bits que define el tipo de mensaje y, por lo tanto indica cómo debe ser interpretado el campo valor.

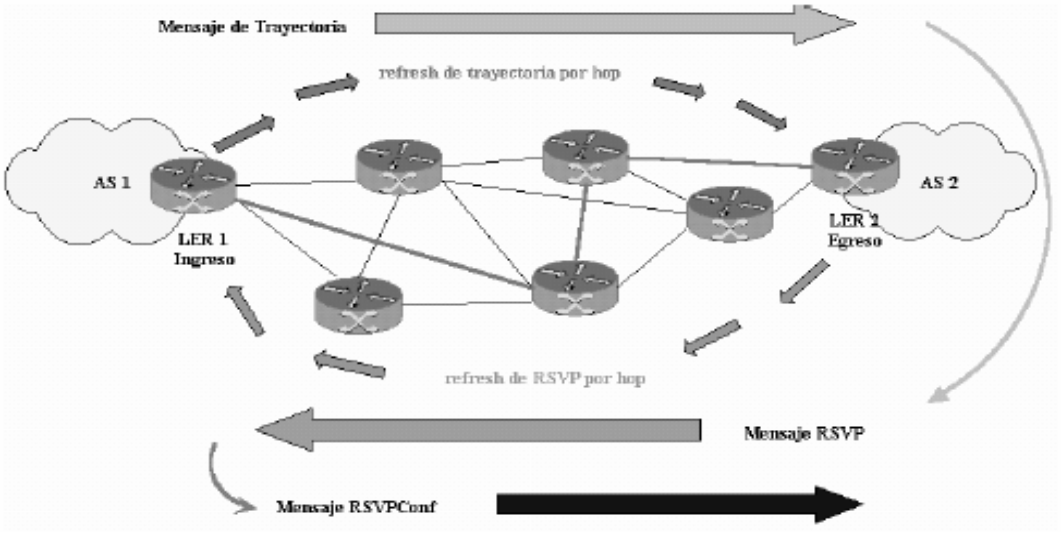
Longitud: campo de 2 octetos que especifica la longitud del campo valor.

Valor Campo de longitud variable que contiene la información del mensaje. La interpretación de la cadena de octetos de este campo depende del contenido del campo tipo.

6.4.3.7.2.2. RSVP–TE (ReSource reserVation Protocol – Traffic Engineering).

El protocolo RSVP–TE es una extensión del protocolo RSVP original, que fue diseñado para ejecutar la distribución de etiquetas sobre MPLS. RSVP–TE soporta además la creación de rutas explícitas con o sin reservas de recursos. Una de las características adicionales más importante de este protocolo es que permite el re-enrutamiento de los túneles LSP, con fin de dar solución ante caídas de red, congestión y cuellos de botella. El usar una extensión, no significa que deba ser totalmente implementado el protocolo RSVP por los LERs y LSRs con los que cuenta la red MPLS.

RSVP–TE es un protocolo de “estado suave” (soft state) que usa datagramas UDP o IP como mecanismo de señalización en el establecimiento de LSPs, incluyendo peticiones de etiquetas, mapeo, descubrimiento y mapeo. En la figura siguiente se muestra un ejemplo de la señalización en RSVP–TE.



Ejemplo de una LSP ruteada por RSVP–TE

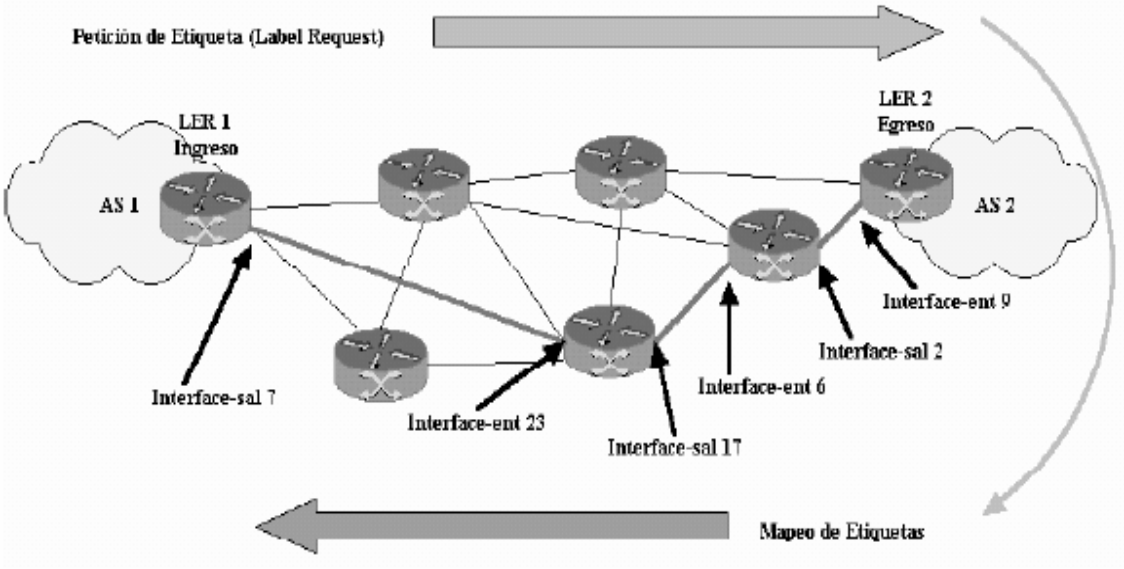
Primero se usa un protocolo BGP para descubrir el LER de egreso apropiado y así poder rutear el tráfico de AS1 a AS2, entonces el LER de ingreso manda un mensaje de trayectoria hacia el LER de egreso a través de cada LSR. Este mensaje de "refresh" de trayectoria que llega a cada nodo, ayuda a crear una sesión de trayectoria en cada LSR. Al llegar el mensaje al LER de egreso, este responde con un mensaje RSVP que se usa para la reservación de recursos (con parámetros de trafico y de QoS) en cada LSR upstream de la trayectoria. De nuevo el LER de ingreso manda un mensaje RSVPConf para confirmar el establecimiento de la trayectoria. Una vez establecida la trayectoria, esta tiene que ser mantenida por los LERs y LSRs por medio del constante envió de mensajes de refresh de trayectoria.

6.4.3.7.2.3. CR–LDP (Constraint-Based Routing–Label Distribution Protocol)

Conocido también como el protocolo de encaminamiento basado en restricciones LDP. Esta extensión del LDP se basa en el cálculo de trayectos que están sujetos a ciertas restricciones: ancho de banda, los requisitos de QoS, demora (delay), variación de demora o jitter, o cualquier otro requisito asociado al trayecto que defina el operador de la red. Esta es una de las herramientas más útiles para controlar el dimensionado del tráfico y la QoS en la red que pueden ofrecer a sus clientes y/o usuarios

Aunque no es tan específico como RSVP, no requiere de la implementación de un protocolo adicional. Usa las estructuras de mensajes existentes, y solo se extiende lo necesario para llevar a

cabo la implementación de la ingeniería en tráfico. Como en RSVP, CR–LDP soporta LSPs ruteados explícitamente (ya sean sueltos o estrictos). Se usa UDP para descubrir pares MPLS y TCP se usa para control, manejo, peticiones y mapeo (señalización). A continuación se muestra un ejemplo del establecimiento de trayectorias usando CR–LDP.



Ejemplo de una LSP estricta, ruteada por CR–LDP

Como se puede observar, se usan los mismos mecanismos de señalización LDP para establecer una LSP estricta limitada al paso por dos LSRs específicos. SE envía un label request en sentido downstream y un label mapping en sentido upstream para establecer la trayectoria. La trayectoria puede ser tan precisamente definida, como para especificar las direcciones IP de cada LER y LSR. Este sistema puede ser muy ventajoso para tráficos específicos, como voz o VPNs, ya que se puede definir la trayectoria óptima para satisfacer sus necesidades de ancho de banda y de prioritización.

CR-LDP y RSVP-TE son dos protocolos de señalización que realizan funciones similares en redes MPLS. Actualmente no hay consenso sobre si uno es superior tecnológicamente al otro.

6.4.3.8. Principales aplicaciones de MPLS.

Veamos brevemente las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales:

- **Ingeniería de tráfico (Traffic Engineering o TE).** Es posible forzar un camino dentro de la red MPLS, teniendo en cuenta aspectos de QoS como ancho de banda y disponibilidad de buffer, en lugar de los algoritmos de enrutamiento actuales (como IGP) donde se considera básicamente la menor distancia. Esto último es una ventaja importante, ya que no siempre el camino más corto es el menos congestionado y el más óptimo para ofrecer una mejor QoS a una aplicación en general. Es aquí donde se define Ingeniería de Tráfico como el proceso de controlar como el tráfico fluye a través de la red con el fin de optimizar el uso de los recursos y mejorar el rendimiento de la red. También se puede usar Ingeniería de Tráfico en ATM ya que también se tiene la posibilidad de forzar el camino, sin embargo, la ventaja de la Ingeniería de Tráfico MPLS es que se puede hacer directamente sobre una red IP. Esto permite realizar la Ingeniería de tráfico de manera más flexible, con menores costos de planificación y gestión para el administrador y con mayor calidad de servicio para los clientes.

- **Diferenciación de niveles de servicio mediante clases.** Está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ de la IETF. MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP. De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:
  - El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
  - Entre cada par de LSR exteriores se pueden poner múltiples LSP, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda.

  DiffServ sobre MPLS permite que se pueda ofrecer a los clientes unos servicios de QoS más predecibles.

- **Soporte de Redes Virtuales Privadas (VPN).** MPLS provee un mecanismo eficiente para el manejo de VPNs. De esta manera el tráfico de una red privada "atraviesa" la Internet eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico extremo y protegiendo la información.

  El problema que plantean las IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremos a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor. En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS.

VPN IP-Sec	VPN MPLS
Se configura a través de Internet	Se configura a través de una red privada
Sujeta a pérdida de paquetes, congestión y otros problemas propios de Internet	El MPLS permite garantizar latencias bajas y reducir la pérdida de paquetes.
Tunelado y encriptación para asegurara la integridad y confidencialidad de los datos	Integridad y confidencialidad de datos por VRF
No soporta CoS (class of service) ni QoS (qualitu of Service)	Permite implementar CoS y QoS
Cada sede necesita estar conectada a Internet para poder implementar VPNs bajo IP-Sec	Las VPN basadas en MPLS permiten compartir un único acceso a Internet entre todas las sedes. No es necesario que las sedes estén conectadas a Internet para acceder a la VPN.
El cliente necesita determinado software o Hardware	No require del cliente de acceso remoto ningún sofware o hardware especifico.

Diferencias básicas de una VPN basada en MPLS frente a VPN IP-Sec.

Las ventajas principales de implementar MPLS en VPN son:

- Maximizar la capacidad de ampliación.
- Actualización transparente para el usuario.
- Utilización optima de los recursos de la red.

- Diferenciación entre los servicios.
- Reducción de costos mediante consolidación de servicios.
- Seguridad y rapidez de transmisión de información.
- Uso de tecnología de vanguardia.

6.4.4. Combinaciones de diferentes técnicas de QoS.

Las tecnologías de QoS explicadas anteriormente en la práctica no se van a utilizar de forma excluyente y de hecho están diseñadas para ser utilizadas de forma conjunta con otras tecnologías para dar soporte a la QoS extremo a extremo.

La mayoría de las especificaciones de cómo se interrelacionan las diferentes tecnologías de calidad de servicio no están todavía estandarizadas, pero se han previsto varias arquitecturas para soportar calidad de servicio extremo a extremo.

6.4.4.1. IntServ/DiffServ.

Esta arquitectura propone usar una combinación de los modelos DiffServ e IntServ de forma estratégica para obtener un rendimiento óptimo de ambas en el entorno en que se usen. Para ello se propone que las aplicaciones se conecten a redes periféricas IntServ para solicitar, reservar y transferir los requerimientos de QoS, donde la clasificación MF y el control de tráfico por flujo son soportados.

Entre las redes periféricas IntServ se ubicaría la red DiffServ, por donde fluirán grandes volúmenes de tráficos, soportando control de tráfico agregado (control de tráfico basado en la clasificación BA, análisis del DSCP).

6.4.4.2. MPLS/IntServ.

Existe el propósito de usar un objeto en RSVP para predeterminar el camino a tomar por parte de las sesiones RSVP con etiquetas. Estas sesiones usan las conexiones establecidas por los encaminadores MLPS. Incluso sin este objeto es posible que MPLS asigne etiquetas con arreglo a las especificaciones de RSVP. En cualquier caso, la consecuencia es una simplificación del funcionamiento de IntServ en los encaminadores MPLS.

6.4.4.3. MPLS/DiffServ.

Como cabría esperar, dada la similitud entre MPLS y DiffServ, la traslación del tráfico DiffServ a conexiones MPLS resuelven gran parte de los problemas de QoS en las redes IP. DiffServ se apoya del campo Tipo de Servicio (ToS) clasificando los tráficos en diferentes clases en los nodos de ingreso al dominio DiffServ. MPLS realiza en cierta manera una clasificación similar a DiffServ, sólo que éste los clasifica y agrupa en FEC para garantizar QoS. Ambos emplean etiquetas, en DiffServ son conocidas como DiffServ Code Point (DSCP) y etiqueta MPLS en ésta última.

La etiqueta MPLS determina la ruta que un paquete tomará, lo cual permite optimizar el ruteo dentro de una red. Además es factible aplicar la Ingeniería de Tráfico, la cual garantiza la asignación de circuitos virtuales con ciertas garantías de ancho de banda para igual número de etiquetas que lo requieran. Por otro lado, el valor DSCP determina el comportamiento de los nodos de acuerdo a esquemas de colas (Queuing).

En la gran mayoría de estas arquitecturas mixtas, se plantean esquemas para mejorar el desempeño que ofrece MPLS, DiffServ e IntServ, no obstante ello, es necesario realizar un estudio y simulaciones previas de los posibles tráficos a soportar, de tal manera que se pueda seleccionar el mejor esquema. El seleccionar erróneamente uno de estos esquemas, podría ser la causa principal de bajo desempeño en nuestras aplicaciones sensibles a retardo.

7. CAPITULO VII. TELEFONÍA IP: COMO ESCENARIO DEL FUTURO DE LA TELEFONÍA Y DEL DESARROLLO DE NUEVOS SERVICIOS.

Este capitulo, evidencia las razones de porque la ToIP resulta tan atractiva para el futuro de las telecomunicaciones. En primer lugar, tras una breve introducción, se realiza un estudio comparativo entre, la PSTN como sistema de telefonía invariante en el tiempo, en relación a la ToIP como tecnología emergente en el mundo de las telecomunicaciones. Dado lo anterior, se hace referencia, al grado de implantación en el mercado, gracias a las ventajas que supone poder ofrecer al alcance de las PYMES y de los usuarios residenciales. Y finalmente su rol a futuro.

7.1. INTRODUCCIÓN.

La integración de voz y datos es en la actualidad, un tema candente en la comunidad empresarial, ya que promete ahorro en costes y fusión de infraestructuras de voz y datos. Si bien los sistemas telefónicos basados en PBX han demostrado claramente su valía en el pasado, existen evidencias crecientes de que las exigencias de la empresa moderna requerirán cada vez más la implantación de sistemas integrados de voz y datos. Hasta ahora, eran las PYMES las que mostraban una mayor predisposición a adoptar el nuevo estándar, pero ya son las propias grandes compañías, con los sistemas basados en PBX existentes, los que están empezando a sentirse atraídos por el significativo aumento de negocio y los beneficios en reducción de costes que puede suponer una migración a la tecnología ToIP.

Los principales beneficios se pueden resumir perfectamente de la siguiente manera:
Fusión de infraestructuras de voz y datos, con la consiguiente reducción de costos que la agrupación de los equipos de soporte conlleva.

- Se elimina la dependencia de sistemas PBX patentados, con sus cauces de actualización que son costosos y que adolecen de incompatibilidad con los productos de otras marcas. La ToIP ofrece una solución que no depende de un solo fabricante sino que se apoya en estándares adoptados universalmente.

- Llamadas de larga distancia económicas. Todas las llamadas que previamente se realizaban entre las distintas oficinas internaciones de una compaña, a las elevadas tarifas de las

llamadas internacionales, se pueden realizar ahora sobre los enlaces de datos WAN existentes en dicha compaña, lo que supone un ahorro considerable.

- Movilidad para los usuarios de teléfono IP. Puesto que un teléfono IP se identifica a través de su dirección MAC de Ethernet, se puede conectar en cualquier punto de la red. A diferencia de los teléfonos tradicionales que se han de conectar a puertos específicos en PBXs, los teléfonos IP permiten unas fáciles reestructuraciones de personal y espacio de oficina, como también facilitan nuevas prácticas de trabajo, por ejemplo el "escritorio virtual", donde el personal acude a la oficina y puede utilizar cualquier escritorio disponible. No obstante, los mayores beneficios provendrán, sin duda, por la vía de unas aplicaciones multimedia todavía más avanzadas. El hecho de que hasta el PC de sobremesa más básico tenga potencia para soportar aplicaciones de multimedia como videoconferencia y correo electrónico integrado con voz, impulsará el continuo desarrollo de las aplicaciones CTI (Computer Telephony Integration) o Integración de Informática y Telefonía, como las desplegadas por los call-centres basados en tecnología web.

La ToIP, forma parte de la nueva solución de comunicaciones unificadas, de voz y datos, para todo tipo de empresas, que permite ahorrar importantes costos frente a las centralitas tradicionales.

7.2. ESTUDIO COMPARATIVO ENTRE LA TOIP Y LA PSTN.

La telefonía tradicional utiliza la tecnología de conmutación de circuitos de una manera poco eficiente, debido a que utiliza un circuito físico completo, aun en periodos en que nada se transmite. En contraste, la ToIP usa tecnología de conmutación de paquetes, haciendo un mejor uso de los recursos de la red, dado que solo transmite cuando hay información que entregar, ahorrando de esta forma ancho de banda y por tanto, constituye una solución más económica.

7.2.1. Comparación de la Arquitectura de ambos Sistemas.

En cuanto a la arquitectura de ambos sistemas, se pueden encontrar diferencias de gran importancia:

Elemento	Telefonía Tradicional	Telefonía IP	Comparación
Terminal	Teléfono Tradicional	Teléfono IP, PC, Teléfono Tradicional + Adaptador	En la telefonía tradicional la inteligencia se delega en su mayoría al sistema centralizado, en cambio la telefonía sobre IP apuesta a delegar responsabilidad al usuario por tanto, a la terminal. Es importante recordar que la telefonía IP, en específico el estándar H.323, cuenta con un Gateway que provee la posibilidad de adaptar los teléfonos de la PSTN, a la red IP. A pesar de la digitalización del sistema PSTN, la nuevas aplicaciones sobre el teléfono se agotan, mientras que grandes manufactureras, como Cisco, apenas empiezan a explorar el sin fin de aplicaciones que posibilita una computadora hecha teléfono, tales como el despliegue, ya sea en el monitor o en el mismo teléfono, de la información completa acerca del cliente que llama a una empresa. Claro está que la diferencia en costo da mérito a su diferencia en cuanto a inteligencia, sin embargo para cada usuario existe un ahorro en otros sentidos como se verá más adelante.
Control de red	Central Telefónica	Gatekeeper	En este la diferencia es aún mayor, a pesar que mucha de la inteligencia dotada al Gatekeeper solventa las necesidades propias de una red compartida por varios servicios, el gatekeeper es por mucho superior tecnológicamente a la central, a pesar que el costo referente es mucho más bajo.
Conexión de la llamada	Central telefónica	Router	La central se limita a realizar una conexión entre dos terminales, ya sea por ayuda de otras centrales o internamente, no existe el concepto de mejor ruta, o el de direccionamiento dinámico (muchas veces proveído por el Gatekeeper). El router a pesar de que debe lidiar con asuntos relativos a la prioridad de tráfico, que le suma inteligencia innecesaria en una red como la PSTN (como el caso del Gatekeeper), la logística de enrutamiento es por mucho superior a la existente de la otra red. Es importante mencionar que esta capacidad de reasignar una ruta le suma confiabilidad al sistema ToIP, ya que una falla en una ruta será rápidamente censada (ya sea por medio del RTPC, u otro protocolo de control), lo que le da la oportunidad de cambiar de ruta dentro de la nube IP.

Señalización	Sistema SS7	Gatekeeper ISUP	Respecto al punto sobre la señalización el sistema SS7 fue desarrollado aparte de la red PSTN con el fin de que esta pudiera expandirse sin depender de la red de transmisión de voz, sin embargo en muchos ámbitos esto se ve como una debilidad, además que en la ToIP basta con el Gatekeeper (el cual puede ser redundante si se quiere), el cual ya se fabrica en tecnología modular, lo cual le da mayor flexibilidad y confiabilidad.
Conversaciones tripartitas o múltiples	Central Telefónica	Multipoint Control Unit	Al igual que en los casos anteriores la diferencia en cuanto al software del elemento IP y las tarjetas de la central telefónica es abismal
Interconexión entre redes	Gateway	Gateway	Este es un elemento propio de la red IP, el cual le da la posibilidad al proveedor y al usuario utilizar la red IP para transportar sus llamadas. Acentuando así las ventajas de una red sobre la otra, respecto a las plataformas e infraestructura existentes, además del aspecto económico y legal que será discutido más adelante.

Como se observó la arquitectura propuesta es por un lado más simple, y por otro mucho más completa. Una terminal, un enrutador y un servidor de llamadas (Gatekeeper) logran implementar la telefonía dentro de un sistema que está emergiendo y creciendo sin freno por todo el mundo,

7.2.2. Redes de Datos versus Redes de Voz.

Las redes desarrolladas a lo largo de los años para transmitir las conversaciones vocales, se basaban en el concepto de conmutación de circuitos, o sea, la realización de una comunicación requiere el establecimiento de un circuito físico durante el tiempo que dura ésta, lo que significa que los recursos que intervienen en la realización de una llamada no pueden ser utilizados en otra hasta que la primera no finalice, incluso durante los silencios que se suceden dentro de una conversación típica. En contraposición a esto tenemos las redes de datos, basadas en el concepto de conmutación de paquetes, o sea, una misma comunicación sigue diferentes caminos entre origen y destino durante el

tiempo que dura, lo que significa que los recursos que intervienen en una conexión pueden ser utilizados por otras conexiones que se efectúen al mismo tiempo.

Las redes en sí presentan semejanzas en cuanto se refiere a la cobertura actual, sin embargo el crecimiento de la red de Internet no conoce freno. Además ambas aplican el concepto del transporte de varias líneas sobre una misma, ambas por medio de la multiplexión. Existen algunas diferencias referentes al ancho de banda de 100Mbps de la red IP, a 64Kbps en la PSTN. En cuanto al medio el más popular para las líneas de IP el cable UTP de cuatro pares, el cual una vez centralizado, en un gateway (diferente al gateway para IP), un multiplexor, normalmente viaja sobre una sola línea, según la distancia ya sea UTP, coaxial, fibra óptica, microondas o vía satelital. La PSTN lo único que no comparte además del gateway es que el cable sólo contiene dos pares.

Desde que se popularizó la Internet, se hizo atractiva la posibilidad de utilizarla para transmitir voz. El motivo principal es que el costo de uso de una red IP normalmente es independiente de la distancia y a menudo independiente del tiempo de conexión, en contradicción con las tarifas de la telefonía convencional. Por otra parte, los avances en las técnicas de compresión de datos logrados en los últimos años no se han podido instrumentar en telefonía por la inercia económica que implica la infraestructura existente. Por último, la conmutación por paquetes característica de Internet es más eficiente en el uso del canal que la conmutación por circuitos utilizada en telefonía.

En general, las ventajas que se obtienen al comprimir la voz con códigos más sofisticados y por la supresión de los períodos de silencio, son contrarrestadas por la tarea (overhead) impuesta por la necesidad de dotar a cada paquete de voz con la información necesaria para enrutarlo a su destino, por lo que es difícil estimar exactamente cuál será el ancho de banda requerido por un sistema de VoIP. Sin embargo, este ancho de banda es siempre considerablemente inferior a los 64 kbps requeridos por la codificación PCM en la telefonía clásica.

Hoy en día, los equipos que logran la tarea de digitalizar, empaquetar y comprimir la voz, lo establecen en un ancho de banda de 10Kbps, en referencia a 64Kbps de la telefonía tradicional.

El fin es lograr proveer la misma calidad de voz, en cuanto a audio y seguridad.

7.2.3. Regulación.

Todo el concepto de unificación de servicios, incluyendo nuevas tecnologías significa un reto para las entidades reguladoras, ya que no calzan dentro del modelo que se ha acarreado, el cual trata servicios de voz y datos por aparte. Especialmente en aplicaciones de terminal a terminal, la introducción de ToIP presenta aspectos relativos a: la colección de fondos de servicios universales y

obligaciones para proveer un servicio universal; pago de acceso u otro tipo de interacción con proveedores locales, de larga distancia e internacionales; calidad de servicio; y el impacto sobre la taza fiscal en los lugares donde estos servicios todavía forman parte de un monopolio.

Sin embargo el tema gana cada día más terreno en las sesiones de organismos internacionales. Una vez vencida la barrera reguladora la ToIP no tendrá límite.

Las empresas de telecomunicaciones dominantes en el mundo han respondido a ToIP de varias maneras. Algunos países de Medio Oriente, han prohibido esta tecnología para proteger sus empresas de telefonía tradicional. Pero en el mundo desarrollado las entidades reguladoras, han respondido de otra forma. Por ejemplo, cambiando a nuevas estructuras de precios, reduciendo sus cobros por llamada y elevando sus cobros mensuales por renta de línea. Muchos operadores han cancelado por completo sus cobros por llamada y ofrecen llamadas locales, nacionales y aun algunas internacionales de manera ilimitada por una cuota fija mensual.

Por el momento hay que considerar, que Chile, al igual que muchos países, no cuenta con regulación en la materia. A mediados del 2004, la Subsecretaría de Telecomunicaciones (Subtel) elaboró un documento de consulta para promover la discusión acerca de la regulación de los servicios de VoIP. Según consta en el documento, el propósito de esta iniciativa es "definir un instrumento normativo que permita la introducción de esta tecnología, sin causar inestabilidades regulatorias, de manera de que los usuarios finales puedan disponer de más y mejores servicios".

Las propuestas de la Subtel generaron cierto rechazo entre las principales operadoras, por lo que la normativa todavía se encuentra en estudio, pero que sin duda es un tema que deberá resolverse en el corto plazo para beneficio de todos los actores. Lo único claro hasta el momento es que la ToIP ha obligado a las empresas de telefonía ha adecuar y ampliar sus servicios y pensar en la futura transmisión de datos por una sola red.

7.2.4. Aplicaciones.

Las múltiples aplicaciones es probablemente la razón principal por la cual el mercado decidirá en un futuro hacer la transición hacia la ToIP. Ya que es posible que la competencia obligue a los proveedores de telefonía tradicional a bajar sus tarifas, y equilibrarse con las ventajas del servicio IP. Sin embargo en cuanto al crecimiento de fantasía que promete la ToIP, la PSTN se queda atrás, debido a la carencia de inteligencia en su sistema además del alto costo en cambios arquitectónicos.

Las aplicaciones de la ToIP se pueden seccionar en tres:

- Gracias a la naturaleza inteligente y al acceso de las bases de datos: todas aquellas aplicaciones que relacionan una dirección IP con una base de datos, ya sea para identificación, para acelerar procesos de atención al cliente en call centres, procesos de compras por medio del mismo sistema. Además por ejemplo aplicaciones para el record de llamadas, grabado y reproducción de ellas, etc.
- Gracias a la facilidad de escalamiento: todas aquellas que incluyen la unificación de la llamada con un fax, mensajes de texto o correo electrónico. Además la integración del transporte completo de multimedia, video conferencias en sonido estéreo, y otros.
- Gracias a la relación Internet-voz: Facilidad de navegación por medio de buscadores accesibles por teléfono, interactuar con una compañía por medio de la página Web y el teléfono, entre otras.

En este momento parece ser que la mejor forma de expansión de la PSTN es por medio de los Gateways del estándar H.323 o SIP, para entrar en el juego del nuevo siglo.

Con el fin de concluir este apartado, se resume en la siguiente tabla, brevemente, las características más relevantes de ambas tecnologías:

Telefonía Tradicional (PSTN)	**Telefonía IP**
Su red actual no puede ser, por motivos técnicos y económicos la red a integrar: Es difícil integrar transmisión de datos con QoS, además video y audio de alta fidelidad están fuera de alcance. Ancho de banda: desde 64Kbps por línea.	Ideal para la integración de servicios: En cuanto al concepto de la convergencia de redes la ToIP es ideal para estandarizar la transmisión de voz y en el futuro todo el paquete multimedia sobre la red IP que es la más popular y completa. Ancho de banda 100Mbps por línea.
Los proveedores de servicios así como, los fabricantes, usuarios y autoridades reguladoras deben de preocuparse por este sistema de telefonía como caso específico, además de las demás redes.	En el caso de la convergencia de redes, se cada vez más fácil de regular, administrar y mantener

La red cuenta con una alta inercia económica, lo cual limita el crecimiento de la infraestructura.	La red es fácil de manipular y las ampliaciones pueden ser realizadas a bajos costos. Además tiende a ser una red modular lo que le agrega flexibilidad. Es importante mencionar que los costos de mantenimiento de una red son mucho menores que el de dos o más de ellas.
En cuanto a las tarifas del usuario este sistema depende de la distancia y del tiempo.	Los costos dependen del mercado y no del tiempo de conexión. Lo cual reduce las tarifas para el usuario final.
El direccionamiento es fijo.	El direccionamiento es dinámico.
El enrutamiento es fijo.	El enrutamiento es dinámico, lo que provee mayor confiabilidad ya que al estar una ruta caída, el resto de los paquetes pueden ser enrutados por otro camino.
Los estándares en cuanto a protocolo y equipo son de naturaleza privada, por tanto las aplicaciones se ven limitadas a los proveedores y sus manufactureras	La red IP no tiene propietario, además entidades como ITU y IETF han definido estándares que prometen operación multifabricante y multiproveedor. Lo cual incrementa la posibilidad de innovaciones en dicha tecnología.
El ancho de banda de las líneas telefónicas se mantiene dedicado completamente durante toda la conversación se utilice o no.	El ancho de banda asignado es exclusivamente el demando por el paquete, aprox. 10Kbps. Existe un manejo inteligente del recurso ancho de banda.
Su mercado se ha mantenido estable en los últimos años, generando un crecimiento insignificante.	La explosión de la demanda de acceso a la red de datos es evidente. El mercado crece rápidamente, apuntando al año de la Telefonía sobre IP.

Las aplicaciones más importantes son: • fax, • conversación tripartita, • identificador de llamadas, • correo de voz, • llamada en espera, • clasificación de llamadas, • interacción con máquinas contestadoras que proveen servicios de información, usando como medio los dígitos, • líneas troncales para adherir centrales telefónicas privadas en empresas. • Conexión a Internet por medio de MODEM a 56Kbps. Sin embargo las posibilidades se agotan y tienden a usar la Internet como soporte.	Al contrario de la PSTN, las posibilidades en este apenas empiezan a imaginarse, algunas de las más importantes son: • Transmisión de fax, e-mail, y mensajes de texto, • conversación de varios usuarios, en sonido estéreo si se quiere, • despliegue de la información completa del usuario que llama, ya sea por el monitor o sobre la interfaz del teléfono IP, • la posibilidad de mantener el correo de voz en la PC, con las ventajas que un software puede ofrecer, • despliegue de todas las llamadas entrantes, con la posibilidad de escoger cualquiera, • aplicaciones web con modalidad click para hablar o click para enviar fax , (soporte telefónico para e-commerce) brindando completa interacción con las compañías, • transmisión de video en tiempo real, • mayor facilidad para las empresas que poseen una LAN. • Monitorio, por medio de software de las llamadas.
La red provee todos los estándares para logran un QoS alto. Sin embargo su límite casi ha sido alcanzado.	En este momento se implementan nuevos y mejores estándares y equipos para lograr un QoS igual y eventualmente mejor al que provee la PSTN.
La seguridad de la llamada es de alto nivel, sin embargo con una intervención física la red puede ser fácilmente invadida.	La seguridad es un asunto de alta delicadez, soluciones como redes privadas, se ven sustituidas por redes virtualmente privadas donde la simple conexión no da la posibilidad de intervenir los paquetes.

7.3 ANÁLISIS DE LA INCORPORACIÓN DE LA TOIP EN GENERAL Y VISIÓN DE FUTURO.

Para las empresas, la ToIP ya no es simplemente una opción "interesante" a la hora de adquirir sistemas de telecomunicaciones, sino que es una necesidad absoluta desde el punto de vista de ahorrar costos al máximo y conseguir el deseado retorno de la inversión.

7.3.1. Migración a un sistema de ToIP.

La migración será el escenario más común, puesto que la mayoría de los emplazamientos disponen al menos de una infraestructura de telefonía tradicional. El sistema de ToIP se debe integrar de forma paralela a la infraestructura existente. Es recomendable una migración por fases. A continuación se muestran las etapas de implantación:

1. **Fase 1: Prueba de transmisión de voz sobre los enlaces WAN existentes**

   Esto se puede llevar a cabo con los teléfonos analógicos, PBX y routers existentes. El requisito primario es un gateway a la red IP que ha de tener un módulo para el router, o bien un dispositivo externo independiente. El gateway proporcionará interconectividad entre el sistema PBX/teléfono y el router y proporcionará prestaciones como muestreo, digitalización y formación de paquetes. Inicialmente se deben seleccionar dos emplazamientos con tan solo uno o dos teléfonos en cada ubicación. Los gestores de red serán capaces entonces de analizar el tráfico WAN para determinar el impacto sobre la utilización del ancho de banda, mientras que un incremento en el número de teléfonos le permitiría al gestor hacer la previsión de cualquier necesidad de capacidad de ancho de banda adicional. También se puede llevar a cabo un análisis financiero para comparar el ahorro producido por estas llamadas entre oficinas. Una vez que los enlaces WAN estén transmitiendo de forma satisfactoria el tráfico de voz entre oficinas, al personal de informática le resultará posible implantar prestaciones de QoS en los routers situados a ambos extremos para comprobar la repercusión del tráfico pesado de datos sobre la calidad de voz. Las prestaciones de QoS, como priorización de colas y compresión de encabezado RTP, son estándares en la mayoría de los routers y se pueden configurar fácilmente de forma que se posibilite su experimentación. En esta fase voz y datos se deben combinar solamente sobre enlaces WAN.

2. **Fase 2: Incorporación de teléfonos IP**

   Una vez que la LAN esté convenientemente preparada para VoIP (los hubs habrán sido remplazados por conmutadores que cumplan 802.1p en el armario de cableado) se podrán conectar los teléfonos a la misma, junto con los PBX de IP en ambas oficinas. No se requieren cambios de routing y las llamadas de teléfono externas pueden ser conmutadas todavía a través del PBX existente. Se puede analizar el tráfico LAN y con la incorporación de más teléfonos IP, los técnicos podrán ahora planificar la fase de eliminación del resto de los teléfonos analógicos / digitales existentes en cada emplazamiento.

3. **Fase 3: retirada del PBX**

   Una vez completada la migración a teléfonos IP, el PBX tradicional se retira y se sustituye con una línea E1/T1 desde el gateway al conmutador Local.

7.3.2. Predicciones del mercado.

En Chile, según los datos aportados por los distintos fabricantes y proveedores (por ejemplo: Cisco System, Telmex, RedVoiss, Netline, Call-IP, etc.), a través de diversas consultas, el avance de la telefonía IP es algo imparable en todo los segmentos de mercado, aunque se trata de un fenómeno que está teniendo una especial fuerza en el mundo de las empresas, tanto en la PYME como en entornos corporativos. Precisamente esta última parcela es el que se encuentra a la cabeza en el despliegue de este tipo de soluciones, y como sucede con frecuencia, son las grandes empresas las primeras en estudiar la implantación de estas nuevas soluciones. Algunos de los sectores especialmente involucrados en esta tecnología son el financiero, el hotelero o el de la salud.

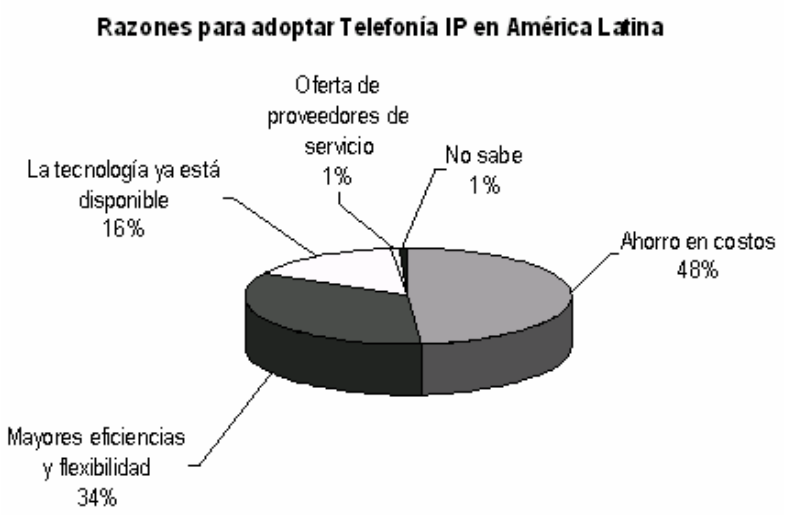
La oferta del mercado de ToIP es variada. La mayoría de los proveedores de soluciones de comunicaciones ofrecen dos opciones: la migración o actualización de la infraestructura instalada (lo que sería lo mismo que IP Enabled) y la sustitución completa o adquisición de equipo nuevo (IP Puro). También hay fabricantes de peso que impulsan muy fuerte este segundo escenario. El 19 % de las grandes empresas nacionales ya tiene una solución de ToIP implementada en sus oficinas, esperando un incremento del un 32 % para el 2007.

A nivel Internacional, según diversas consultoras, como Frost & Sullivan, IDC y Probe Research, los pronósticos indican un crecimiento significativo en el mercado de la ToIP.

De acuerdo con el estudio de IDC (International Data Corporation), la principal razón que lleva a las empresas a migrar de sus soluciones de voz tradicionales a ToIP, es el ahorro en costos, en

la medida en que las empresas de todos los tamaños tienen una presión fuerte para reducir sus inversiones en capital en telecomunicaciones y sus gastos operativos. Por esto la convergencia (integración de voz y datos en una misma red) emerge como una solución real para reducir costos y generar aumentos en productividad

El 42 % de las empresas de Latinoamérica está implementando o utilizando sistemas de ToIP en el 2005, versus un 28 % en el 2004, y para el 2006 se pronostica más de 50 % de las empresas que implementarán ToIP. (Según se desprende de la encuesta realizada por IDC, "ToIP En Latinoamérica, Perspectiva del usuario Final, 2005).



Hacia el 2010, se estima que un 35% de las llamadas telefónicas en todo el mundo será efectuado sobre redes basadas en IP (Protocolo de Internet).

7.3.3. Empresas que brindan soluciones de ToIP.

Aunque las posibilidades a largo plazo de la ToIP están constituidas por las nuevas funciones y aplicaciones que traerá consigo dicha telefonía, su ventaja a corto plazo son los recortes de costo que permite en comparación con la telefonía convencional con conmutación de circuitos. Para los consumidores, la ToIP es siempre más barata que las llamadas con conmutación de circuitos, especialmente en el caso de las llamadas originadas en mercados no liberalizados o transmitidas por Internet y/o que generan ingresos con la publicidad.

Dentro de los entornos corporativos, se tiene la participación de:

Cisco System es líder en **soluciones PBX IP-puro**. La participación de Cisco en Latinoamérica en el mercado de ToIP es: Argentina 91 %; Chile 69%; México 73 %; Brasil 53%; Colombia 53 % y Venezuela 11 %, siendo sus más cercanos competidores Nortel, Avaya y 3Com.

En el segmento de Teléfonos IP, Cisco tiene el 42.7 %, seguido por Avaya (11.3 %) y Nortel (8.4 %) a nivel mundial, de acuerdo con Sinergy Research. En el segmento de Voz por paquetes para empresas, Cisco tiene el 36.3 %, seguido por Avaya (19.5 %) y Nortel (7.9%). En el segmento de Gateways de Voz para empresas, Cisco tiene el 73.2 %. En el segmento de ToIP Empresarial, Cisco tiene el 27.4 %, seguido por Avaya (21.5%) y Nortel (9.9 %).

Otras compañías con menor participación en entornos corporativos, pero con gran protagonismo en entornos residenciales en chile, tenemos:

NETLINE provee el servicio "**Dilo IP**". Es el primer servicio de ToIP en Chile orientado a usuarios residenciales. Esta tecnología se puede ejecutar desde un teléfono tradicional o de un IP Phone inalámbrico (bajo una conexión Wi-Fi).

Con este servicio se puede llegar a reducir la cuenta telefónica entre un 70 % y 90 % menos, gracias a las convenientes tarifas de larga distancia nacional e internacional.

Este servicio, en algunos destinos, un minuto de llamada puede ser hasta un 90 % más barato que en la telefonía tradicional y entre clientes de la empresa las llamadas son gratis (llamadas On Net). Por ejemplo, el minuto a Buenos Aires, Argentina, tiene un costo de $14, USA $21 y todo Chile a $24. (IVA incluido).

Para acceder al servicio "dilo IP" sólo se debe contar con una conexión de banda ancha a Internet y alguno de los 3 kit "dilo IP" disponibles en el mercado. De lo cual dispone de servicios adicionales como: movilidad geográfica, mensajería, acceso a llamadas de emergencia, conferencia tripartita, redirección de llamadas, entre otras.

Valor de llamadas por minuto						
	Local	Larga distancia Internacional		Larga distancia Nacional desde santiago		
Telefonía	Dentro de Santiago	B.Aires	Lima	Concepción	Valparaíso	Antofagasta
Tradicional	18*	106**	106**	203**	177**	230**
Netline	15	14	26	24	24	24
RedVoiss	15	12	24	22	22	20

Cifras en pesos ($). *Horario normal. **Más $47 por cargo de acceso.
Fuente: Centro de atención de las compañías.

Igualmente RedVoiss, hoy en día, posee un gran protagonismo en el mercado a través de su servicio **"SippyPhone"**, que consiste en una excelente y flexible herramienta de comunicaciones vía Internet, ejecutable a través de un PC.

RedVoiss, es la primera empresa en Latinoamérica y Chile en ofrecer el servicio ASP (Application Service Provider) de voz: "ToIP". Permite realizar llamadas a teléfonos de la red pública de todo el mundo (Off Net), con tarifas muy económicas. Y hacer y recibir llamadas gratis e ilimitadas entre usuarios (On Net). Dentro las tarifas destacadas, por ejemplo, el minuto a USA tiene un costo de $21, a Argentina $12, y $16 como destino Santiago-Chile.

Es evidente que proporciona un gran ahorro en el costo de las llamadas, lo que es avalado por más de 14 mil usuarios que operan bajo esta red. Como lo es el caso de: CDF (canal del fútbol), Carozzi, Universidad Federico Santa María, etc.

Y otros servicios como: "SippyPhone Number", permite a su SippyPhone recibir llamadas desde la red telefónica tradicional a través de un número de teléfono real de la red pública. Y otros servicios como WebPhone (ToIP desde una Pág. Web).

A estas empresas podemos añadir otras como, **ITSW WORLDWIDE SA**, empresa chilena líder en la comunicación desde Softphones a teléfonos de red fija y celulares, con cobertura nacional e internacional. Y Además otras soluciones integrales tales como: ENTEL IP, Tecnoera, Enet, Call IP, etc.

7.3.5. Facilidad de escalabilidad en la convergencia de servicios.

La ToIP ofrece todos los servicios tradicionales de voz, además de nuevas funciones que enriquecen la infraestructura de comunicaciones.

Al estar los elementos que controlan la ToIP, conectados a la red IP, se hacen accesibles en forma nativa a otros servidores informáticos (como servidores de correo, de Web, etc.). Puesto que están montados sobre la misma infraestructura de comunicaciones, se facilita su interoperabilidad. Pueden brindarse varios servicios de llamada telefónica básica y de valor agregado, como por ejemplo: mensajería unificada, multiconferencia, videotelefonía, consultar entornos Web o gestionar directorios, enviar fax, entre otros servicios. Estos servicios son ofrecidos por los ITSP de distintas formas, según las necesidades del cliente.

A continuación, se hace referencia a los más relevantes:

- **Mensajería unificada**

  La mensajería unificada brinda facilidades para que los usuarios recuperen, respondan y administren todos sus mensajes, independientemente del horario, ubicación o dispositivo. La mensajería unificada usa un enfoque inteligente para encaminar las llamadas telefónicas, los mensajes de voz, el correo electrónico y los faxes, de acuerdo a categorías definidas por el usuario, incluso tipo y prioridad, hora y fecha. Los usuarios tienen acceso y administran sus mensajes de voz, correo electrónico y fax mediante un solo casillero de entrada, y todos sus mensajes son accesibles desde una PC, una conexión a Internet o desde cualquier teléfono por tonos.

- **Multiconferencia.**

  La ToIP permite la conexión de 3 o más usuarios simultáneamente compartiendo las conversaciones de voz o incluso documentos sobre el que todos los miembros de la multiconferencia pueden participar en la revisión, esto resulta de gran utilidad para empresas que realicen reuniones virtuales, con los consiguientes ahorros de gastos que supone el desplazamiento de personas.

- **Videotelefonía**

  Es un servicio audiovisual, que permite la comunicación entre clientes mediante voz e imágenes en tiempo real, mejorando la comunicación dado que un buen porcentaje es no verbal. Se requiere de un videotelefóno o precisar de un PC conectado al teléfono IP y una webcam. Ambos interlocutores deben tener conexiones de alta velocidad a Internet (con un servicio de “envío de información” de 256 Kbps se garantiza una notable calidad de

transmisión de imagen que permite la comunicación), y, en la mayoría de los casos, el mismo tipo de videoteléfono.

- **Redes Privadas virtuales de Voz (PABX IP y Centrex IP).**

  Permiten la interconexión de las centrales telefónicas privadas por medio de la red de datos de la empresa. De esta manera, se pueden generar llamadas gratuitas, si se aprovecha la infraestructura de datos ya existente.

- **Servicios de directorio.**

  Para que cualquier empleado pueda acceder fácilmente y desde su propio terminal telefónico a la base de teléfonos de la organización.

- **Señal de espera de e-mail.**

  El servicio de señal de espera de e-mail le informa al suscriptor que ha recibido un mensaje de e-mail utilizando el mismo método que usa el sistema de mensajes de voz basados en la red. Esta información se recibe en el teléfono del suscriptor, sin la necesidad de encender la PC. La información de espera de un mensaje se señala a través del panel de visualización del teléfono, un LED o un tono de discado especial "entrecortado" similar a un correo de voz.

- **Llamada en espera de Internet.**

  Mientras un suscriptor está "navegando por" Internet, el servicio de llamada en espera de Internet alerta al usuario de que hay llamadas entrantes por medio de una ventana en la pantalla. Hasta ahora, la persona que recibe la llamada no tiene manera de reconocer y aceptar las llamadas entrantes. La línea de teléfono estaría constantemente ocupada mientras el usuario está conectado a una sesión de Internet. Este nuevo servicio le permite al receptor decidir si acepta o no la llamada o si continúa con la sesión de Internet y tal vez, llama más tarde.

- **Realización de la llamada.**

  Este servicio es como el servicio anterior (de llamada en espera de Internet), excepto que la sesión de Internet no necesita interrumpirse para aceptar la llamada. Utilizando la capacidad de Voice Over-IP (por ejemplo del switch integrado EWSD multi-servicio de Siemens), el receptor puede hablar desde el PC y continuar, de este modo, con la sesión de Internet ininterrumpida mientras acepta llamadas telefónicas entrantes.

- **Servicios avanzados de centralita.**

  Solución que permite, "operadora automática", posibilidad de configurar menús que permitan al usuario acceder a diferentes departamentos, dejar datos grabados, etc. sin necesidad de una recepcionista que controle el proceso. Encolamiento de llamadas, música en espera, identificación de llamadas y otras muchas funciones que facilitan y optimizan la atención de las llamadas.

- **Centros de llamadas (Call centers).**

  Los centros de llamadas pueden usar la ToIP, mejorando la calidad de la información intercambiada en cada sesión. Por ejemplo un usuario podría navegar por información on-line, antes de realizar la consulta a un operador. Una vez en comunicación con el operador, se podría trabajar con un documento compartido a través de la pantalla. De esta forma se consigue sistemas de una gran calidad en el servicio a ofrecer, además de reducir de forma considerable el costo de líneas telefónicas y de Distribuidores Automáticos de Llamadas (ACD).

- **Comercio electrónico.**

  Es la aplicación de la que se espera un fuerte crecimiento en los próximos años. A fin de proveerlo, se necesita una fuerte integración entre los servicios vocales y de datos. Así, sería atractivo para aquel usuario que está visitando una determinada página Web, se comunique telefónicamente con un agente de ventas (por ejemplo, a través de un botón o vínculo en dicha página). También es conveniente para el agente que al recibir la llamada pudiera disponer de información adicional como el historial de las páginas visitadas por el usuario, los datos de éste y, si existiera, su historia de relación con la compañía en cuestión, cuidando de no entrar en contradicción con el derecho de los usuarios a la privacidad de sus datos personales. Dentro de dicha historia, se podría encontrar un perfil de preferencias del usuario, qué tarjeta de crédito posee, etc. para que el agente pueda ofrecer "con más certeza" lo que el cliente necesita.

- **Aplicaciones de FAX.**

  Al igual que se hace con la voz, cabe la posibilidad de realizar transmisiones de FAX sobre redes de ToIP, consiguiendo de esta manera reducir de forma significativa los costos de una empresa en transmisión de fax. En este caso no es necesario para el usuario que recibe el fax de disponer de equipos especiales ya que los faxes se seguirán recibiendo a través de una máquina de fax convencional. Una aplicación típica en este tema es el envío masivo de fax, ya

que el usuario sólo enviará una copia del fax que desea enviar, así como la lista de números telefónicos de destino y el sistema se encargará de realizar todos los envíos enrutando los faxes al punto desde donde la llamada de destino es más económica.

- **Entrada controlada por el suscriptor.**

  Utilizando la tecnología basada en la Web, los suscriptores pueden por sí mismos configurar estos servicios de llamadas personalizadas para sus líneas telefónicas con la ayuda de una interfaz gráfica fácil para el usuario en sus PCs. También pueden obtener una visualización online de los gastos actuales de servicios, que en consecuencia, puede reducir en un 40 % estimado los costos de aprovisionamiento al cliente de los proveedores.

7.3.6. Ventajas y desventajas en la adopción de ToIP.

La ToIP aporta numerosos beneficios para las empresas, tanto de carácter tangible como de negocio. Dentro de las ventajas encontramos:

- **Un único numero de teléfono.** En primer lugar, la ToIP permite la movilidad geográfica y que el usuario del servicio disponga de su extensión telefónica en cualquier punto donde haya conexión a Internet. En consecuencia, el acceso remoto a la compañía y el teletrabajo cobran relevancia por la efectividad de la solución.

- **Ahorro de costos.** Con los sistemas de telefonía basados en IP se han detectado ahorros tan considerables, cerca tanto como el 74% respecto a la facturación de las compañías de telefonía tradicional, lo que es sustancial para aquellos usuarios que realizan muchas llamadas de larga distancia (llamadas internacionales). Las llamadas internas entre sedes de la empresa suelen ser gratuitas. Y en cuanto a los usuarios residenciales, es muy beneficioso, ya que las comunicaciones no dependerán de la duración de la llamada, como es el caso de PSTN, sino más bien por el precio de mercado del ITSP.

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

- **Mensajería unificada y Correo de voz.** La ToIP permite asimismo la unificación de los sistemas de gestión, de los sistemas de mensajería (vocal y electrónica), la unificación en equipamiento de acceso al domicilio del cliente, contratos de mantenimiento, formación del personal, etc., lo que se traduce claramente en beneficios tanto en funcionalidad como en costos.

- **Recursos optimizados.** Puede reducir los costos de mantenimiento, ya que las empresas sólo tienen que encargarse del mantenimiento de una única red de voz y datos, en lugar de dos redes diferentes. Además, los costos de los traslados, nuevos usuarios y cambios (MAC, Mores, adds and changes), resulta un proceso pesado cuando se utiliza un sistema basado en telefonía tradicional que implica un acceso físico a la centralita, reduciéndose casi a cero con los sistemas IP, ya que se pueden realizar de forma remota, con una herramienta de autogestión de usuario basada en la web o desde una única consola con funciones complejas.

- **Impuestos y Cargos Adicionales.** Actualmente, la ToIP está sujeta a menos impuestos y cargos reguladores que el servicio telefónico estándar. No obstante, esto podría cambiar ya que las nuevas políticas federales y estatales evolucionan a la par que la tecnología y la tendencia hacia un mercado de telecomunicaciones más competitivo.

- **Ventajas para las entidades corporativas.** Esta convergencia de servicios de voz, datos y vídeo en una sola red implica para una empresa que lo adopte, un menor costo de capital, procedimientos simplificados de soporte y configuración de la red y una mayor integración de las ubicaciones remotas y oficinas sucursales en las instalaciones de la red corporativa. La ToIP utiliza la red de datos para proporcionar comunicaciones de voz a toda la empresa, a través de una sola red de voz y datos. Es evidente que el hecho de tener una red en vez de dos, es beneficioso para cualquier organización. ToIP proporcionaría a las sucursales de una misma empresa, comunicaciones gratuitas entre ellas, con el ahorro de costos que esto supondría. No solo entre sus sucursales, sino entre proveedores, intermediarios y vendedores finales, las comunicaciones se podrían realizar de forma completamente gratuita. Además, la red de comunicaciones de la empresa se vería enormemente simplificada, ya que no habría que cablear por duplicado la red, debido a que se aprovecharía la red de datos para voz. Esta capacidad permite a las compañías reducir los costes de fax y teléfono, agrupar los servicios

de datos, voz, fax y vídeo, y construir nuevas infraestructuras de red para aplicaciones avanzadas de comercio electrónico.

- **Videoconferencia integrada o Multiconferencia.** Con los datos de ancho de banda requeridos actualmente (de 8 a 16kbps por llamada), se podrían establecer de 15 a 30 comunicaciones simultaneas con una línea ADSL estándar, que podría satisfacer sobradamente los requerimientos de una mediana empresa.

- **Ventajas para los operadores o proveedores del servicio.** Es obvio que este tipo de redes proporciona a los operadores una relación ingreso/recursos mayor, es decir, con la misma cantidad de inversión en infraestructura de red, obtiene mayores ingresos con las redes de conmutación de paquetes, pues puede prestar más servicio a sus clientes. Otra posibilidad sería que prestará más calidad de servicio, velocidad de transmisión, por el mismo precio.

Y dentro del las desventajas tenemos:

- **Calidad de la comunicación.** Algunas de sus desventajas son la calidad de la comunicación (ecos, interferencias, interrupciones, sonidos de fondo, distorsiones de sonido, etc.), que puede variar según la conexión a Internet y la velocidad de conexión del ISP. Por ahora, el servicio está restringido a redes privadas (y en consecuencia a pocos usuarios), ya que en un ambiente como una red pública Internet, los niveles de calidad telefónica son bajos pues tal red no puede proveer anchos de banda reservados ni controlar la dramática fluctuación de carga que se presenta.

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

- **Asuntos con 911.** A diferencia de las redes telefónicas tradicionales, una llamada a 911 de un teléfono de Internet no siempre podrá suministrarle al centro de llamadas de emergencia el número y localización de la persona que está llamando. Muchos proveedores de servicios de

ToIP siguen mejorando sus servicios de 911, u otra forma de marcación rápida para acceso a servicios de emergencia.

- **Interrupción del Servicio Eléctricos Significa Interrupción del Servicio**. Si el servicio eléctrico se interrumpe, los servicios del teléfono Internet se interrumpen por igual, a menos que los teléfonos IP permitan la "tele-alimentación" del propio teléfono (tecnología Inline Power) a través de la línea de datos.

- **Directorio Telefónico.** Si cambia de un servicio telefónico tradicional a un servicio telefónico IP, probablemente su nuevo número no aparecerá en la guía telefónica ni estará disponible para el servicio de asistencia de directorio.

- **Conservando su Número Telefónico Actual.** Los clientes quizás no puedan conservar sus números telefónicos actuales cuando cambian de un servicio telefónico estándar a uno de ToIP.

- **Incompatibilidad de proveedores del servicio.** No todos los sistemas utilizados por los ITSP son compatibles (Gateway, Gatekeeper, Servidores, etc.) entre sí. Este ha sido uno de los motivos que ha impedido que la ToIP se haya extendido con mayor rapidez. Actualmente esto se está corrigiendo, y casi todos los sistemas están basados tanto en el protocolo H.323 como SIP (compatibilidad entre estos).

7.3.7. Futuro de la ToIP.

Internet es la red del futuro y en ella convergen todos los servicios: voz, datos y video. La demanda por la tecnología de redes de conmutación de circuitos ha venido disminuyendo drásticamente. En contraste, las redes basadas en protocolos IP, crecen en forma acelerada. Uno de los factores que estimulan el cambio, es el hecho de que los servicios de ToIP pueden ofrecerse a precios mucho menores. La razón principal reside en la reducción del costo de la transmisión de larga distancia, dado que aquel es en buena medida, independiente de esta.

Dentro el contexto de redes públicas (por ejemplo, Internet), originalmente hace tan solo cuatro años atrás los programas que posibilitaban esta comunicación, como así también las

computadoras multimediales eran una excepción a las ventas masivas. El servicio que se prestaba era defectuoso y con una Qos que no era comparable con la forma tradicional de hablar en tiempo real.

Hoy en día la ToIP, se ha transformado. Términos como calidad, masividad y competencia, se deben en parte a la adopción de IPV6, que es la nueva versión del protocolo Internet que reemplazará de forma progresiva a la versión actual IPV4, responsable de la interconexión de las miles de redes a lo largo de Internet. Y otras estaregias basadas en la adopción de nuevos estándares y protocolos (SIP, IntServ, DiffServ, MPLS, VPNs, etc).

El tráfico de voz, medido en término de conexiones o líneas, crece normalmente en consonancia con el PIB de un país. Las comunicaciones de datos crecen sin embargo, a un ritmo de tres veces mayor para el tráfico de voz, desde la década de los 90. Se estima que para el año 2007 la ToIP representará el 45% (según la firma Analysis) y el 60% (según la firma Tarifica), del total mundial. Actualmente la principal utilización de la ToIP, es para tráfico internacional, no para tráfico local o nacional.

Por otro lado, el futuro de la ToIP también se pinta sin cables. El auge de las redes locales con tecnología WiFi ha dado paso a la ToIP inalámbrica. Hoy, algunos proveedores ya tienen equipos y aplicaciones que permiten a los usuarios disfrutar de las ventajas de la ToIP con la mayor movilidad que brinda Wi-Fi.

En cuanto a la ToIP inalámbrica:

- ✓ Con el comité 802.11 y los jugadores de la industria Wi-Fi trabajando juntos para proveer estándares de calidad de servicio, seguridad mejorada y redes confiables y fáciles de implementar, las aplicaciones de ToIP Inalámbrica están destinadas a prosperar.
- ✓ La disponibilidad y confiabilidad de estas redes en las empresas y en los “hot-spot” públicos ayudarán a abrir el mercado a nuevos dispositivos inalámbricos para voz. Los incrementos en el ancho de banda y las velocidades de transmisión y recepción proveen el medio para nuevas oportunidades para redes listas para múltiples aplicaciones.
- ✓ Los teléfonos IP Inalámbricos ofrecen a los usuarios no solo la misma calidad de voz y facilidades que existen hoy en otras tecnologías inalámbricas, sino que también abren todo un nuevo horizonte de posibilidades para que los usuarios alcancen nuevos niveles de productividad y riqueza de interacción, al aprovechar al máximo la infraestructura convergente a la cuál están conectados.
- ✓ Dispositivos tales como PDAs con conectividad inalámbrica están comenzando a surgir y las aplicaciones de datos y voz diseñadas para estas plataformas ya están disponibles.

- ✓ Teléfonos celulares con capacidad de conectividad dual (por ejemplo, TDMA, CDMA ó GSM + WiFi) han sido ya anunciados por los principales fabricantes de estos dispositivos. Estas nuevas terminales de comunicación móvil, aunadas a actualizaciones en la infraestructura de los proveedores de servicio telefónico celular, serán capaces de entregar al fin la promesa de uniformidad de dispositivo y punto terminal prometida tantas veces antes.
- ✓ Nuevos protocolos de señalización diseñados para manejar este tipo de aplicaciones multimedia, como SIP, permitirán que la transferencia transparente e inmediata de las conversaciones e interacciones de datos entre las redes celulares públicas y las redes WLAN privadas.

El resultado final será que los usuarios tendrán más y mejores opciones para el manejo de sus comunicaciones personales y de negocios, las empresas contarán con sistemas de comunicación unificada, sobre redes convergentes, con aplicaciones que impulsan la productividad, reducen los costos y proveen ventajas competitivas sostenibles.

Dentro de este contexto, Cisco es el único fabricante del mercado que puede entregar una solución de ToIP inalámbrica de punta a punta. Cisco es pionero en la integración de las redes alámbricas e inalámbricas con la introducción de su portafolio de Red Estructurada Inalámbrica (Structured Wireless-Aware Network), extendiendo su liderazgo en la infraestructura de Redes de LAN, a la WLAN.

8. CAPITULO VIII. ANÁLISIS DE LA REGULACIÓN.

Esta ponencia presenta las principales implicaciones regulatorias asociadas al desarrollo de la ToIP, en un momento en que ésta se hace realidad y puede adquirir una importancia decisiva, particularmente si se considera su relación con el despliegue de la banda ancha.

8.1. INTRODUCCIÓN.

A pesar de que la ToIP todavía se encuentre en una etapa de desarrollo, es posible señalar que existe un mercado que se verá afectado con la implementación de estas nuevas técnicas. Es así como el servicio de voz por Internet podría ocasionar grandes pérdidas a las compañías telefónicas convencionales, las cuales piden a gritos un sistema que regule el servicio.

La ToIP presenta un gran desafió al actual modelo de negocios de los operadores de telecomunicaciones, los proveedores de servicios y los vendedores están ingresando al mercado de la ToIP a una taza extraordinaria Los bajos costos y el estado de **"no regulación"** de este mercado significan que nuevos competidores cuentan con una herramienta competitiva muy poderosa

El diferencial de precios actual a favor de la ToIP permitirá a los nuevos operadores de telecomunicaciones con servicios mejorados en la plataforma IP integrada del futuro. Los operadores de telecomunicaciones deben tomar este desafió muy seriamente.

Actualmente existen diferentes posiciones en cuanto a las necesidades de introducir un marco regulatorio a los nuevos servicios relacionados a la ToIP. Por una parte, algunos son de la opinión de que es prematuro regular servicios que aún no cuentan con la madurez y presencia en el mercado como para poder sobrevivir a medidas reguladoras y de control.

Por otro lado, la experiencia dicta que en la introducción de nuevos servicios en el mercado suele ser mucho más sencilla en aquellos países en los que existe un mercado estable en lo que se refiere a leyes de competencia y medidas de protección al usuario, sin embargo, en aquellos otros en los que el mercado es dominado por un monopolio o por la presencia de un operador incumbente, que domine y restringa el acceso a usuarios finales y la interconexión a redes internacionales; el marco regulatorio debe facilitar la entrada y supervivencia de los nuevos servicios y proveedores.

Aunque aún no está clara la necesidad de intervenir mediante medidas reguladoras, lo que si no cabe a dudas es la consideración ineludible de aspectos implícitos en los servicios de telefonía tradicional y que deben ser extrapolados de cierta manera a los nuevos servicios de ToIP:

- ✓ Garantizar la calidad de los servicios de voz, en términos de calidad de transmisión de la voz, clara información y aplicación de precios y tarifas,
- ✓ Asegurar el acceso permanente a llamadas de emergencia, incluyendo provisión a información de localización del número llamante,
- ✓ Publicación de información relativa del suscriptor del servicio en directorios públicos,
- ✓ Portabilidad de números y direcciones,
- ✓ Acceso a la red para asuntos de seguridad nacional y policial,
- ✓ Legislar y garantizar la protección en la transmisión de voz y datos

Sin embargo, existen ciertos factores que dificultan la definición de un marco regulatorio:

- Existen aún muy pocas leyes en relación a las redes IP,
- Existe una gran variedad de servicios relacionados a la ToIP,
- Tecnológicamente no es fácil aún garantizar la calidad del servicio,
- Los rápidos cambios tecnológicos y de mercado dejan sin validez cualquier iniciativa reguladora,
- Dificultades aún existentes con respecto a la interconexión a redes internacionales.

En ciertos países los gobiernos han definido los servicios de ToIP de tal modo que permiten el suministro de este servicio al público, pese a la exclusividad comercial del operador principal en lo que concierne a la telefonía vocal básica. En otras naciones estos servicios se han prohibido, mientras que en otras quedan sujetos a licencia y se promueven.

Dado que las llamadas telefónicas IP se cursan principalmente fuera de la PSTN y, por consiguiente, fuera de las estructuras reglamentarias y financieras que se han desarrollado alrededor de dicha red, se dice que la ToIP y su posible uso a través de la red Internet no sólo puede socavar las fuentes de ingresos de los principales operadores comerciales de los países en desarrollo, sino también los programas de servicio universal encaminados a extender los servicios y redes a zonas no atendidas o poco atendidas. En otros países se considera que la ToIP y, particularmente, el despliegue de redes IP es una forma de ofrecer así como de estimular servicios nuevos y más baratos y, por ende, de presionar a la baja los precios de la telefonía cursada a través de circuitos conmutados

8.2. ANÁLISIS DE LA NORMATIVA EN CHILE.

8.2.1. Telefonía Tradicional (Local, Móvil y Larga Distancia).

La regulación de la telefonía tradicional tiene su origen en la Ley General de Telecomunicaciones (LGT), establecida por la Subsecretaría de Telecomunicaciones (Subtel), que reconoce específicamente al servicio público telefónico, formado a su vez por el servicio telefónico local, el servicio telefónico de larga distancia y el servicio telefónico móvil.

La LGT (articulo 8) señala que la instalación, operación y explotación de servicios públicos de telecomunicaciones (telefonía local y telefonía móvil) y de servicios intermedios de telecomunicaciones (telefonía de larga distancia) requiere de concesión otorgada por decreto supremo. Asimismo, el artículo 25 de la LGT señala que será obligación de los concesionarios de servicios públicos de telecomunicaciones y de los concesionarios de servicios intermedios prestar servicio telefónico de larga distancia, establecer y aceptar interconexiones según las normas técnicas, procedimientos y plazos que ha establecido Subtel.

De acuerdo a la LGT el "**servicio telefónico local"** está afecto además a regulación técnica, ya que los concesionarios de este servicio deben cumplir, por ejemplo, con todos los planes técnicos fundamentales vigentes (numeración encaminamiento, transmisión y señalización), con las disposiciones relativas al sistema multiportador de larga distancia (que prohíben que un concesionario de servicio telefónico local curse tráfico entre zonas primarias o con el extranjero) y con el Reglamento del Servicio Público Telefónico (que entre otras obligaciones exige la edición de la guía telefónica, reglamenta la factura única, etc.). La LGT también considera que, en caso que no haya suficientes condiciones de competencia, el servicio telefónico local estará afecto a regulación tarifaría, lo que esencialmente se aplica, por ejemplo, a CTC y Telefónica del Sur, que tienen fijadas sus tarifas a público en las zonas donde son dominantes. Asimismo, para todas las empresas .dominantes o no. se regulan sus tarifas de interconexión.

La LGT somete a cierta regulación técnica al "**servicio telefónico móvil"**, ya que los concesionarios de este servicio deben cumplir determinadas partes de los planes técnicos fundamentales vigentes que les son aplicables, con las disposiciones relativas al sistema multiportador (pero sólo para las llamadas internacionales) y con las disposiciones aplicables del Reglamento del Servicio Público Telefónico. En el ámbito tarifario el servicio telefónico móvil está exento de regulación, ya que la LGT dispone expresamente que las tarifas a público de este servicio son libres, y sólo se regulan sus tarifas de interconexión.

La LGT también somete a cierta regulación técnica y tarifaría al "**servicio telefónico de larga distancia"**, pero en la práctica éste se encuentra hoy prácticamente libre de restricciones.

Es muy importante observar que a LGT no contempló expresamente la existencia de servicios como Internet o ToIP.

8.2.2. Internet.

La red Internet no pertenece a ninguna empresa o entidad específica, sino que está formada por la suma de todos los elementos que la integran (computadores, enlaces, ISPs, redes de acceso, etc.). No obstante, sus principales protocolos y normas son establecidos por el IETF, que es una organización sin fines de lucro conformada por los usuarios interesados en el desarrollo de Internet.

Por tanto, el "**servicio Internet"** se ha considerado en casi todo el mundo, como un servicio no regulado. En el caso de Chile, si hubiese que dar sustento legal esa consideración, existe una inclinación mayorista, por aceptar que el servicio Internet que proveen los ISP es un servicio complementario, ya que por disposición del artículo 8 de la LGT quedaría exento de regulación tarifaría y además podría quedar exento de regulación técnica.

En efecto, si bien el artículo 8 de la LGT señala que la instalación, operación y explotación de servicios públicos de telecomunicaciones requiere de concesión, el mismo artículo señala que las empresas concesionarias de servicios públicos de telecomunicaciones o terceros, podrán dar prestaciones o servicios complementarios por medio de las redes públicas, a lo cual agrega que la instalación y explotación de los equipos para proveer servicios complementarios no requiere de concesión o permiso, y que la prestación o comercialización de los mismos no estará condicionada a anuencia previa alguna de las empresas concesionarias, ni a exigencias o autorizaciones de organismos o servicios públicos.

8.2.3. ToIP sobre banda ancha.

Los cambios tecnológicos permiten prestar servicios telefónicos de voz utilizando las conexiones de banda ancha. Para ello el usuario debe contar con una conexión con un proveedor de Internet, ya sea a través del par de cobre de una línea de teléfono local o bien un cable coaxial. Es por esto que el regulador chileno "Subtel" o "Subsecretaría de Telecomunicaciones" pensó normar el servicio de voz sobre banda ancha. Un nuevo reglamento hubiera definido una concesión de "servicio público de telecomunicaciones de voz sobre banda ancha" (SPTVBA), la que hubiera permitido interconectar a empresas de ToIP sobre banda ancha con las redes telefónicas públicas.

Generalmente, se suele pensar que su introducción sólo trae beneficios, principalmente por una competencia más intensa y porque se trata de progreso tecnológico. De lo cual varios operadores de telefonía tradicional, piensan que esta conclusión debe matizarse. Una razón es que la voz sobre banda ancha sigue usando la red de acceso de la telefonía tradicional; en realidad sólo sustituye a la conmutación y transmisión. También es cierto que para prestar servicios de ToIP sobre banda ancha es necesario invertir en equipos. Por último, la migración de clientes y tráfico hacia la ToIP sobre banda ancha aumenta los costos medios de las empresas telefónicas tradicionales y, con ello, las tarifas que las autofinancian. Así, y aunque esto no forma parte de una evaluación social, a los efectos de eficiencia se les deben agregar otros distributivos: ganan aquellos clientes que emigran a la telefonía IP sobre banda ancha, y pierden quienes permanecen en la compañía tradicional.

Supone, por tanto, y valga la redundancia, que la ToIP se presta mediante una conexión de banda ancha. Así, la voz del usuario se paquetiza en su hogar, se envía por la red de datos tal como un correo electrónico o una conexión con una página Web, y el proveedor del servicio de banda ancha la entrega en el ISP del proveedor de ToIP. Más aún, el proveedor de ToIP no instala electrónica entre el adaptador telefónico en la casa del usuario (el aparato que transforma la voz en paquetes) y su ISP de ToIP. Estos son los servicios que Subtel quiere normar por medio de las concesiones de SPTVBA.

8.2.4. Intentos por establecer un marco regulatorio.

8.2.4.1. Documento de consulta.

El proceso de convergencia entre las telecomunicaciones y la informática ha dejado de ser una visión futurista para instalarse como una realidad que impone desafíos a todo nivel en el ordenamiento sectorial.

La Subtel en el mes de agosto de 2004, somete a consulta pública un documento para el establecimiento de la normativa que regule los servicios de voz sobre el protocolo IP, en concordancia con los objetivos de competencia, uso eficiente de redes, desarrollo de nuevos servicios a los usuarios y aprovechamiento de las nuevas tecnologías para el desarrollo del sector de telecomunicaciones.

Se elaboró dicho documento de trabajo con el objetivo de definir un instrumento normativo que permita la introducción de esta tecnología, sin causar inestabilidades regulatorias, de manera que los usuarios finales puedan disponer de más y mejores servicios.

El alcance de este documento era únicamente para fines de consulta a los distintos actores del mercado chileno, estableciéndose en ningún caso como un documento oficial. El cual cita los siguientes aspectos:

- La regulación de la ToIP, debe responder a ciertos "**principios"**:
  - **Regulación de servicios;** debe maximizar el bienestar de la sociedad en términos de QoS, precio y cobertura.
  - **Neutralidad tecnológica;** transparencia de la regulación, no favoreciendo un tipo de tecnología por sobre otro.
  - **No discriminación;** la prestación de servicios debe ser equivalente.
  - **Beneficio y protección del consumidor;** deben establecerse garantías mínimas para el resguardo de los consumidores respecto de las empresas.
  - **Apertura a la innovación y la inversión;** debe establecer las condiciones adecuadas para permitir la innovación, el cambio tecnológico, etc.
  - **Mínimo necesario;** debe orientarse a corregir problemas o asimetrías presentes en el mercado, procurando generar las mínimas distorsiones.
  - **Apertura a la inversión;** debe facilitar el desarrollo de proyectos que generen grandes ingresos para el país.

- Como así también con el objeto de evaluar las distintas regulaciones que se pueden implementar para los servicios de ToIP, se citan los aspectos que definen la **"naturaleza de los servicios"**, como: la ubicación geográfica, los medios de accesos (físicos e inalámbricos), interconexión con la red publica telefónica (y/o otros servicios de VoIP), numeración y calidad.

- Se hace necesario, a objeto de la definición de la política regulatoria, distinguir las **"distintas tipologías"** de los servicios de VoIP. Esta diferenciación se obtiene del hecho de que Internet puede llegar a los usuarios utilizando cualquier tipo de infraestructura de red (por ejemplo: telefonía fija y/o móvil). Diferenciándose las siguientes tipologías: Servicio Web Unidireccional (comunicaciones PC a PC en Internet o de PC hacia la red telefónica pública), Servicio Privado y/o restringido (comunicaciones de voz en un grupo cerrado de usuarios a través de redes privadas físicas o virtuales) y el Servicio Público de Telecomunicaciones de

Voz (aquellas que se ofrecen a la comunidad en general, ya sea a través de teléfonos IP o tradicionales).

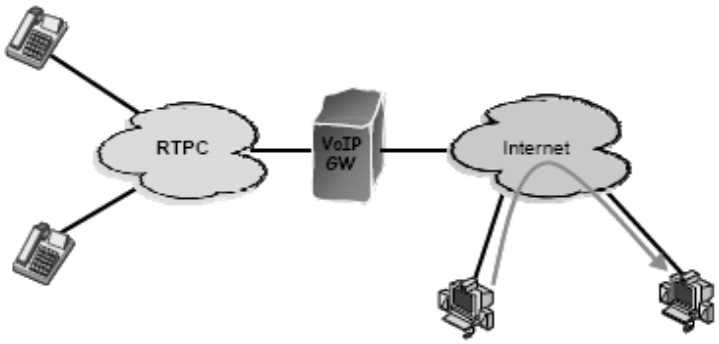
- Se evidencia una **"propuesta de política"**, que establece la regulación a cada modalidad de comunicación VoIP.

- En particular, para los servicios públicos de servicios de telecomunicaciones sobre Banda Ancha (BA) o IP se propone que dispongan de una **"concesión de servicio"** publico: concesión de "Servicio Publico Telefónico Local" (SPTL), que corresponde al servicio de telefonía a través de redes IP dedicada (no Internet), o bien, concesión de "Servicio Publico de Telecomunicaciones de Voz sobre Banda Ancha" (SPTVBA), que permite la prestación de comunicaciones de voz sobre banda ancha (Internet).

8.2.4.2. Análisis de las modalidades planteadas por la Subtel.

En su documento, Subtel considera que en el fondo existen cuatro modalidades para prestar Servicios de VoIP:

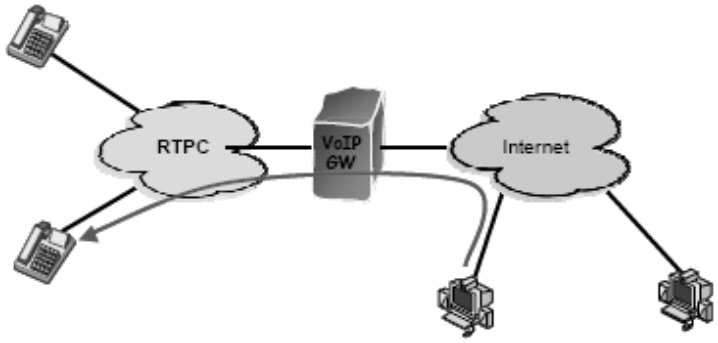
i. La primera consiste en aprovechar la infraestructura de Internet para transmitir señales de voz y establecer comunicaciones telefónicas entre dos o más computadores conectados a Internet:



Servicio privado y/o restringido.

El documento de Subtel denomina: **"Servicio privado y/o restringido"** a esta modalidad y propone dejarla sin regulaciones.

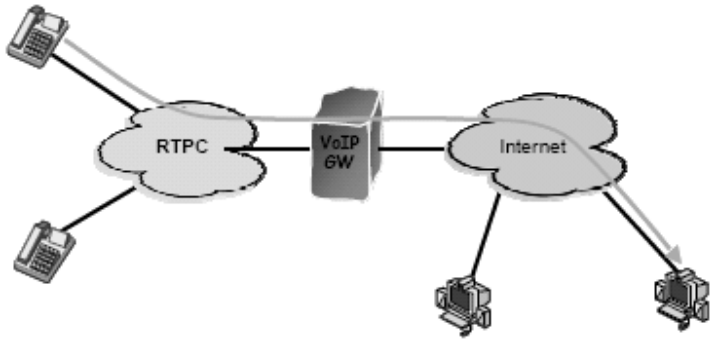
ii. La segunda modalidad consiste en aprovechar la infraestructura de Internet para transmitir señales de voz y establecer comunicaciones telefónicas originadas en un computador conectado a Internet y terminadas en la Red Telefónica Pública Conmutada (RTPC), pero no así comunicaciones en sentido inverso.



Servicio Web unidireccional.

El documento de Subtel denomina: "**Servicio Web unidireccional"** a esta modalidad y también propone dejarla sin regulaciones.

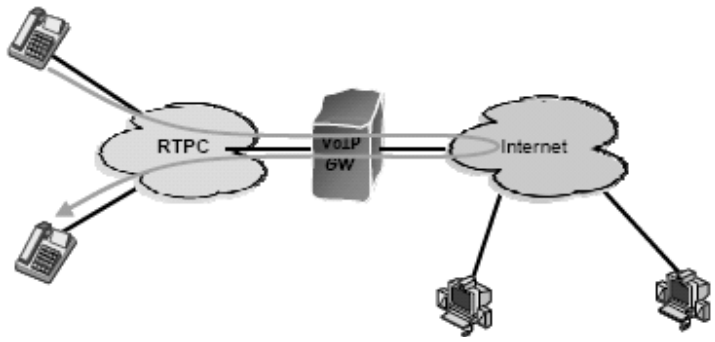
iii. La tercera modalidad consiste en aprovechar la infraestructura de Internet para transmitir señales de voz y establecer comunicaciones telefónicas en sentido inverso, es decir, originadas en la RTPC y terminadas en un computador conectado a Internet:



Servicio con separación red física-lógica IP.

El documento de Subtel denomina: **"Servicio con separación red física-lógica IP"** a esta modalidad y propone dejarla sujeta a una regulación específica, consistente en la obtención de una Concesión de Servicio Público de Telecomunicaciones de Voz sobre Banda Ancha (SPTVBA) y el cumplimiento de ciertas normas técnicas a dictarse en el futuro, y

iv. La cuarta modalidad, consiste en que los operadores de las instalaciones telefónicas tradicionales puedan sustituir a voluntad los protocolos de conmutación TDM por el protocolo IP, renovando así .sólo desde el punto de vista tecnológico la forma de prestar el servicio telefónico tradicional.



Servicio con integración red física-lógica IP

El documento de Subtel denomina: **"Servicio con integración red física-lógica IP"** a esta modalidad y propone dejarla sujeta a la misma regulación que hoy afecta a la telefonía fija, es decir, la obtención de una Concesión de Servicio Público Telefónico y el cumplimiento de la normas vigentes, como es la división del país en 24 zonas primarias y la prohibición de establecer comunicaciones entre zonas primarias o con el extranjero, que sólo pueden cursarse a través de los actuales operadores de servicio intermedio.

Hay que destacar que, las empresas concesionarias no podrán ejecutar acto alguno que implique discriminación o alteración a una sana y debida competencia entre todos aquellos concesionarios o terceros sin concesiones que proporcionen servicios complementarios.

Además es necesario mencionar que cuando los servicios de telecomunicaciones se entregan en competencia, no se regula la calidad de servicio, ya que los consumidores pueden escoger la combinación "precio-calidad de servicio" que mejor se adapta a sus necesidades.

8.2.4.3. Síntesis de algunas opiniones vertidas por empresas y operadores de servicios de telecomunicaciones.

Los comentarios manifestados en el proceso de consulta pública respecto de la conveniencia e inconveniencia de la propuesta de "Marco Normativo de los Servicios de VoIP" son diversos y, en general, para las empresas involucradas en la prestación de servicios reflejan su visión particular de como les resulta de mayor conveniencia que se dé el desarrollo de la industria de telecomunicaciones. Los comentarios enviados por los diferentes actores apuntan a aspectos de carácter técnico, jurídico, y económico donde, empresas de telefonía fija se muestran contrarias a una desagregación de sus redes, las empresas de telefonía móvil no apoyan entusiastamente la propuesta de crear los MVNO (Mobile Virtual Network Operator o Operador Móvil de Red Virtual), la empresas de servicios de LD (Larga Distancia) se oponen a la desagregación de su segmento aún cuando ésta es limitada, las empresas de Cable plantean que en telefonía fija la desagregación de redes sólo se debe aplicar al operador dominante y no rechazan la desagregación de la telefonía móvil, y por último los ISP si se muestran favorables al Marco Normativo contribuyendo con antecedentes que apuntan a mayores precisiones del documento presentado.

A la consulta realizada por SUBTEL en el mes de diciembre de 2004, parte de los que enviaron comentarios son:

ALCATEL	HEILSNBERG S.A.
AT&T	IFX Networks
BellSout	INALAMBRICA S.A.
BSTeam	INTELZET
BT Global Net	Manquehue Net S.A.
CHILE SERVICE	Metrópolis Intercom S.A.
CMET	Netline Comunicaciones S.A.
Colegio de Ingenieros de Chile A.G.	Regulación y Mercado
CONADECUS	Smartcom S.A.
Entel Telefonía Móvil S.A.	Telefónica CTC
Entel PCS Telecomunicaciones S.A.	Telefónica Móvil de Chile
Entel S.A.	Telmex
ETSE S.A.	Telefónica del Sur S.A.
Global Croossing	VOISSNET
GTD	VTR Banda Ancha S.A.

Ciertamente parece necesario y conveniente que se regule la prestación de los servicios de voz sobre protocolo IP, fundamentalmente en lo que dice relación con la interconexión y las condiciones

de igualdad respecto a los concesionarios de la red pública de telecomunicaciones, para fomentar el desarrollo de una sana competencia y por tanto de la industria.

Al día de hoy el proceso esta siguiendo su tramitación, y la Subtel esta analizando los extensos documentos legales, técnicos y financieros presentados.

8.3. REGULACIÓN INTERNACIONAL.

A nivel mundial, aun no hay una definición en como regular al emplear esta nueva tecnología. Algunos reguladores la han prohibido, ya sea explícita o implícitamente, otros la permiten e incluso fomentan, pero la mayoría todavía no han abordado oficialmente el tema.

En algunos países se distingue la regulación sobre la base de:

- tipo de servicio y/o equipo terminal empleado;
- el modo de transmisión de la red;
- la calidad del servicio;
- si es voz o datos; entre otras formas.

En la actualidad países como Argentina, Australia, Canadá, Colombia, Chile, España, Estados Unidos, Perú, Reino Unido, Singapur y ahora México, realizan diversos estudios, consultas y análisis de posicionamiento inicial respecto al tratamiento regulatorio que darán a la Voz por IP en sus respectivas jurisdicciones.

Examinando, a continuación algunos de los distintos planteamientos:

- **PERÚ**. La ToIP está permitida en un marco de libre competencia y no regulación de precios, basados en la premisa de que se trata de un servicio de valor agregado definido en un entorno de libre competencia y sobre el cual el ente regulador OSIPTEL (Organismo Supervisor de Inversión Privada en Telecomunicaciones) no puede ejercer regulación de precios.

- **ARGENTINA.** Según el organismo regulador CNC (Comunicación Nacional de Comunicaciones), la prestación del servicio de ToIP se encuentra no reglamentada (no está tipificada como servicio en sí mismo), actualmente no existe un plan o estrategia gubernamental para el desarrollo de la ToIP.

- **MÉXICO.** La ToIP todavía no cuenta con una regulación específica que permita su prestación de una manera lícita y en condiciones de competencia respecto a los

concesionarios. La Comisión Federal de Telecomunicaciones (COFETEL) se encuentra analizando la ToIP para establecer la regulación específica, de conformidad con lo previsto en las disposiciones legales, reglamentarias y administrativas aplicables al servicio de telefonía.

- **BRASIL.** La prestación de servicios de voz utilizando el protocolo IP es permitida siempre y cuando se cuente con una concesión, permiso o autorización por parte de ANATEL (Agencia Nacional de Telecomunicaciones). La reglamentación es basada en servicios y no en tecnología. El asunto de ToIP se encuentra en estudio.

- **CANADÁ.** Se permite el uso de la ToIP, el marco regulatorio establece la no regulación de Internet. En cuanto a la ToIP, en mayo de 1997 la entidad regulatoria, CRTC (Canadian Radio-Television and Telecommunications Commission), estableció que los sistemas de ToIP que generan llamadas Teléfono a Teléfono eran susceptibles de pagar contribuciones por cada minuto causado, esta política fue confirmada e implementada en enero de 1998. Luego de esto se reguló que las llamadas PC a PC y PC a teléfono no eran candidatas a pagar contribuciones. De lo anterior se deduce que el régimen se basa en la naturaleza de la terminal utilizada para originar la llamada y por ende de cómo se causa el tránsito de la comunicación a través de la red, determinando que si es originada en la RTPBC y a través de cualquier dispositivo de hardware enrutada a través de Internet, se sigue considerando como telefonía convencional.

Y en otros como:

- **ECUADOR.** CONATEL (Consejo Nacional de Telecomunicaciones), ha resuelto definir a la ToIP como una aplicación tecnológica disponible en Internet. La decisión se tomó luego de analizar técnica y jurídicamente las características, modalidades e implicaciones de la VoIP en el Ecuador. Cuando la voz en forma de paquetes viaje a través de la Internet no será regulada, ya que esta es una red de redes mundial, en la cual ningún regulador ha intervenido. Según el documento, tanto los proveedores de Internet, los cibercafés o cualquier persona natural o jurídica, podrán comercializar planes para el uso de la VoIP. Sin embargo, cuando un operador de telecomunicaciones, como Andinatel, Pacifictel o Etapa, entre otros, preste el servicio de telefonía utilizando el protocolo IP, esa telefónica "estará sujeta al marco legal, las normas de regulación y control aplicables".

- **CHINA.** La ToIP está permitida a través de proveedores autorizados. Inicialmente se tenía un marco regulatorio por medio del cual se prohibía la prestación de estos servicios, sin embargo, este marco cambio a raíz de una decisión judicial, la cual implicaba a los propietarios de un café Internet en donde se prestaba el servicio de ToIP; estos fueron arrestados y sus equipos confiscados. Al final los propietarios del café terminaron ganando en segunda instancia la demanda que entablaron contra el ente regulador, provocando un cambio radical de la política, hasta tal punto en que la China se propuso como política de Estado incentivar la ToIP e invertir capital en I+D, con el fin de desarrollar el estándar chino de ToIP a la mayor brevedad ya que se encuentran convencidos de la posibilidad de reemplazar la telefonía convencional por completo.

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

- "se trata de telecomunicaciones o transmisión de datos", (aquí esta determinación implica si paga impuestos o no y qué tipo de licencias se requieren para prestar el servicio).

El tipo de regulación que se necesita tiene que estar acorde con el mercado, con las necesidades de los usuarios y con el desarrollo tecnológico.

9. CAPITULO IX. CONCLUSIONES.

La Telefonía IP (ToIP) queda definida como la transmisión de voz mediante el protocolo IP, en interconexión con la red publica telefónica conmutada (PSTN), a través de un gateways. De ésta manera, gracias a extensas recomendaciones o protocolos como, UIT-T H.323 y otras propuestas más actualizadas como, SIP de la IETF es posible la transmisión de voz en paquetes de datos. Y paralelamente el despliegue de distintas posibilidades para prestar QoS a través de redes IP, entre las que figuran RSVP, DiffServ, MPLS y la versión 6 de IP (IPv6), han permitido la transmisión de voz (y video) en tiempo real, mejorando la eficiencia en el ancho de banda.

Las aplicaciones, como ya se mencionó, de la ToIP son ilimitadas y apenas se empiezan a implementar, en contraste con las aplicaciones de la PSTN que llegan a su tope tecnológico. La ToIP, entre otras ventajas importantes en redes locales como reducción de tiempo y costos en relación a la transmisión de voz estándar especialmente en el caso de empresas con tráfico de voz internacional, está ampliando perceptiblemente la gama de los servicios para los usuarios y está abriendo nuevos mercados.

A pesar que la PSTN ya ofrece un QoS de alto nivel, hoy en día los nuevos estándares de ToIP proveen la posibilidad de alcanzar los mismos niveles, y la posibilidad de mejorarlos, respecto a rutas alternas, mejores técnicas de compresión, entre otras. Dadas estas características, la ToIP es considerada como el futuro de la telefonía, estableciendo un futuro incierto en cuanto a la existencia de la PSTN.

Uno de los principales factores que pueden convencer de la conveniencia de implantar ToIP, especialmente en el caso de empresas con tráfico de voz internacional, es el ahorro de costos asociados a las tarifas de los operadores. Pero aquí el nivel de calidad de la voz, perjudicado por la latencia, si el ancho de banda no es el adecuado, constituye un importante escollo. En este punto es importante tener en cuenta que el resultado de la calidad de la voz en redes IP es muy distinta en el caso de una red publica, como Internet, o una red privada, trátese de una Intranet, LAN o WAN.

Fuera de la WAN, garantizar la QoS requerida por las aplicaciones de voz, sigue siendo un problema en la Internet pública, donde los proveedores de servicios son incapaces de controlar la infraestructura de extremo a extremo. En este ámbito no veremos voz con calidad telefónica en toda la extensión de la Internet pública, hasta que la totalidad de la infraestructura de los operadores, haya sido actualizada a la próxima versión del protocolo IP, IPv6.

El problema es que el protocolo IP actual (IPv4) es ya un protocolo muy sobrecargado, de tal forma que su propio enrutado genera demasiada latencia, u mucho más sobre Internet. La solución ideal para la ToIP es que se soporte sobre IPv6 y en redes especificas de comunicaciones por voz, de tal forma que se consiga toda la versatibilidad del protocolo y toda la calidad diferenciadora de los operadores.

Desde luego, en la "Internet privada", que puede crearse mediante la contratación de servicios de redes privadas virtuales (VPN), la situación es diferente. Los proveedores de servicios están preparados para ajustar las redes troncales, y asegurar los niveles QoS requeridos por el cliente. En la LAN no hay problema, dado que las empresas tienen el control absoluto de extremo a extremo y pueden ampliar el ancho de banda.

Así como también, dado que las comunicaciones de voz transitan a través de varios ISP para llegar al destino, y si una de las redes del ISP encargadas de proporcionar la comunicación confiere a su parte de la red una QoS inferior a la ofrecida por otras redes, la QoS del flujo se verá reducida en consecuencia. En este contexto mientras no se adopten los modelos combinados RSVP e InterServ en ambientes LAN y DiffServ en entornos WAN no se podrá garantizar la Qos extremo a extremo.

Por otro lado, ante todo lo expuesto hasta ahora, no debería haber ninguna discusión a la hora de decidir que "protocolo de gestión de sesión" adoptar en telefonía IP. Todo el mundo coincide en afirmar que el futuro está en SIP de la IETF. Este diseño de un agente de usuario SIP supone una forma fiable de intercomunicar a personas a través de una red, independientemente de su localización actual, con una calidad de audio muy aceptable y con unos requerimientos de ancho de banda mínimos.

Hay que tener en cuenta que algunos fabricantes ya han realizado inversiones en el desarrollo y fabricación de equipos de acuerdo a las especificaciones de UIT-T H.323, lo cual hace pensar que esta migración hacia SIP será gradual, puesto que los proveedores no se van ha decidir a cambiar hasta no ofrezca un nivel de madurez y flexibilidad aceptable. Así pues, en principio coexistirán los dos protocolos, por lo que es imprescindible garantizar el interfuncionamiento entre ambos.

En lo que respecta a la regulación de la ToIP aún quedan muchas dudas por despejar, sin embargo, lo que si está claro es que tanto los operadores que pretendan ofrecer estos nuevos servicios, así como los posibles usuarios (bien sean residenciales o corporativos); necesitan la garantía de poder desplegar infraestructura, participar y competir en el mercado, así como de disponer de servicios con garantías y calidad de suficientes. Cada país debe tener en cuenta la realidad del mercado local y tomar las medidas necesarias en pro de la evolución tecnológica y por ende del bienestar y calidad de vida de sus habitantes, aunque la coordinación a nivel internacional, tendrá un papel de suma importancia. Y por ultimo,

Actualmente, la comunicación de voz, faz y video a través de la red IP, de manera económica y efectiva, es un hecho, por lo que es importante que las empresas utilicen las posibilidades que les ofrece la red IP para incrementar la productividad y competitividad. Lo más importante es, desde el punto de vista de los usuarios, la configuración más adecuada de los equipos a utilizar, y desde el punto de vista del proveedor de red, la sobreventa adecuada de los servicios y el análisis permanente del comportamiento de la red, de forma tal de poder ofrecer estos servicios a los usuarios de forma económica y efectiva, y que a su vez permita aumentar la competitividad de la empresa como proveedor de servicios, tratando a su vez de maximizar las ganancias.

REFERENCIA BIBLIOGRAFICA.

Textos:

- William Stallings. “High Speed Networks. TCP/IP and ATM Design Principles”, Vol. I. Prentice Hall, 2001.
- Douglas E. Comer. “Internetworking with TCP/IP. Vol. I: Principles, Protocols and Architecture”. Cuarta Edición. Prentice-Hall, USA.2002.
- O. Hersent. “IP Telephony: Packet-Based Multimedia Communications Systems”, Vol. I. Primera Edición. Addison-Wesley, 1999.
- O Hersent. “IP Telephony: Deploying Voice-over-IP Protocols”, Vol. I. Segunda Edición. 2004

Revistas:

- R. Fischer y P. Serra, Evaluación de regulación de las telecomunicaciones en Chile, Revista Perspectivas de Política, Economía y Gestión, 2005.
- D. Bradner, La evolución en los sistemas de comunicaciones telefónicas en Chile, Revista Consideraciones, Técnicas, Legales y Comerciales, 2006.

Sitios Web:

- E.Perez. Modulo Oirs. Subtel, Subsecretaría de Telecomunicaciones. Procesos regulatorios de comunicaciones de Voz sobre redes IP: http://www.subtel.cl/
- Rango de servicios avanzados de telecomunicaciones – Empresa Telmex de Chile http://www.telmex.cl/
- Fundamentos de Telefonía sobre IP - Cisco Systems: http://www.cisco.com/
- Actualidades de la ITU / Internacional Telecommunication Union, Regulación de las Telecomunicaciones a nivel Internacional: http://www.itu.int/home/index.html y de la IETF Internet Engineering Task Force, Normalización Internacional: http://www.ietf.org/
- Y otras direcciones asociadas. Buscador en la Web, Google. Palabras claves “IP Telephony“ and “Quality of Service”: www.google.com

ANEXO. EQUIPOS Y SOLUCIONES TECNOLÓGICAS

ATA – Adaptador Telefónico Analógico, equipos ATA Cisco modelo 186

El equipo Cisco ATA modelo 186 es un dispositivo basado en estándares de comunicación que entregan exactas, terminales de próxima generación VoIP a negocios y residencias por todo el mundo.

Este modulo de fax / voz, se conecta a un enlace de Internet (Ethernet, Fast Ethernet - 100 Mbps) de banda ancha de por lo menos 256 Kbps. En cada ATA se pueden utilizar hasta 2 líneas telefónicas.

Datos característicos:

- Dos puertos (“Phone 1” y “Phone 2”) que permiten conectar hasta 2 líneas telefónicas independientes:
  - A estas líneas se conectan teléfonos analógicos estándar (conector RJ11).
  - Si se contrata solo una línea hay que conectarla al puerto “Phone 1”
  - Cada línea utiliza 80 Kbps del enlace a Internet cuando está en uso.
- Un puerto Ethernet denominado “10BaseT”, que se conecta al enlace a Internet

  - En el modelo ATA186, de 2 puertos Ethernet, el puerto denominado “UPLINK” es el que se conecta al enlace de internet,
- Un puerto donde se conecta el adaptador que a su vez se conecta a la corriente eléctrica.
- Soporta los siguientes protocolos.
  - Protocolos de señalización digital: MGCP, H.323v2, H.323v4, SIP.
  - Protocolos de compresión de datos: G.729, G.711, G.723.1, G.729A, G.729B, G.729AB.
- Cancelación de eco de línea.
  - Cancelación de eco para cada puerto.
  - Longitud del eco de 8 ms.
  - Supresión no lineal del eco (ERL mayor que 28 dB para f = 300 a 3400 hertzios).
  - Tiempo de la convergencia = ms 250.
  - ERLE = 10 a 20 dB.
  - Doble-talk la detección.
- Características de voz.
  - Detector de actividad de voz (VAD).
  - Generador de ruido confortable (CNG).
  - Jitter buffer dinámico (adaptante).
- Fax.
  - Paso de fax G.711.
  - Modo de fax G.711.
- Dimensiones (ancho x profundidad x altura): 16,5 cm x 14,6 cm x 3,8 cm.

Rentable

Los Cisco ATA 186 ayudan a los clientes a convertir sus dispositivos análogos de teléfono en los dispositivos IP rentable y son la solución preferida para tratar las necesidades de los clientes que conectan con las redes de la empresa, ambientes de pequeña oficina, o la emergente administración VoIP de servicios de voz que emerge y mercado local de servicios.

Valor comercial

  - Su precio en el mercado es US$ 140, 6 (equivalente aprox. a $ 76.000 pesos).

TELEFONO IP DE CISCO 7905G Y 7912G

Los teléfonos IP de Cisco mantienen un claro liderazgo del mercado en una verdadera voz a través de IP, ya que ofrecen una completa cartera de teléfonos IP atractiva y con un estilo distintivo para grandes empresas y pymes. Al proporcionar acceso basado en visualización a los servicios y las aplicaciones, los teléfonos IP de Cisco permiten la personalización, integración y acceso a Web, ya que conectan los procesos y las personas a la información más crítica.

Los productos de los teléfonos IP de Cisco incluyen una interfaz de switches Ethernet de dos puertos que permite a los administradores de red gestionar la calidad de la voz asignando prioridad a los datos de red de la voz sobre otros tipos de datos de red y soporte para la alimentación en línea a través de Ethernet. Proporcionan operaciones seguras y eficaces, y las características necesarias para mejorar la productividad y las comunicaciones empresariales

Características

- Teléfono básico para empresas
- Pantalla de píxeles
- Una sola línea
- Cuatro "teclas programables" dinámicas
- El teléfono IP cisco 7912G tiene un switch Ethernet integrado

Teléfono IP Cisco 7905G

El teléfono IP Cisco 7905G proporciona acceso con una sola línea y cuatro teclas programables interactivas que guían al usuario a través de las características y funciones de las llamadas, empleando para ello la pantalla LCD basada en píxeles. Los usuarios agradecen la capacidad gráfica de la pantalla, ya que en las versiones futuras del firmware presentará la información de las llamadas, un acceso intuitivo a las características y elección del idioma.

El teléfono IP Cisco 7905G admite la alimentación en línea, lo que permite al teléfono recibir su alimentación a través de la LAN. Esta capacidad proporciona al administrador de redes un control centralizado sobre la alimentación, lo que se traduce en una mayor disponibilidad de la red. El teléfono IP Cisco 7905G es compatible con Cisco CallManager Express, versión 3.0 y posteriores.

Valor comercial.

- Su precio en el mercado es US$ 187, 6 (equivalente aprox. a $ 102.000 pesos).

Teléfono IP Cisco 7912G

El teléfono IP Cisco 7912G proporciona características empresariales fundamentales y cubre las necesidades de comunicación de aquellos trabajadores que tienen un tráfico telefónico pequeño o medio. El teléfono IP Cisco 7912G ofrece cuatro teclas programables dinámicas que guían al usuario a través de las diferentes características y funciones de las llamadas. Los usuarios agradecen la capacidad gráfica de la pantalla, ya que ofrece información de las llamadas y un acceso intuitivo a las características. El teléfono IP Cisco 7912G admite un switch Ethernet integrado, con lo que puede proporcionar conectividad LAN a un PC próximo. Además, el teléfono IP Cisco 7912G admite la alimentación en línea, lo que permite al teléfono recibir su alimentación a través de la LAN. Esta

capacidad proporciona al administrador de redes un control centralizado sobre la alimentación, lo que se traduce en una mayor disponibilidad de la red. La combinación de alimentación en línea y soporte de switches Ethernet reduce las necesidades de cableado hasta el punto de que sólo requiere un cable al equipo de sobremesa. El teléfono IP Cisco 7912G es compatible con Cisco CallManager Express, versión 3.0 y posteriores.

Valor comercial.

- Su precio en el mercado es US$ 230, 7 (equivalente aprox. a $ 125.000 pesos).

Y entre otros modelos, tenemos el "teléfono IP Cisco 7920G"

Cisco extiende la potencia de las comunicaciones por IP por toda la empresa, para lo que ofrece una potente solución inalámbrica convergente con una infraestructura inalámbrica inteligente y un producto innovador con la introducción del teléfono IP inalámbrico Cisco 7920.

El modelo Cisco 7920 es un teléfono IP inalámbrico IEEE 802.11b fácil de utilizar que proporciona exhaustivas comunicaciones de voz en conjunción con Cisco CallManager Express y las series Cisco Aironet® 1200, 1100, 350 y 340 de puntos de acceso Wi-Fi (IEEE 802.11b). El teléfono IP inalámbrico Cisco 7920 ofrece servicios inteligentes, como seguridad, movilidad, QoS y gestión en cualquier red de extremo a extremo de Cisco.

Datos característicos.

- IEEE 802.11b, en una escala de 1, 2, 5.5, and 11 Mbps.
- Compatible con Cisco CallManager Versiones 5.0, 4.2, 4.1, 4.0, 3.3.
- Codecs: G.711a, G.711u, y G.729a.
- Rango de frecuencias: 2.4-2.497 GHz.
- Dimensiones (largo, ancho, profundidad): 132.1 x 53.3 x 25.4 mm.
- Peso: 136.1g.

Valor comercial.

- Su precio en el mercado es US$ 292, 05 (equivalente aprox. a $ 158.000 pesos).

Soluciones tecnológicas: CISCO CALLMANAGER EXPRESS

Cisco ® Call Manager Express es una solución integrada en el software Cisco IOS® que permite a los teléfonos IP de Cisco el procesamiento de las llamadas. Esta solución permite a la gran cartera de routers (1760, 2600XM y 3700) de acceso inteligente de Cisco ofrecer características telefónicas similares a las que suelen emplear los usuarios empresariales para satisfacer los requisitos de la pequeña empresa, con lo que posibilita la instalación en las empresas pequeñas de una solución de comunicaciones por IP eficaz y muy fiable.

Los clientes ya pueden escalar la telefonía por IP a un sitio pequeño o a una delegación gracias a una solución que es muy sencilla de instalar, administrar y mantener. La solución Cisco CallManager Express es perfecta para los clientes que buscan una solución económica, fiable y con gran cantidad de características para una instalación de un máximo de cien usuarios.

Al estar integrado en un router, la solución Cisco CallManager Express aumenta las ventajas de la convergencia, ya que ofrece los siguientes beneficios exclusivos:

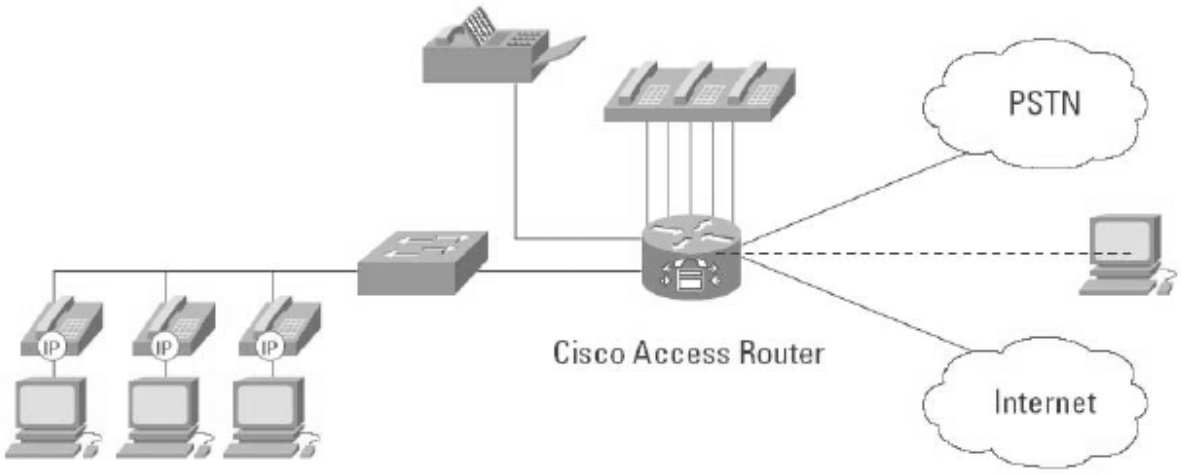
Ventajas de la solución Cisco CallManager Express

- **Funcionamiento económico gracias a una sola plataforma de voz y datos para cubrir todas las necesidades de la delegación:** Varios routers de acceso muy fiables, como las plataformas de las series Cisco 1700, 2600, 3600 y 3700, ya ofrecen las mejores características del sector, entre las que se incluyen una sólida calidad de servicio (QoS), seguridad en la red, cifrado y firewall, y ofrecen nuevos módulos de red que proporcionan redes de contenido y servicios de VPN mejorados que satisfacen las necesidades empresariales de las delegaciones y oficinas pequeñas. Estos routers ya pueden ofrecer también otros elementos integrados, como la telefonía por IP, el correo de voz y la operadora automatizada, lo que permite a los clientes instalar en su oficina un solo dispositivo para cubrir todas las necesidades de la empresa, lo que simplifica la gestión, el mantenimiento y el manejo, reduciendo así el coste total de propiedad (TCO).

- **Un conjunto sólido de capacidades clave del sistema y de PBX de gama baja que se utilizan habitualmente:** las oficinas pequeñas tienen flujos de trabajo diferentes y requieren características especializadas que soporten sus prácticas laborales. Cisco CallManager Express ofrece un sólido juego de características telefónicas para la pequeña empresa y

proporciona capacidades de valor añadido únicas, a través del lenguaje extensible de marcado (XML), que mejoran la productividad del usuario final y de la empresa, y que no pueden ofrecer las soluciones tradicionales.

- **Protección de la inversión y facilidad para su actualización a soluciones centralizadas de procesamiento de llamadas:** a través de una sencilla actualización del software o del firmware, y en la mayoría de los casos solamente con un cambio de configuración del router, un sistema con Cisco CallManager Express se puede convertir en un gateway de voz robusto y muy disponible para un sitio remoto en una arquitectura centralizada de instalación de Cisco CallManager. Esta flexibilidad ayuda a garantizar una total protección de la inversión para crear empresas con éxito que pueden superar la capacidad del sistema.



Cisco CallManager Express permite a los routers de acceso de Cisco proporcionar procesamiento de llamadas a teléfonos IP conectados de forma local. Todos los archivos y configuraciones necesarias de los teléfonos IP se almacenan internamente en el router, por lo que no hacen falta bases de datos ni servidores de archivos externos.

Además, la solución ofrece un sólido conjunto de interfaces de la red de telefonía pública conmutada (PSTN), una amplia selección de interfaces WAN y una mayor cartera de teléfonos. La solución tiene integrados el correo de voz y la asistencia automática, un sólido juego de características de voz líderes del sector presentes en el software Cisco IOS diseñadas para sistemas

basados en IP, como la señalización H.323, QoS avanzada e interoperatividad con un gatekeeper, se pueden utilizar en las instalaciones de Cisco CallManager Express.

Entre otras, las tarjetas de interfaz de PSTN cuentan con funciones integradas, como los dispositivos de unidad de servicio de canal/unidad de servicio digital (CSU/DSU) y de terminación de red 1 (NT1), que proporcionan servicios de voz flexibles y sólidos. El funcionamiento de los teléfonos IP y la ubicación de los botones y teclas programables son similares a los de Cisco CallManager, lo que reduce la formación de los usuarios, por si al cliente se le queda pequeña la solución Cisco CallManager Express y decide migrar a Cisco CallManager.

Compatibilidad con teléfonos IP

Mientras que Cisco CallManager Express se suele recomendar para menos de cien usuarios, con CallManager Express se pueden utilizar un máximo de 120 teléfonos IP, dependiendo de las plataformas.

Plataforma	Nº máximo de teléfonos
Dispositivos de acceso integrado de las series Cisco IAD 24xx	24
Routers de acceso Cisco 1751-V y 1760-V	24
Routers de acceso de las series Cisco 261xXM y 262xXM	36
Router de acceso Cisco 265xXM	48
Router de acceso Cisco 2691	72
Router de acceso Cisco 3725	96
Router de acceso Cisco 3745	120

Plataformas de Cisco CallManager Express

Cisco Systems® ha desarrollado Cisco CallManager Express para todos los routers de acceso de Cisco que soportan voz. En la actualidad, esta capacidad la soportan los dispositivos integrados de acceso de la serie Cisco IAD 2400, los routers modulares de acceso Cisco 1751-V y 1760-V, y los routers de las series Cisco 2600XM, 2691 y 3700. La tabla 3 compara las especificaciones del sistema de una oficina pequeña que utiliza Cisco CallManager Express, representado por los routers Cisco 1760-V o Cisco 2621XM, y del sistema de una oficina mediana que utiliza Cisco CallManager Express, representado por el router de acceso Cisco 3745. Se puede seleccionar cualquiera de los routers que ya hemos visto si se ajusta más a las necesidades de instalación de la oficina.

	Cisco 1760-V	Cisco 2621XM Router oficina pequeña	Cisco 3745 Access Router oficina
Número máximo de teléfonos	24	36	120
Número máximo de líneas	120	216	288
Máximo de enlaces FXO analógicos	16	8	32
Máximo de enlaces E&M	8	4	16
Máximo de enlaces BRI	12	8	32
Máximo de enlaces PRI/T1/E1	4	3	10
Máximo de puertos FXS analógicos	16	12	48
Máximo de túneles DSP T1	24	72	240
Máximo de túneles DSP E1	30	90	300
Máximo de puertos Ethernet con alimentación en línea integrada	- Switch Cisco Catalyst externo	16	36
Velocidad de procesamiento de datos	16 kpps	30 kpps	225 kpps
Memoria Flash (por defecto/máxima)	32 MB/64 MB	32 MB/48 MB	32 MB/128 MB
Memoria del sistema (por defecto/máxima)	64 MB/128 MB	96 MB/128 MB	128 MB/256 MB
Ranuras para módulos de red	-	1	4
Ranuras de interfaz WAN integradas	4	2	3

Resumen

Cisco CallManager Express ofrece características telefónicas similares a las que suelen emplear los usuarios de las empresas para satisfacer las necesidades de las oficinas pequeñas. También usa una infraestructura XML para ofrecer características de valor añadido que no pueden ofrecer los sistemas tradicionales. Dichas características mejoran la productividad de los empleados y de la empresa, además de ofrecer un menor TCO. Teniendo en cuenta que esta solución se integra en routers de acceso muy fiables y que ofrecen capacidades de datos avanzadas, como redes de contenido, VPN, firewall, cifrado, acceso telefónico y conmutación Ethernet, los clientes pueden cubrir todas sus necesidades de voz y datos de las oficinas pequeñas con una sola plataforma, lo que reduce sus costes de gestión, mantenimiento y funcionamiento. Si los requisitos de conjuntos de características o números de teléfono de un cliente aumentan, Cisco CallManager Express puede migrarse fácilmente a una instalación de telefonía por IP a gran escala. Todo el hardware y el software que emplea esta solución es totalmente compatible con Cisco CallManager y Cisco Survivable Remote Site Telephony (SRST).