UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

# “VOZ SOBRE IP CON APLICACIONES A INGENIERIA DE PROYECTOS PARA LA INDUSTRIA PETROLERA”

TESIS

QUE PARA OBTENER EL TITULO DE:

INGENIERO EN TELECOMUNICACIONES

PRESENTA:

MARCO ANTONIO DIAZ FONSECA

DIRECTOR DE TESIS: ING. JOSE RAFAEL GARCIA HERNANDEZ

CODIRECTOR DE TESIS: ING. ADALBERTO GARCIA ESPINOSA


MEXICO, D.F., MAYO DE 2004

# Voz sobre IP con Aplicaciones a Ingeniería de Proyectos para la Industria Petrolera

# Voz sobre IP con Aplicaciones a Ingeniería de Proyectos para la Industria Petrolera

## I. Objetivos

El objetivo primordial de la presente tesis es el de servir como un manual de referencia técnica, para el personal del Instituto Mexicano del Petróleo (IMP) del área de telecomunicaciones, para realizar la implementación efectiva de redes de Voz sobre IP (VoIP) para la industria petrolera nacional, principalmente para el mayor cliente del IMP, Petróleos Mexicanos (PEMEX), de tal manera que dichos sistemas cumplan con los niveles de calidad de voz que actualmente brindan las redes telefónicas tradicionales a la vez que proporcionen nuevas y más poderosas herramientas de comunicaciones.

Para lograr lo anterior se requiere comprender la naturaleza del funcionamiento de los sistemas involucrados, entender los protocolos de comunicación correspondientes, conocer los elementos o equipos requeridos, así como los factores que afectan a las comunicaciones telefónicas a través de redes IP y las herramientas disponibles para minimizarlos, para esto la presente tesis tiene por objetivos los de:

- Describir los fundamentos del funcionamiento de las redes telefónicas de conmutación de circuitos modernas y de los principales sistemas de transporte empleados por dichas redes.

- Especificar los fundamentos del funcionamiento de las redes IP, de los elementos que las constituyen y los requerimientos de Calidad de Servicios (QoS) para dichas redes.

- Hacer notar las ventajas de VoIP respecto a las redes telefónicas tradicionales.

- Describir los fundamentos de VoIP y los estándares utilizados actualmente para su implementación.

- Describir los factores que afectan la calidad de las redes de VoIP y las herramientas empleadas para asegurar la calidad de las llamadas y servicios.

- Sugerir una guía para realizar la implementación efectiva de este tipo redes en PEMEX y presentar un ejemplo práctico que pueda servir de referencia para implementaciones futuras.

## II. Descripción del Problema

*Contexto*

El Instituto Mexicano del Petróleo (IMP) ha sido desde su creación, una importante plataforma para la investigación científica y el desarrollo tecnológico al servicio de las industrias petrolera, petroquímica básica, petroquímica derivada y química. El IMP es una institución moderna y competitiva que se propone asegurar el fortalecimiento de la investigación y el desarrollo tecnológico, con programas y proyectos de investigación de vanguardia, manteniendo una sana capacidad de autofinanciamiento y orientado sus esfuerzos hacia soluciones con servicios integrados a plena satisfacción de Petróleos Mexicanos (PEMEX), su cliente principal.

El área de telecomunicaciones del IMP realiza el diseño de algunas de las redes y sistemas de comunicaciones de PEMEX, que es una institución que continuamente requiere el fortalecimiento de su infraestructura de telecomunicaciones para responder a las crecientes necesidades del personal para compartir archivos, bases de datos, impresoras, correo electrónico, mensajes de voz, multimedia, etc.

PEMEX requiere el mejoramiento de su red telefónica para hacer frente a la creciente demanda de servicios orientados a incrementar la productividad de sus trabajadores y para facilitar la comunicación con sus clientes y proveedores.

PEMEX ha venido operando redes separadas para el transporte de llamadas telefónicas (voz) y comunicaciones informáticas (datos) con grandes niveles de calidad y con tecnología de punta, sin embargo la gestión y el mantenimiento de estas infraestructuras paralelas ha ido aumentando progresivamente en dificultad y complejidad, consumiendo cada vez más tiempo y más recursos.

Adicionalmente, la demanda sobre la red de comunicaciones se ha incrementado de forma considerable. El tráfico de voz y datos se eleva día a día porque los usuarios se apoyan cada vez más en el establecimiento de conexiones constantes con compañeros, socios externos y clientes mediante correo electrónico y teléfono para la realización de sus tareas cotidianas. La creciente naturaleza móvil de los negocios modernos viene a complicar aún más las cosas.

PEMEX dispone de una red corporativa dispersa, integrada por diversos emplazamientos que están geográficamente separados por grandes distancias, lo que incrementa el costo de las comunicaciones telefónicas entre las diferentes oficinas, principalmente por los costos de mantenimiento y administración de dicha red.

Dada esta situación el Área de Telecomunicaciones del IMP busca una nueva forma de diseñar y gestionar redes de voz y datos complejas, respondiendo a las demandas de PEMEX, buscando optimizar la productividad de los empleados y mantener a PEMEX a la vanguardia en tecnología.

*Alcance*

Este trabajo pretende servir de guía para el personal responsable en el IMP de diseñar las redes de voz y datos de PEMEX, definiendo los parámetros más adecuados para que se pueda lograr la convergencia de dichas redes y hacer frente a las nuevas demandas de servicios de voz y datos en PEMEX.

*Conexión con Otros Problemas*

Desde hace años la convergencia de las redes de comunicaciones de voz, datos y video, en una sola red convergente es el gran reto de la industria de las telecomunicaciones. Sus ventajas son claras y múltiples, entre ellas, la más llamativa, aunque no la más importante, es el ahorro de costos. Los beneficios económicos se obtienen al integrar en un solo sistema dos o más infraestructuras hasta el momento separadas, como lo son la red telefónica y la red de datos, así como también de los beneficios derivados de simplificación de la administración y gestión de una única red de comunicaciones. Hasta hace un tiempo el principal problema era la incompatibilidad de dichos sistemas debida a diferencias tecnológicas, sin embargo actualmente ya se cuenta con las herramientas y sistemas que lo pueden hacer posible de una manera segura y efectiva.

Este trabajo pretende en un principio proponer la convergencia de las redes de datos y telefónica, en una sola red de comunicaciones, para los futuros proyectos diseñados por el IMP, y que a su vez permita la futura incorporación de otros servicios multimedia como son videoconferencias y circuitos cerrados de televisión transportados por dicha red convergente.

*Justificación*

Gracias al desarrollo de Internet, la telefonía sobre IP ha pasado en poco tiempo de ser una innovadora e interesante posibilidad a convertirse en una imperiosa necesidad, relegando otras propuestas, como la voz sobre Frame Relay o la voz sobre ATM.

Los beneficios son reales y demostrables. Existe una inmediata reducción del gasto consecuencia de la racionalización de los recursos que supone la unión de dos redes en una, no sólo en términos de compra de equipamiento, sino también del posterior mantenimiento y administración de la infraestructura. Además actualmente la oferta de productos disponibles en el mercado cuenta con soluciones adecuadas para empresas de cualquier tamaño.

Esta alternativa pone a disposición de los usuarios las ventajas de la mensajería unificada (un único sistema integrado para correo electrónico, correo de voz, fax y datos), y un mejor soporte para el trabajo remoto, permitiendo a los empleados acceder a la infraestructura de la empresa desde cualquier lugar, enviando y recibiendo llamadas telefónicas y correos electrónicos exactamente de la misma manera que si estuvieran en la oficina. Además, funciona con independencia del medio de transporte y del dispositivo de acceso, soportando desde teléfonos convencionales, teléfonos IP, teléfonos inalámbricos, hasta computadoras personales, computadoras portátiles y otros dispositivos portátiles.

Un atractivo importante a la hora de evaluar una solución de Voz sobre IP (VoIP) es la facilidad de instalación y administración. Con esta tecnología es posible realizar cambios, movimientos y adiciones de forma centralizada y con un navegador *web* como única interfaz. El administrador, por ejemplo, puede resolver remotamente casi cualquier problema que surja al utilizar, por ejemplo, una característica avanzada de correo de voz.

Otra gran ventaja de la tecnología VoIP es que el cambio no tiene que ser drástico, la inversión realizada en equipamiento de telefonía convencional puede aprovecharse. Los fabricantes han desarrollado diversas arquitecturas que facilitan la introducción de la nueva tecnología, permitiendo tanto implementaciones puras como otras en las que existe espacio para la convivencia de PBX basadas en conmutación de circuitos con plataformas PBX LAN.

Con VoIP es posible utilizar la red IP Ethernet ya existente, puede instalarse un teléfono IP o terminal en cualquier lugar donde ya exista un nodo de red para computadora, estos teléfonos son muy similares, tanto en apariencia como en funcionamiento, a los teléfonos convencionales. Además si se lleva la interfaz de control de llamadas al entorno PC, los sistemas de voz sobre IP reducen el rol del teléfono ya que la funcionalidad de las teclas añadidas en los teléfonos convencionales más avanzados se traslada al software, lo que resulta en un uso mucho más amigable para el usuario.

Las PBX IP permiten crear infraestructuras capaces de hacer frente a los picos de utilización de usuarios, así como a los de consultas y peticiones de los clientes. Esta característica cobra una especial relevancia, ya que proporciona la posibilidad de contar con un centro de llamadas principal e integrar grupos de otras ubicaciones dinámicamente, en función de la carga de trabajo y las habilidades específicas de cada empleado. De esta forma, el personal, el activo más caro, es aprovechado con la máxima eficiencia.

Una PBX IP puede integrar múltiples dispositivos geográficamente dispersos dotándolos de capacidad para colaborar entre sí como un único sistema. Esta característica, comúnmente conocida como arquitectura distribuida, aporta múltiples ventajas, incluida la tolerancia a fallos.

*Relevancia*

Adicionalmente a los importantes ahorros económicos derivados de la instalación y administración de una red única de comunicaciones, la implementación de VoIP en las redes de PEMEX significaría proveer a sus trabajadores de mayores herramientas de comunicación que les permitirían ser más eficientes, al facilitarse el intercambio de información en tiempo real, ya que este sistema permite que los usuarios puedan mantener una comunicación permanente entre ellos, facilita el intercambio de archivos, propicia la colaboración remota, permite videoconferencias y conferencias de voz, entre otras aplicaciones que definitivamente impactaran positivamente en la toma de decisiones y en la realización de tratos y negocios.

## III. Método

Para resolver esta problemática se recurrió a la consulta de profesionistas de las telecomunicaciones que tienen experiencia en el diseño e implantación de este tipo de tecnología, se consulto también a organismos de normalización de telecomunicaciones como la **ITU** (*International Telecommunication Union*) o el **IETF** (*Internet Engineering Task Force*), se consultó literatura especializada en voz sobre IP y se consultó información relacionada publicada en Internet.

En el área de telecomunicaciones del IMP se consultó a personal con experiencia en el diseño de redes que emplean este tipo de tecnología. Se consultaron los estándares que soportan VoIP y que definen el control de llamadas en esta tecnología: **H.323** de la UIT y **SIP** (*Session Initiation Protocol*) de la IETF. También se hizo uso de la información publicada en Internet por los principales fabricantes de equipo de esta tecnología (principalmente Cisco y Nortel Networks) y se consultó bibliografía referente a VoIP.

**IV. Inventario de Materias que se Utilizaron para Desarrollar esta Tesis**

- Telefonía
- Redes de Teleinformática
- Redes Digitales de Servicios Integrados
- Temas Especiales de Telecomunicaciones

**V. Resultados Esperados**

- Adquisición de experiencia profesional, de nuevos conocimientos de ingeniería en telecomunicaciones y desarrollo de nuevas habilidades.
- Aplicación de los conocimientos del tesista en la solución de un problema práctico.
- Elaboración de una guía de implementación que sirva de base o referencia para futuros diseños de proyectos de ingeniería de telecomunicaciones referentes a VoIP para PEMEX realizados en el Instituto Mexicano del Petróleo (IMP).
- Presentación de un ejemplo práctico que sirva ilustrar los conceptos y métodos de diseño propuestos en esta tesis.

# Capitulo 1

# Fundamentos de las Redes Telefónicas Conmutadas

### 1.1 Arquitectura y Funcionamiento

La **red telefónica conmutada** es la red de comunicaciones de mayor cobertura geográfica y la que mayor número de usuarios tiene. Permite establecer una llamada entre dos usuarios en cualquier parte del planeta de manera distribuida, automática y prácticamente instantánea. Este es el ejemplo más importante de una red de **conmutación de circuitos**.

Una llamada iniciada por el usuario origen llega a la red por medio de un canal de muy baja capacidad, el canal de acceso, dedicado precisamente a ese usuario denominado línea de abonado. En un extremo de la línea de abonado se encuentra el aparato terminal del usuario (teléfono, fax o módem) y el otro está conectado al primer nodo de la red, la central local.

La función de una central consiste en identificar en el número marcado, la central a la cual está conectado el usuario destino y enrutar la llamada hacia dicha central, con el objeto de que ésta le indique al usuario destino por medio de una señal de timbre, que tiene una llamada. Al identificar la ubicación del destino reserva una trayectoria entre ambos usuarios para poder iniciar la conversación, esto es a lo que se llama conmutación de circuitos. La trayectoria o ruta no siempre es la misma en llamadas consecutivas, ya que ésta depende de la disponibilidad instantánea de canales entre las distintas centrales.

Por la dispersión geográfica de la red telefónica y de sus usuarios existen varias centrales locales, las cuales están enlazadas entre sí por medio de canales de mayor capacidad, de manera que cuando ocurran situaciones de alto tráfico no haya un bloqueo entre las centrales. Existe una jerarquía entre las diferentes centrales que le permite a cada una de ellas enrutar las llamadas de acuerdo con los tráficos que se presentan en ellas.

Los enlaces entre los abonados y las centrales locales son normalmente cables de cobre, pero las centrales pueden comunicarse entre sí por medio de enlaces de cable coaxial, de fibras ópticas o de canales de microondas. En caso de enlaces entre centrales ubicadas en diferentes ciudades se usan cables de fibras ópticas, enlaces de microondas y enlaces satelitales, dependiendo de la distancia que se desee cubrir.

Como las necesidades de manejo de tráfico de los canales que enlazan centrales en los diferentes niveles jerárquicos aumentan conforme incrementa el nivel jerárquico, también las capacidades de los mismos deben ser mayores en la misma medida, de otra manera, aunque el usuario pudiese tener acceso a la red por medio de su línea de abonado conectada a una central local, su intento de llamada sería bloqueado por no poder establecerse un enlace completo hacia la ubicación del usuario destino (cuando el usuario destino está haciendo otra llamada, al llegar la solicitud de conexión a su central local, ésta detecta el hecho y envía de regreso una señal que genera la señal de ocupado).

La red telefónica está organizada de manera jerárquica. El nivel más bajo (las centrales locales) está formado por el conjunto de nodos a los cuales están conectados los usuarios. Le siguen nodos o centrales en niveles superiores, enlazados de tal manera que entre mayor sea la jerarquía, mayor será la capacidad que los enlaza. Con esta arquitectura se proporcionan a los usuarios diferentes rutas para colocar sus llamadas, que son seleccionadas por los mismos nodos, de acuerdo con criterios preestablecidos, tratando de que una llamada no sea enrutada más que por aquellos nodos y canales estrictamente indispensables para completarla (se trata de minimizar el número de canales y nodos por los cuales pasa una llamada para mantenerlos desocupados en la medida de lo posible).

Asimismo existen nodos (centrales) que permiten enrutar una llamada hacia otra localidad, ya sea dentro o fuera del país. Este tipo de centrales se denomina centrales de larga distancia. El inicio de una llamada de larga distancia es identificado por la central por medio del número marcado, que indica además el tipo de

enlace, nacional o internacional, en este último caso le indica también el país de que se trata. A pesar de que el acceso a las centrales de larga distancia se realiza en cada país por medio de un código propio, éste señala, sin lugar a dudas, cuál es el destino final de la llamada. El código de un país es independiente del que origina la llamada.

Cada central realiza las siguientes funciones básicas:

- Cuando un abonado levanta el auricular de su aparato telefónico, la central lo identifica y le envía una señal de invitación a marcar.
- La central espera a recibir el número seleccionado, para escoger una ruta del usuario fuente al usuario destino.
- Si la línea de abonado del usuario destino está ocupada, la central lo detecta y le envía al usuario fuente una señal de tono de ocupado.
- Si la línea del usuario destino no está ocupada, la central a la cual está conectado genera una señal para indicarle al destino la presencia de una llamada.
- Al contestar la llamada el usuario destino, se establece un canal bidireccional de comunicación y se suspende la generación de dichas señales.
- Al concluir la conversación, las centrales deben desconectar la llamada y poner los canales a la disposición de otro usuario, a partir de ese momento.
- Al concluir la llamada se debe contabilizar su costo para su facturación, para ser cobrado al usuario que la inició.

El servicio para el cual fueron diseñadas las redes telefónicas, es el de comunicación de voz, es decir, la transmisión bidireccional de señales de voz, con el objeto de que dos usuarios puedan establecer y sostener una conversación. Este servicio tiene básicamente tres componentes:

1) Etapa de señalización: Que incluye la selección del número del destinatario, la identificación de una ruta por medio de la conmutación, la reservación de la misma y el timbrado
2) Etapa de Transmisión: Que consiste en la conversión de las señales acústicas en señales eléctricas, su transporte a través de los medios de comunicación, y la conversión de señales eléctricas nuevamente en acústicas para ser entregadas al destinatario.
3) Etapa de Finalización de Llamada: Que consiste básicamente en la liberación de los canales reservados para que puedan ser empleados por otros usuarios.

### 1.2 Señalización

Por **s**eñalización se entiende el conjunto de información intercambiada entre dos puntos de la red (abonado-central o central-central) que permiten:

- Supervisión: Detección de condición o cambio de estado de un canal de comunicación.
- Direccionamiento: Establecimiento de llamada.
- Explotación: Gestión y mantenimiento de la red.

A los largo del desarrollo de las redes telefónicas han existido varias técnicas de señalización, actualmente las más ampliamente utilizadas son la señalización DTMF utilizada entre abonado y centrales telefónicas y el sistema de señalización SS7 utilizado entre centrales telefónicas.

#### 1.2.1 Señalización DTMF

La transmisión entre los abonados y las centrales locales se realiza normalmente de forma analógica, son muy pocas las terminales que transmiten digitalmente, como en el caso de las terminales telefónicas conectadas a redes digitales de servicios integrados (RDSI), por lo que se utiliza un tipo de señalización analógica entre los abonados y las centrales locales.

En la red telefónica pública, se emplean varios tonos de una frecuencia o monotonos o combinaciones (suma) de señales senoidales de diferentes frecuencias para realizar la señalización, estas señales son analógicas y se presentan en forma continua en el tiempo ó bien pueden estar presentes durante un tiempo sí y un tiempo no, ó bien presentarse en una ráfaga (*Burst*) de señal.

Los tonos que una central telefónica envía al abonado telefónico que esta llamando, son distintivos y le van notificando el progreso que su llamada tiene (*Call Progress*), por ejemplo el tono de invitación a marcar, tono de llamado, tono de ocupado, le va dando idea al usuario del estado que guarda su comunicación, en la siguiente tabla, se muestran las frecuencias y cadencias de los principales tonos usados en México.

| TONO | FRECUENCIA MÉXICO | CADENCIA MÉXICO |
|---|---|---|
| Invitación a Marcar | 420 Hz. | Continuo |
| Ocupado (Busy) | 420 Hz. | 200 ms ON - 200 ms OFF |
| Llamando Normal (Ring Back) | 420 Hz. | 1seg ON - 4 seg OFF |
| Llamando PBX | 500 Hz. | 0.4 seg ON - 0.8 seg OFF |
| Congestión | 420 Hz. | 200 ms ON - 200 ms OFF |

*Frecuencias y cadencias empleadas en México*

Tradicionalmente la manera de señalizar en telefonía había sido mediante interrupciones controladas (40 ms - 60 ms) de la línea telefónica y se le denominaba señalización por pulsos, el sistema de marcación era el disco giratorio que al regresar iba abriendo y cerrando la línea telefónica, mediante sistemas mecánicos (levas) y contactos eléctricos, sin embargo desde la década de los 70´s, se empezaron a concebir nuevos métodos que funcionaran dentro de la banda telefónica, de 300 a 3400 Hz, y que la marcación se enviara por tonos, es decir señales audibles que se agregaran sin introducir ruido a la línea o transitorios indeseables, y que se pudieran enviar y detectar en forma inconfundible, por esto se ideo el concepto DTMF.

La señalización **DTMF** (*Dual Tone Multi Frecuency*), utiliza dos tonos de múltiples frecuencias, y que y se denomina marcación por tonos. Se dice que es un sistema de señalización en banda porque la señalización se transporta "en banda" (cambios de nivel y tonos dentro del propio canal telefónico).

Se eligió un conjunto de frecuencias bajas y un conjunto de frecuencias altas o tonos bajos y tonos altos, y para cada dígito del 1 al 0, se envía la suma algebraica de dos señales senoidales, una del conjunto de tonos bajos y otra del conjunto de tonos altos, de acuerdo a la siguiente tabla:

| TECLA | FRECUENCIA | TECLA | FRECUENCIA |
|---|---|---|---|
| 1 | 697+1209 Hz. | 7 | 852+1209 Hz. |
| 2 | 697+1336 Hz. | 8 | 852+1336 Hz. |
| 3 | 697+1477 Hz. | 9 | 852+1477 Hz. |
| A | 697+1633 Hz. | C | 852+1633 Hz. |
| 4 | 770+1209 Hz. | * | 941+1209 Hz. |
| 5 | 770+1336 Hz. | 0 | 941+1336 Hz. |
| 6 | 770+1477 Hz. | # | 941+1477 Hz. |
| B | 770+1633 Hz. | D | 941+1633 Hz. |

*Frecuencias usadas por DTMF*

En este caso al pulsar alguna tecla del teclado telefónico, se ordena al circuito generador de señalización DTMF, que sume las frecuencias de la matriz y las envíe por la línea telefónica, así se transmiten señales por cada tecla.

Los teléfonos normales utilizan el teclado comercial y los teléfonos o aparatos especiales utilizan además las teclas especiales que junto con el teclado convencional constituyen el teclado extendido. Así por ejemplo cuando la tecla 4 se pulsa se envía la señal que es la suma de dos senoidales una de frecuencia 770 Hz y la otra de 1209 Hz, entonces la central telefónica podrá decodificar esta señal como el dígito 4 y realizara la acción correspondiente.

Los tonos de las señales de multifrecuencias fueron diseñados de forma que no sean armónicos de frecuencias muy usadas como la de 60 Hz de modo que si los tonos son enviados con exactitud así también son

decodificados. La señalización DTMF supera a la de pulsos al ser más rápida, tener más dígitos (16 en lugar de 10), ser más inmune al ruido y estar en la banda audible. Los tonos solo pueden tener variaciones de ± 1.5 % de su fundamental, y normalmente la señal de tono alto es 3 a 4 dB más fuerte que la de tono bajo.

En los accesorios telefónicos se utiliza frecuentemente la señalización DTMF, para programar alguna función, para ordenar que el aparato haga alguna operación, para activar o desactivar alguna característica, para cambiar claves, y muchas otras aplicaciones, sin embargo siempre es necesario que se utilice un teléfono de teclas ó de señalización de tonos.

### 1.2.2 Sistema de Señalización SS7

La señalización en la línea de abonado del servicio de telefonía tradicional ha evolucionado muy poco por ser analógica, es dentro de la red donde se ha realizado una revolución muy importante, transparente al usuario y que ha permitido la introducción de servicios suplementarios, de telefonía móvil, de red inteligente, y de interfuncionamiento con sistemas de telefonía sobre IP (VoIP) entre otros.

Los primeros protocolos de señalización instalados en los sistemas de conmutación digital tenían una capacidad muy limitada y se basaban en el estado de ciertos bits de la trama **TDM** (*Time Division Multiplexing*) permanentemente asociados a cada canal de voz, eran representaciones binarias de las señales analógicas de los sistemas anteriores. El gran avance se consiguió cuando se aplicó totalmente la tecnología de redes de datos y las señales se convirtieron en mensajes intercambiados por aplicaciones sobre una red de conmutación de paquetes independiente y dedicada a este fin.

El sistema de señalización de red que ha soportado esta evolución con gran flexibilidad es el Sistema de Señalización Numero 7 **SS7** (*Signaling System 7*).

La red SS7 es una red (orientada a no conexión) basada en paquetes que transporta el tráfico de señalización entre los conmutadores implicados en la llamada. Los puntos de control del servicio (SCP) son las bases de datos que ejecutan las consultas para traducir números de teléfono a los detalles de la conmutación de circuitos. Los puntos de conmutación de señalización (SSP) son las interfaces entre el equipo de la conmutación del circuito y la red SS7. Es aquí donde los mensajes SS7 se traducen a los detalles de la conexión que el conmutador necesita para establecer una llamada.

El equipo especializado llamado puntos de transferencia de la señal (STP) transporta los mensajes de señalización, los mensajes son llevados en paquetes llamados partes de transferencia de mensaje (MTP).

La red SS7 es bastante extensa (una gran colección de redes) y se despliega por todo el mundo desarrollado. Permite agregar inteligencia de red y características sin una dependencia en la infraestructura de la conmutación de circuitos.

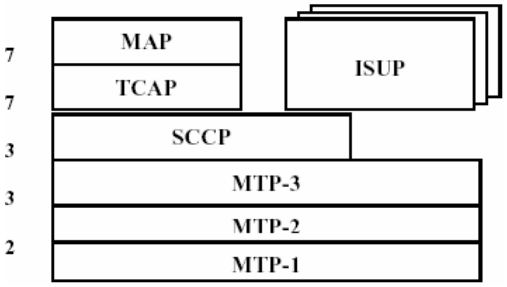
El Sistema de Señalización SS7 es una arquitectura de protocolos de señalización completa en el que las unidades de señal son mensajes de las aplicaciones de señalización transportados en paquetes. Las características esenciales de este sistema son:

- Los enlaces y nodos de señalización constituyen una red de conmutación de paquetes lógicamente independiente de la de conmutación de circuitos, con un plan de direccionamiento distinto y definido a nivel internacional por la ITU (*International Telecommunication Union*).
- Es un sistema de señalización por canal común, es decir que existe un conjunto predefinido de canales entre centrales (y puntos de transferencia de señalización sin capacidad de conmutación de circuitos) dedicados a transportar mensajes de señalización relativa al establecimiento, liberación y supervisión de cualquier canal de 64 Kbps de voz o datos. En los sistemas de señalización previos, por canal asociado, la señalización asociada a cada circuito de voz se transportaba por un canal de transmisión dedicado exclusivamente a él.
- Es una arquitectura de protocolos estructurada en cuatro niveles.

#### 1.2.2.1 Modelo de Capas del SS7

El ITU-T ha fijado y diseñado el SS7 con el propósito de ser compatible con la red digital futura y con los servicios integrados de redes digitales **ISDN** (*Integrated Services Digital Network*). La estructura lógica del SS7 se fundamenta en el modelo de 7 capas de Interconexión de Sistemas Abiertos **OSI** (*Open System Interconnetion*) aunque el modelo se reduce a 4 capas para obtener un ahorro sustancial en el tiempo de procesamiento.

En la señalización por canal común, la red de señalización puede ser distinta a la red de información debido a que se pretende una red redundante para asegurar al máximo la confiabilidad del mensaje. En otras palabras, se pretende que la comunicación entre procesadores de los centros de conmutación se mantenga aún cuando las condiciones de la red de transporte de información de usuario se encuentren interrumpidas.



*Modelo de Capas del SS7*

**MTP-1 Capa 1:** Tiene las funciones de conexión física entre módulos a interconectar.

**MTP-2 Capa 2:** Se ocupa del alineamiento de paquete mediante banderas (*flags*) al inicio y final, permite la detección de errores mediante un código CRC-16, realiza el proceso de numeración secuencial de mensajes e indicación de retransmisión, efectúa la confirmación o rechazo del mensaje para la retransmisión automática en mensajes con errores e indica la longitud total del mensaje transmitido.

**MTP-3 Capa 3:** Posee una dirección del punto de acceso al servicio **SAP** (*Service Access Point*) en la información de servicio (*SIO)*. SAP permite identificar a la capa superior SCCP sobre el protocolo MTP3, en la red telefónica publica conmutada (RTPC) se dispone de las direcciones de procesador CPU de origen y destino (14 bits de dirección), por otro lado identifica el enlace de señalización utilizado cuando existe más de uno. Realiza las funciones de enrutamiento dentro de la red de señalización SS7.

**UP Capa 7:** (Parte de usuario) Asegura la generación y tratamiento del mensaje de señalización, contiene:

- Usuario de telefonía (**TUP)**.
- Usuario de datos (**DUP)**.
- 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 son:

**IAM:** Contiene la información inicial de llamada para el enrutamiento.
**SAM:** Transporta las cifras no enviadas en el mensaje IAM.
**ACM:** Indica que se ha obtenido un acceso al destino.
**ANM:** Indica que el usuario llamado ha respondido.
**BLO:** Permite el bloqueo del canal útil.
**UBL:** Desbloquea el canal útil.
**REL:** (*Release Message*) Permite iniciar la liberación del canal.
**RLC:** Informa que la liberación ha sido completada.

**SCCP Capa 3:** Efectúa funciones de direccionamiento adicionales a MTP3, especial para sistemas celulares. La combinación de SCCP y el MTP3 se denomina parte del servicio de red **NSP**, SCCP puede brindar servicios con y sin conexión. En telefonía celular se trata de un servicio sin conexión (*connectionless*) y la capa superior es TCAP, en el caso de servicio con conexión la capa superior es ISUP. El caso con conexión se aplica para consulta de base de datos (ejemplo, tarjeta de crédito).

SCCP entrega una dirección (adicional a la de 14 bits de MTP3) que se denominada **SSN** (*SubSystem Number*) que permite direccionar al usuario del protocolo SCCP en el nodo. Se trata de 4 direcciones: el registro de localización VLR y HLR, la red de conmutación MSC y el centro de autentificación EIR. El campo de direcciones de SCCP posee la dirección de origen y destino y la selección de ruta de señalización, dispone de 16 tipos de mensajes: Requerimiento de conexión, confirmación de conexión, conexión negada, formato de datos, control de flujo, datos urgentes (control de flujo), requerimiento de reset y confirmación de reset, etc.

**TCAP Capa 7:** Facilita la transferencia de mensajes en tiempo real entre MSC, HLR y VLR. En tarjetas de crédito permite verificar la autenticidad y movimientos de cuenta. Realiza el control de diálogo con la terminal remota, es un servicio de transporte. La información contiene: Tipo de mensaje (unidireccional, inicio, final, intermedio, abortado); 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 rechazo) y contenido de información (código de operación, de error, de problema, parámetros, etc.).

**MAP Capa 7:** MAP se usa para la 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.

#### 1.2.2.2 Tipos de Mensajes para Telefonía.

**1. Mensajes de Señalización Telefónica**

1.1 Grupo de mensajes de señalización hacia adelante
- Mensaje inicial de dirección de enrutamiento y mensaje subsiguiente.

1.2 Grupo de mensajes hacia adelante para establecimiento de llamada
- Mensaje hacia adelante con información general
- Mensaje de verificación de continuidad o falla

1.3 Grupo hacia atrás con petición para establecimiento de llamada
- Mensaje de petición general (identidad o categoría)

1.4 Grupo hacia atrás con información sin establecimiento de llamada
- Mensaje de dirección completo y mensaje de tasación

1.5 Grupo hacia atrás con establecimiento no completado
- Mensaje simple hacia atrás con establecimiento no completado

1.6 Grupo de supervisión de llamada adelante-atrás
1.7 Grupo de supervisión de circuitos adelante-atrás
1.8 Grupo de supervisión de haz de circuitos
1.9 Grupo de mensajes de gestión de la red de circuitos
- Mensaje de información de control de congestión

**2. Información de Servicio**

2.1 Indicador de servicio de generador del mensaje
2.2 Indicador de red para mensaje nacional e internacional.

**3. Información de Señalización**

3.1 Elementos de la etiqueta
- Código de puntos de destino y de punto de origen
- Código de identificación de circuito

3.2 Identificadores de formato de mensaje
- Encabezamiento e indicador de longitud de campo

3.3 Señales hacia adelante para establecimiento de llamada
- Indicador de prueba de continuidad
- Indicador de línea llamante, categoría y estado de indisponibilidad
- Indicador de transferencia de llamada
- Indicador de identificación de llamada maliciosa
- Indicador de retención e información de tasación
- Señal de dirección y señal de fin de numeración
- Categoría de abonado que llama

3.4 Señales hacia atrás para establecimiento de llamada
- Indicador de petición de identidad y categoría llamante
- Indicador de supresor de eco
- Señal de información de tasación
- Señal de congestión en el equipo de conmutación

3.5 Señales de supervisión de llamada
- Señal de colgar, de fin de conexión y de liberación

3.6 Señales de supervisión de circuitos
- Señal de bloqueo y desbloqueo
- Señal de petición de prueba de continuidad

3.7 Mensaje de supervisión de haz de circuitos
3.8 Señales de control de congestión automática

### 1.3 Conmutación

Una red telefónica consiste en una sucesión alternante de nodos y canales de comunicación, es decir, después de ser transmitida la información a través de un canal, llega a un nodo, éste a su vez, la procesa para enviarla por el siguiente canal que llega al siguiente nodo, y así sucesivamente.

#### 1.3.1 Tipos de Conmutación

Existen dos tipos de conmutación en este tipo de redes: conmutación de paquetes y conmutación de circuitos.

En la **conmutación de paquetes**, el mensaje se divide en pequeños paquetes, a cada uno se le agrega información de control (por ejemplo, las direcciones del origen y del destino), y éstos circulan de nodo en nodo, posiblemente siguiendo diferentes rutas. Al llegar al nodo al que está conectado el usuario destino, se reensambla el mensaje y se le entrega.

En la **conmutación de circuitos** se busca y reserva una trayectoria entre los usuarios, se establece la comunicación y se mantiene esta trayectoria durante todo el tiempo que se esté transmitiendo información, por esto se dice que es una conmutación orientada o conexión. Para establecer una comunicación con esta técnica se requiere de una señal que reserve los diferentes segmentos de la ruta entre ambos usuarios, y durante la comunicación el canal quedará reservado para esta pareja de usuarios.

Las redes telefónicas están basadas en redes de conmutación de circuitos. Actualmente, el proceso de conmutación de las redes telefónicas se realiza de manera digital mediante centrales digitales que realizan el control de la conmutación mediante una unidad de control (control mediante un programa almacenado). De este modo, los canales de 64 Kbps son conmutados octeto a octeto espacial y temporalmente. Estos conmutadores están controlados íntegramente por procesadores que hablan un protocolo de señalización con procesadores de otras centrales.

La Unidad de Control. Cumple básicamente tres funciones:

- Establecimiento de la conexión: Gestiona y confirma peticiones, determina si el destino está libre y construye el camino dentro del conmutador.
- Mantenimiento de la conexión.
- Desconexión: Ya sea por solicitud o por una necesidad interna.

Durante el establecimiento de la llamada se reservan recursos físicamente (canales dentro de la trama TDM) de forma que los bits que entran por un puerto sean conmutados instantáneamente a un canal de un puerto de salida. Este tipo de redes funciona a nivel físico y transportan fundamentalmente voz en forma digital.

La transmisión de información digital como fax y datos, necesita de una transformación digital/analógica y analógica/digital en sus extremos.

### 1.3.2 Mecanismos de Conmutación

Hay dos mecanismos de conmutación digital:

**Conmutación Espacial:** se basa en una matriz por puntos de cruce (cada punto de cruce es una compuerta lógica) que conecta puertos de entrada con puertos de salida. Para optimizar el número de puntos de cruce se usan sistemas multi-etapa (matrices con menor puntos de cruce conectadas consecutivamente).

**Conmutación Temporal:** se basa en la utilización de buses TDM internos al conmutador que permiten la conmutación entre puertos de entrada y salida. La lógica del conmutador está gestionada por un control que habilita las puertas lógicas o los canales de los buses TDM.

### 1.3.3 Arquitectura de Niveles

La arquitectura de niveles en una conmutación de circuitos consiste en conmutadores que implementan únicamente el nivel físico. Este nivel físico usa multiplexación TDM para transportar los datos. Sin embargo en la conmutación de circuitos puede haber canales de control asociados a los de datos que se utilizan para establecer y liberar la conexión. Estos canales pueden usar un protocolo de nivel de enlace para asegurarse de que el circuito ha sido establecido. En una red de conmutación los retardos son constantes, es decir, para el usuario es como una conexión punto a punto.

## 1.4 Multiplexación

Como se mencionó anteriormente, la arquitectura de las redes telefónicas conmutadas corresponde a un esquema jerárquico, por esto es necesario que las señales de voz y señalización sean multiplexadas durante su transporte dentro de la red y que sean demultiplexadas para ser entregadas a las terminales de abonado correspondientes, es decir que se tienen que agrupar varias señales para que sean transportadas dentro de un mismo canal de comunicación de una manera simultanea mientras viajan por la red telefónica y que después sean separadas para ser entregas a sus correspondientes líneas de abonado.

### 1.4.1 Tipos de Multiplexación

Para hacer esto anteriormente se utilizaba un esquema de multiplexación por división de frecuencia **FDM** (*Frequency Division Multiplexing*) en el cual los canales de voz se modulan o trasladan en frecuencia de tal manera que viajen por un mismo canal de una forma independiente, pero actualmente en su gran mayoría este proceso se realiza mediante un esquema de multiplexación por división de tiempo **TDM** (*Time Division Multiplexing*) donde cada usuario tiene sucesivamente todo el ancho de banda del canal por un momento.

TDM se puede usar solamente con datos digitales lo que implica que cuando las señales analógicas (voz y señalización) provenientes de la línea de abonado llegan a las centrales locales estas sean digitalizadas, por ejemplo, mediante un proceso de modulación de pulsos codificados **PCM** (*Pulse Code Modulation),* es decir

que las señales analógicas tienen que ser muestreadas, cuantizadas y codificadas a un código binario o secuencia de bits.

La voz humana contiene frecuencias entre 300 Hz y 3400 Hz, pero debido al esquema FDM se tomo la convención de utilizar canales de voz de 4000 Hz de ancho de banda, que permiten demultiplexar las señales de voz sin que sufran efectos de interferencia entre canales adyacentes. De acuerdo a esta convención se dice que los canales de voz analógicos tienen un ancho de banda de 4000 Hz por lo que para poder capturar la información más importante de dichas señales se requiere muestrear el flujo 8000 veces por segundo de acuerdo al teorema de Nyquist, es decir que cada muestra dura 125 microsegundos, para codificar cada muestra se utilizan 8 bits, lo que arroja que cada canal de voz requiere una tasa de **64 kbps**.

### 1.5 Tecnologías de Multiplexación Telefónica

Las centrales telefónicas emplean diversas tecnologías de multiplexación que se basan es un esquema TDM, a continuación se describen las principales, PDH, SDH y ATM, y que son las que se emplean principalmente en la industria petrolera nacional.

#### 1.5.1 PDH

Cualquier tecnología de transmisión utilizada para transportar voz debe admitir una muestra del canal cada 125 microsegundos. Una de estas tecnologías es la llamada de Jerarquía Digital Plesiocrona **PDH** (*Plesiochronous Digital Hierarchy*) que se describe a continuación.

##### 1.5.1.1 Trama PDH

PDH es una técnica de TDM síncrona, por lo tanto la estructura de trama de cualquier trama PDH debe durar necesariamente 125 μs, independientemente del número de canales de voz transportados.

Dos aproximaciones han sido adoptadas, que difieren principalmente en el número de canales de voz que la trama contiene y en la forma en la que la señalización es transportada. La primera aproximación es la adoptada en Japón y USA, en la que 24 canales de voz son transportados en la trama. Además de esos 24 canales de voz, que son los que forman básicamente la trama T1, un único bit es añadido a esta trama para proporcionar alineamiento de trama y el servicio mínimo de señalización. De esta forma, la capacidad total requerida es:

$$(24 \text{ canales} * 8\text{bit/canal} + 1\text{bit}) / 125\ \mu s = 1.544 \text{ Mbps}.$$

Una aproximación diferente fue la adoptada en Europa, se tuvo un cuidado especial en proporcionar servicios de señalización y sincronización en la trama E1. En este caso 30 canales de voz son transportados por la trama, además de dos canales, de la misma capacidad que el canal de voz, que permiten la transmisión de información de alineamiento de trama, comunicación de alarmas y bits de **CRC**. Además, cada canal de voz es señalizado mediante un canal especialmente dedicado a ello, lo que permite disponer de 2 Kbps de información de control para cada canal. De esta forma la capacidad total de transmisión en un enlace E1 es:

$$(32 \text{ canales} * 8 \text{ bits/canal}) / 125\ \mu s = 2.048 \text{ Mbps}.$$

Estos circuitos pueden a su vez ser multiplexados dentro de circuitos de nivel más alto, dando lugar a las jerarquías de multiplexación, requiriendo cada nivel más bits de control.

##### 1.5.1.2 Características de PDH

La multiplexación en PDH no está exenta de problemas. Estos problemas surgen principalmente cuando se tienen que demultiplexar los circuitos transportados hasta cierto nivel, especialmente si es necesario extraer un canal de voz básico. Al tener todos los circuitos, en cada jerarquía su propio reloj no hay una base de tiempos común para todos los sistemas (excepto en los que transmiten a la misma velocidad), no es posible extraer un circuito sin tener que demultiplexar completamente la señal hasta el nivel requerido.

Este hecho se debe a una razón histórica, dado que los sistemas digitales han desplazado gradualmente a los anteriores sistemas analógicos, que tenían diferentes valores de temporización debido a razones tecnológicas.

La principal consecuencia de esta aproximación es que cada canal no tiene una asignación estricta en ningún *slot* temporal, y por lo tanto cada circuito es mapeado dentro de un nivel superior utilizando justificación, para acomodar cualquier diferencia en sus respectivas temporizaciones. Es por esta razón que PDH es denominada plesiócrona, porque no es exactamente síncrona.

La justificación, o la inserción de bits para resolver la ausencia de información que se produce en ciertos momentos debido a diferencias de reloj resuelve algunos problemas, como el de la sincronización entre equipos terminales, pero también introduce otros. De estos problemas, uno de los más importantes, por lo menos cuando se considera el diseño de esta tecnología, es la necesidad de identificar el inicio de una nueva trama.

Una vez que este inicio ha sido localizado, y dado que ya se conoce como es la estructura de trama, es un procedimiento sencillo desmapear y extraer toda la información transportada en ese nivel. Para realizar estas tareas se han desarrollado lo que se denominan Multiplexores de Inserción y Extracción **ADM** (*Add-Drop Multiplexer*), equipos que permiten añadir o sustraer cualquier señal hasta el nivel de detalle requerido.

Ello incrementa el costo de la totalidad de la red PDH, dado que las líneas de transporte tienden a ser de la más alta velocidad posible, y que los circuitos a extraer serán, naturalmente, los de velocidad más baja, que son los que la inmensa mayoría de usuarios demandan.

Otro factor a tener en cuenta es la dificultad de realizar una correcta monitorización del estado de los enlaces, dado que es realmente difícil extraer e interpretar las señales de alarma. Ello hace más complicado reducir problemas en la red y corregir funcionamientos incorrectos.

#### 1.5.1.3 Alineamiento de Trama

PDH, a cualquier nivel, es una tecnología de transmisión estructurada, y por lo tanto cada bit tiene un significado y una función. Para una correcta comprensión de cada bit es necesario tener una indicación del inicio de la trama. Para que el receptor de la trama básica E1 pueda reconocer el inicio de la trama una estructura de bits especial se inserta en el inicio de algunas tramas. De esta forma se realiza la sincronización. Una señal de alineamiento de trama **FAS** (*Frame Aligment Signal*) se introduce en el principio de las tramas pares, esto es, una FAS se introduce cada dos tramas E1. El byte restante en las tramas impares es denominado **NFAS** (No FAS) y es utilizado para el transporte de información de alarmas, bits sobrantes reservados para uso nacional y algunos más son bits de alineamiento de multitrama.

##### 1.5.1.3.1 FAS & CRC-4

Dentro del byte de FAS el primer bit se dedica a realizar un CRC-4, por lo tanto es necesario recibir 4 FAS para formar el código que permita el reconocimiento de una correcta sincronización y recepción de tramas. El resto de los bits de la FAS, es decir los bits del 1 al 7, siempre forman la combinación 0011011, lo que permite identificar el inicio de la nueva trama.

La trama E1 completa, a la que se denomina **Multitrama**, esta formada por 16 tramas básicas, con una duración cada una de ellas de 125 μs. Por lo tanto, la multitrama tiene una duración total de 2 ms. La multitrama misma, se divide en dos submultitramas, cada una consta de 8 tramas básicas. Es sobre esas 8 tramas que el CRC-4 es calculado, y su CRC es enviado sobre los primeros bits de las tramas pares de la siguiente submultitrama.

En el lado de recepción, el CRC-4 es calculado de la submultitrama ya recibida y comparado con el CRC-4 recibido en la siguiente submultitrama para realizar la inspección. En caso de que un error sea detectado, una alarma será señalizada hacia el emisor a través de otra trama viajando en el sentido contrario. Este método, CRC-4, para la detección de errores es una buena opción para tasas de bit erróneos **BER** (*Bit Error Rate*) mejores de 10E-3, dado que para mayores valores de BER podrían dañar los bits de CRC. La gran ventaja del

método de CRC es que todos los bits son monitorizados y no solo algunos bits, como se hace con otras técnicas.

#### 1.5.1.4 Tratamiento de Errores

Los errores de transmisión son monitorizados y comunicados, y si la red proporciona un rendimiento demasiado bajo, se toman las medidas necesarias para corregirla. La corrección y recuperación de errores se deja para la capa de enlace en el modelo OSI, y PDH únicamente se ocupa de una parte de la capa física.

#### 1.5.1.5 Canal de Señalización y Multitrama

El *slot* número 16 de cada trama básica de 2 Mbps se reserva para el transporte de protocolos de señalización para los 30 canales de 64 Kbps que llegan directamente a los usuarios de la red telefónica. Por esta razón, los multiplexores de la red deben modificar la información de señalización de los canales.

Cada canal tiene asignado un espacio de señalización de 2 Kbps en la multitrama E1, a través de 4 bits (conocidos genéricamente como a, b, c y d) en el canal 16, que constituye un canal de señalización de 64 kbps. Para realmente conocer donde esta el inicio de este canal de señalización, los primeros cuatro bits son marcados como cero (0000), y los siguientes cuatro bits de este byte no transportan información de señalización, sino información de justificación y alarmas. Estos cuatro primeros bits son los denominados **MFAS** (*Multiframe FAS*) mientras que los siguientes cuatro bits se denominan **NMFAS** (no señal de alineamiento de multitrama).

#### 1.5.1.6 Administración de Alarmas

Para la transmisión de alarmas, PDH hace uso de los campos NFAS y NMFAS. Cuando un multiplexor de inserción y extracción **ADM** (*Add Drop Multiplexer*) detecta una disminución en la calidad de transmisión, o porque el nivel de error es demasiado alto o porque un desalineamiento de trama ha sido detectado, debe comunicar este hecho al otro extremo de la conexión, esto es, al transmisor. Esta alarma es comunicada en el bit 3 de la NFAS y normalmente se denomina **Indicador de Alarma Remota**.

Entonces, el multiplexor remoto considera si la situación es peligrosa, y procede a realizar un realineamiento de trama. Este realineamiento se realiza poniendo toda la tributaria a uno ('1'), esto es, todos los contenidos de los canales a 1, para facilitar la resincronización, pero manteniendo la palabra FAS en su correcto valor.

Un procedimiento similar es efectuado por la señal de NMAS. Cuando el receptor pierde el sincronismo de multitrama, envía hacia atrás una alarma en el sexto bit del primer byte del canal 16 (el dedicado a la información de señalización). Esta alarma es denominada AIS64, o señal de indicación de alarma. De esta forma, el multiplexor indica que puede recuperar la información de los canales, pero no la información de señalización, ni los bits de CRC.

#### 1.5.1.7 Justificación de Tramas

Debido a diferencias entre los relojes respectivos de los multiplexores, es necesario implementar un mecanismo para adaptar las diferentes velocidades de bit y de esta forma garantizar la correcta transmisión de las tributarias sin *slips* (deslizamientos) ni fallos. Con este fin, algunos bits en los niveles altos pueden dejarse desocupados, y ser llenados selectivamente con información o simplemente con bits de relleno.

Para conocer cuando estos bits están transportando información o no, existen también algunos bits de control distribuidos en la trama que sirven de indicación. Utilizando un sistema de decisión por mayoría, para evitar errores, estos bits de control obligan al multiplexor a ignorar ese bit cuando no contiene información, o incorporarlo a la tributaria que esta siendo demultiplexada. De hecho en la jerarquía de transmisión PDH, la justificación significa dejar cierto bit que normalmente esta lleno desocupado. Esto se denomina justificación positiva.

#### 1.5.1.8 Arquitectura de Multiplexado

Desde el nivel primario a 2 Mbps hacia arriba, cada nivel en la jerarquía se compone de 4 tributarias del nivel inmediatamente inferior, donde cada nivel proporciona capacidad de transporte y justificación para cada una de ellas.

La conmutación en PDH es sólo posible si previamente se demultiplexa la portadora hasta el nivel requerido de conmutación, por lo tanto se puede deducir que el nivel de transporte básico es el de 2 Mbps y que esta señal tendrá una estructura diferente de las otras (8, 34 y 140 Mbps).

La trama de 2 Mbps transporta 30 canales de voz y 2 canales adicionales para funciones de entramado y señalización. Está estructurada sobre la trama básica de 125 μs, que contiene 32 canales de 64 Kbps, o *slots* temporales. El *slot* 0 siempre se utiliza para control específico de la trama: CRC, alineamiento de trama, alineamiento de submultitrama, señalización de alarmas y detección de errores de bit, mientras el slot 16 se utiliza para señalización asociada a los canales (CAS). Cada ocho tramas de 125μs se consideran una submultitrama, porque el control de CRC se genera para cada submultitrama (una submultitrama transporta la información de CRC-4 de su precedente), y dos submultitramas componen la multitrama completa, que consiste en 16 tramas básicas. Resulta fácil ver la razón principal de esta organización, el hecho es que se necesitan cuatro bits (un canal de señalización de 2 Kbps) para señalizar cada canal de 64 kbps, por lo tanto 15 bytes son necesarios para señalizar los 30 canales de voz, y un byte suplementario para proporcionar alineamiento de multitrama y bits de relleno.

*Primer nivel de Multiplexación: 2 Mbps* (**E1**)

Empezando desde el primer nivel a 2 Mbps, todos los niveles superiores utilizan una estructura de trama similar con una señal de alineamiento de trama (FAS) en el inicio de la trama. Debido al hecho de que una señal de nivel superior es construida multiplexando cuatro señales del nivel inmediatamente inferior, que son multiplexadas bit a bit, no es posible extraer una señal concreta sin demultiplexar completamente la señal de orden superior en la cual está completamente transportada.

*Segundo Nivel de Multiplexación: 8 Mbps* (**E2**)

Los 8 Mbps se dividen en cuatro bloques, que están separados por los bits de control de justificación. Los bloques segundo y tercero son idénticos, una multiplexación simple de las señales transportadas de 2 Mbps, mientras que el primer y cuarto bloques son diferentes.

El primer bloque contiene la palabra de FAS (1111010000), el bit A de alarma urgente (utilizado hacia atrás para señalizar eventos o problemas), los bits sobrantes S, reservados para uso nacional (a veces utilizados como alarma no urgente) y 20 bits de información.

El cuarto bloque contiene cuatro bits de justificación, para cada tributaria contenida en la señal de E2, y más bits de información. Como ya ha sido señalado, la justificación es positiva, esto significa que la justificación no contiene información la mayoría del tiempo. Para que el demultiplexor sepa cuando el bit de justificación contiene información o no, se utilizan los bits de control de justificación. Estos bits están distribuidos a lo largo de la trama para minimizar la probabilidad de que un error pueda modificar a dos de ellos, y la decisión es tomada por mayoría.

*Tercer Nivel de Multiplexación: 34 Mbps* (**E3**)

La estructura de trama de la señal de 34 Mbps está definida en la recomendación G.751 de la ITU-T. En esta trama la estructura de multiplexación es idéntica a la utilizada en el nivel de 8 Mbps.

*Cuarto Nivel de Multiplexación: 140 Mbps* (**E4**)

La estructura de trama de la señal E4, está definida en la recomendación G.751 de la ITU-T. En este caso, pueden verse 6 bloques diferentes, mientras, en los otros niveles, únicamente el primer y el último bloque eran diferentes. La palabra de alineamiento de trama es también diferente: 111110100000

### 1.5.2 SDH

La Jerarquía Digital Síncrona **SDH** (*Synchronous Digital Hierarchy*) es un estándar para redes de telecomunicaciones de alta velocidad y alta capacidad, específicamente es un sistema de transporte digital síncrono.

En todo sistema de transmisión digital, la sincronización debe garantizarse en tres niveles diferentes. Para transmisión PCM los niveles son: bit, intervalo de tiempo y trama.

Para transmisión de datos existen 2 técnicas:

**Transmisión Asíncrona**: Cuando los datos viajan por el canal sin una velocidad fija, es decir que el tiempo que transcurre desde la transmisión de un dato, hasta la transmisión del próximo dato es variable.

**Transmisión Síncrona**: En este caso los datos son transmitidos a una velocidad fija de bits, por una línea que se mantiene activa aun cuando no se esté enviando información. En los sistemas PCM la transmisión es siempre síncrona pues el receptor deriva su propia temporización de la señal entrante, mientras los alineamientos de intervalo y de trama se obtienen utilizando un formato predeterminado.

SDH es un sistema de transporte digital síncrono diseñado para proveer una infraestructura de redes de telecomunicaciones más simple, económica y flexible que PDH.

Como las velocidades de transmisión de PDH no son las mismas para EEUU y Japón que para Europa y otros países, la operación entre redes de ambos tipos es compleja y costosa. Además si se tiene en cuenta que para poder llegar a un canal de 64 Kbps (canal de voz), hay que demultiplexar toda la señal PDH, hasta llegar al canal mismo, se usa una cadena de multiplexores y demultiplexores, lo que representa un incremento de costo. En un principio el objetivo de la jerarquía SDH era superar las desventajas inherentes a los sistemas PDH, así como también normalizar las velocidades superiores a 140Mbps que hasta el momento eran propietarias de cada compañía.

#### 1.5.2.1 Aspectos Generales de SDH

Características que ofrece:

- Acceso directo a afluentes de baja velocidad sin tener que demultiplexar toda la señal que viene a alta velocidad, como ocurre con PDH.
- Facilidad de multiplexación y demultiplexación.
- Mejor capacidad de operación, administración y mantenimiento.
- Adopción de canales auxiliares estandarizados.
- Estandarización de interfaces.
- Fácil crecimiento hacia velocidades mayores, en la medida que lo requiera la red.
- Implementación de sistemas con estructura flexible que pueden ser utilizados para construir nuevas redes (incluyendo LAN, MAN, ISDN).

La tecnología SDH, ofrece las siguientes ventajas:

- Altas velocidades de transmisión: Los sistemas SDH logran velocidades de varios Gbps. SDH es una tecnología adecuada para los *backbones*.
- Función simplificada de inserción/extracción: Comparado con los sistemas PDH tradicionales, con SDH es mucho más fácil extraer o insertar canales de menor velocidad en las señales compuestas SDH de alta velocidad. No es necesario demultiplexar y volver a multiplexar la estructura plesiócrona, procedimiento complejo y costoso. Esto se debe a que en la jerarquía SDH todos los canales están perfectamente identificados por medio de una especie de “etiquetas” que hacen posible conocer exactamente la posición de los canales individuales.

- Alta disponibilidad y grandes posibilidades de ampliación: La tecnología SDH permite reaccionar rápida y fácilmente frente a las demandas de los usuarios. Empleando un sistema de gestión de redes de telecomunicaciones, el administrador de la red puede usar elementos de redes controlados y monitorizados desde un lugar centralizado.
- Fiabilidad: Las redes SDH incluyen varios mecanismos automáticos de protección y recuperación ante posibles fallos del sistema. Un problema en un enlace o en un elemento de la red no provoca el colapso de toda la red. Estos circuitos de protección se controlan mediante un sistema de gestión.
- Interconexión: Las interfaces SDH están normalizadas, lo que simplifica las combinaciones de elementos de redes de diferentes fabricantes. La consecuencia inmediata es que los gastos en equipamiento son menores en los sistemas SDH que en los sistemas PDH.

#### 1.5.2.2 Punteros

En la red síncrona todos los nodos y multiplexores SDH están controlados por un reloj muy estable. Sin embargo pueden surgir perdidas de sincronismo en alguna parte de la red o puede ser necesario efectuar algún ajuste en los puntos donde el tráfico traspasa las fronteras nacionales. Esta tarea de ajustar el sincronismo, se realiza mediante los punteros. Estos indican la posición en que comienza una carga útil. Como cada octeto de una trama STM, tiene un número que lo identifica, el puntero indica uno de tales números, y es donde se encontrara el primer octeto de la carga útil asociada a dicho puntero. De esta forma la carga útil puede flotar en una trama STM, pues siempre su posición estará indicada por el puntero.
En las señales SDH es una condición fundamental que antes de proceder a la multiplexación se efectúe la alineación de los punteros. Esto no significa que la señal sea retrasada ya que esto no es posible, la información contenida en el *payload* es información que debe ser transmitida en tiempo real, lo que se hace entonces, es cambiar el contenido del puntero reacomodando la posición a la cual debe apuntar (posición donde empieza el *payload*). Es decir que el *payload* tiene cierta libertad para deslizarse dentro del VC, siempre siendo apuntado por el puntero correspondiente.

#### 1.5.2.3 Trama STM-1

La jerarquía STM-1 es la de menor velocidad prevista para la transmisión a través de un enlace de SDH, es decir es la jerarquía básica.

La STM-1 tiene una estructura de trama que se conforma de 2430 bytes en serie, que por lo general se ilustran en forma de matriz para hacer más cómoda su representación, quedando entonces una estructura bidimensional de 9 reglones, con 270 bytes por reglón. Esta matriz es recorrida en izquierda a derecha, y en sentido descendente, para así ir siguiendo la secuencia en serie.

La duración de transmisión de cada trama es de 125μS, la cual corresponde a una frecuencia de repetición de trama de 8000 Hz. La capacidad de transmisión de un byte individual es de 64Kb/s.

La STM-1 está conformada por tres bloques: La *Section Over Head* (SOH), el puntero (PTR), y la carga útil (*Payload*).

#### 1.5.2.4 Contenedor C

Toda información útil, ya sea plesiócrona o síncrona, se coloca en contenedores antes de ser transmitida en una STM-1. El tamaño de los contenedores se indica en bytes, esta cantidad de bytes se pone a disposición como capacidad de transmisión en contenedores cada 125 μs. Los tamaños de los contenedores establecidos corresponden a las señales plesiócronas.

La información útil debe caber en estos contenedores, esto se logra mediante un relleno de bits y bytes, para el cual se emplea tanto el procedimiento de relleno positivo como el de relleno negativo-cero-positivo.

El contenedor contiene:

- Información útil (por ejemplo una señal PDH)

- Bytes y bits de relleno fijos (*fixed stuffing*) para la adaptación del reloj. Estos rellenos, son siempre Bytes (bits) sin información para adaptar la velocidad PDH aproximadamente a la velocidad del contenedor, que suele ser mayor. La adaptación más precisa se efectúa por medio de bits de relleno individuales.
- Bits de relleno para la adaptación precisa del reloj. Según sea necesario, estos bits pueden usarse como bits de información útil o bien como bits de relleno.

#### 1.5.2.5 Contenedor Virtual

A cada contenedor C se le agrega un encabezado de camino (POH), luego el contenedor junto con el POH correspondiente forman lo que se denomina contenedor virtual **VC** (*Virtual Container*), y se transporta como una unidad a través de una ruta en la red.

El POH consiste en información que sirve para transportar de manera confiable el contenedor desde el origen hasta el destino. El POH se agrega al formar el VC al principio de la ruta y se evalúa solo al final de ésta, en el momento que se descompone el contenedor, entonces el POH contiene información para la supervisión y mantenimiento de una ruta en la red.

| VC type | VC bandwidth | VC payload |
|---|---|---|
| VC-11 | 1664 kbit/s | 1600 kbit/s |
| VC-12 | 2240 kbit/s | 2176 kbit/s |
| VC-2 | 6848 kbit/s | 6784 kbit/s |
| VC-3 | 48 960 kbit/s | 48 384 kbit/s |
| VC-4 | 150 336 kbit/s | 149 760 kbit/s |
| VC-4-4c | 601 344 kbit/s | 599 040 kbit/s |
| VC-4-16c | 2 405 376 kbit/s | 2 396 160 kbit/s |
| VC-4-64c | 9 621 504 kbit/s | 9 584 640 kbit/s |
| VC-4-256c | 38 486 016 kbit/s | 38 338 560 kbit/s |

*Tipos de Contenedores Virtuales y Capacidad*

Un VC puede (según el tamaño) transmitirse en una trama STM-1 o bien, depositarse en un VC mayor, el cuál se transporta luego directamente en la STM-1. Se hace una distinción entre VC de orden superior HO (*Higher Order*), y VC de orden inferior LO (*Lower Order*). Se conocen como LO aquellos que se transmiten en contenedores más grandes. Por ejemplo, los VC11, VC12, VC2, son del tipo LOVC. El VC3 es un LOVC cuando es transmitido en un VC4. Los HO son aquellos que se transmiten directamente en la trama STM-1, por ejemplo el VC4 es un HOVC, esto es valido también para el VC3 que se transmite directamente en la trama STM-1

Una red basada en SDH proporciona los medios para transportar los contenedores entre diversos puntos, para cargar y descargar contenedores de los STM-1 y para transferir contenedores de un medio de transporte a otro (STM-N). Estas acciones determinan las funciones básicas que se deben realizar en una red SDH. En los puntos de acceso a la red se ensamblan los VC adecuados a la señal a transmitir, una vez conformado el VC debe ser transportado a través de la red, durante el viaje del VC por la red SDH puede presentarse el caso en que un VC o varios deben ser descargados del STM-1 o también casos en que deban ser cargados en los STM-1. En su recorrido por la red, el VC pasara por diferentes rutas y con diferentes velocidades.

#### 1.5.2.6 Unidad Administrativa

Los contenedores virtuales VC4 y VC3, son transmitidos directamente en la trama STM-1, en este caso los apuntadores de bloque (PTR AU) incorporados en la trama STM-1 contienen la relación de fase entre la trama y el VC respectivo. La parte de la trama dentro de la cuál puede deslizarse el VC se denomina **Unidad Administrativa**, también el puntero denominado PTR AU, forma parte de la AU.

En los primeros 9 bytes del cuarto renglón de la trama STM-1 están contenidos 3 punteros de 3 bytes cada uno. En la trama STM-1 pueden transmitirse, 1 x AU4, o bien 3 x AU3. La transmisión del VC3 puede

efectuarse directamente (AU3) en la STM-1 o indirectamente, en un AU4, por lo cual se depositan 3 VC dentro de un VC4.

### 1.5.2.7 Grupo de Unidades Administrativas

Varias AU pueden agruparse, es decir multiplexarse, por bytes para formar el llamado grupo AU (AUG). El grupo AUG es una unidad con sincronía de trama que corresponde al STM-1 sin la SOH. Agregando la SOH STM-1 al AUG se obtiene un STM-1. Un grupo AUG puede constar entonces, de 1 x AU4 ó de 3 x AU3.

### 1.5.2.8 Unidad Tributaria

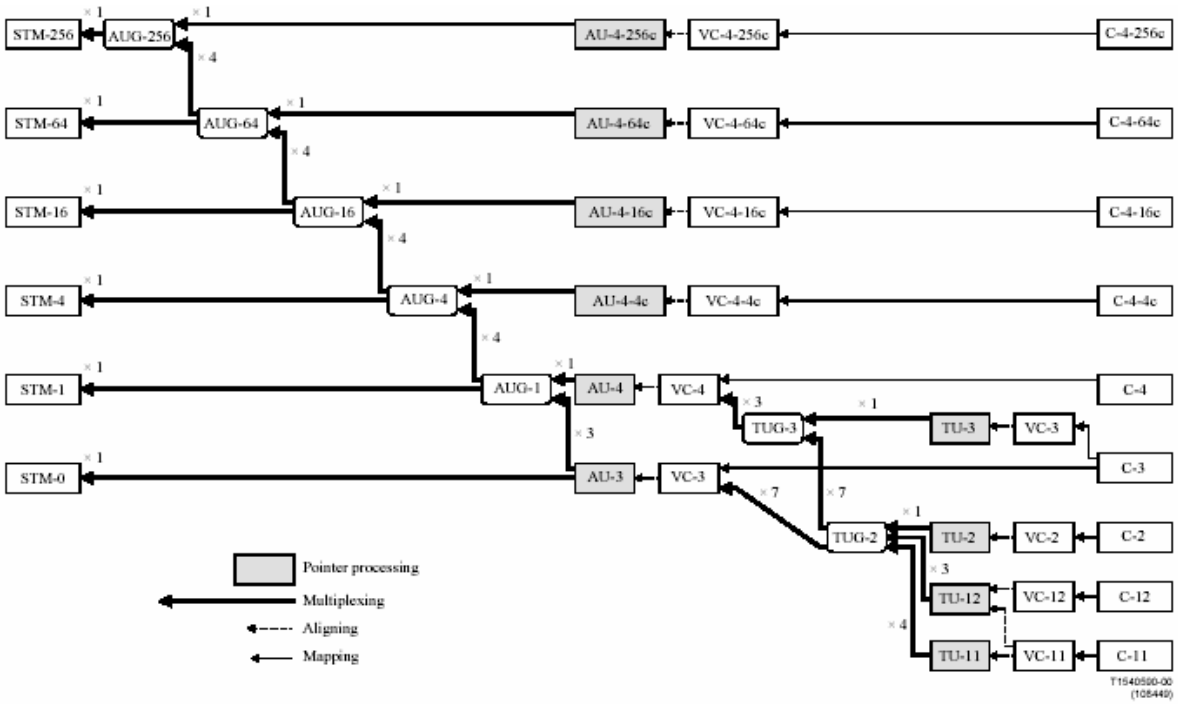
Todos los VC, excepto el VC4, pueden transmitirse dentro de la STM-1, depositados dentro de un VC más grande. El VC menor puede, por regla general, tener deslizamientos de fase dentro del VC mayor (de orden superior), a tal efecto el VC de orden superior debe tener incorporado un puntero que reduzca la relación de fase entre ambos VCs. Por Unidad Tributaria **TU** (*Tributary Unit*), se entiende la parte del contenedor de orden superior dentro del cual puede deslizarse el LOVC incorporado, más el puntero correspondiente (PTR-TU).

### 1.5.2.9 Grupo de Unidades Tributarias

Antes de ser depositadas en un contenedor de orden superior, las TU se agrupan, es decir, se concatenan por bytes, y los grupos resultantes se denominan TUG (Grupo de Unidades Tributarias).

### 1.5.2.10 Estructura de Multiplexación

A continuación se muestra la estructura de multiplexación de SDH




*Estructura de Multiplexación de SDH*

### 1.5.2.11 Sincronización

SDH es una jerarquía digital síncrona y es muy importante que sea realmente síncrona. Si no se garantiza la sincronización puede producirse una degradación considerable en las funciones de la red e incluso el fallo total de la red. Para evitarlo todos los elementos de la red deben estar sincronizados respecto a un reloj central, generado mediante un reloj de referencia primario (PRC) de alta precisión conforme a la recomendación G.811 de la UIT. Esta señal de reloj debe distribuirse por toda la red. Para ello se recurre a una estructura jerárquica, siendo las unidades de sincronización (SSU) y los relojes de equipos síncronos (SEC) quienes transfieren la señal. Las señales de sincronización circulan por los mismos circuitos que las comunicaciones SDH.

La señal de reloj se regenera en las SSU y en los SEC. Si falla la fuente de reloj, el elemento afectado conmuta a otra fuente de reloj de igual o menor calidad o, si esto no fuera posible, pasa al modo de *holdover* (se mantiene con la señal de reloj regenerada). En esta situación, la señal de reloj se mantiene relativamente precisa controlando el oscilador aplicando valores de corrección de frecuencia almacenados durante las últimas horas y teniendo en cuenta la temperatura del oscilador.

Deben evitarse estas situaciones ya que, con el transcurso del tiempo, podrían llevar a la pérdida del sincronismo y al fallo total de la red. Los *holdovers* se evitan comunicando a los elementos de la red con la ayuda de mensajes de estado de sincronización (SSM). El SSM informa al elemento vecino sobre el estado de la fuente de reloj utilizada para generar la señal por este recibido y es parte de la cabecera de sección de multiplexación. Los *gateways* o puentes entre redes con fuentes de reloj independientes plantean algunos problemas especiales. Los elementos de redes SDH pueden compensar desplazamientos de reloj hasta ciertos límites mediante operaciones con punteros.

#### 1.5.2.12 Gestión y Mantenimiento.

Para los propósitos de la red de gestión y mantenimiento, la red de SDH puede ser descrita en función de tres diferentes sectores dentro de la red. Estas son la *Multiplexer Section Overhead* (MSOH), *Regenerator Section Overhead* (RSOH), y *Path Overhead* (POH).

***Multiplexer Section Overhead***

Esta sección está destinada a transferir información entre los elementos regeneradores. Es decir estos regeneradores tendrán acceso a la información que viene en los bytes del ROH, la sección regeneradora contiene una estructura de 12 bytes.

Las funciones básicas de esta sección son las siguientes:

- Chequeo de paridad
- Alineación de la trama
- Identificación de la trama STM-1
- Canales destinados a los usuarios (sin fines específicos)
- Canales de comunicación de datos
- Canales de voz

***Multiplexer Section Overhead***

Esta sección provee las funciones necesarias para monitorear y transmitir datos de la red de gestión entre elementos de red. Las funciones básicas de esta sección son las siguientes:

- Chequeo de paridad
- Punteros del *payload*

- Conmutación automática a la protección
- Monitoreo de canales de comunicación de datos
- Monitoreo de canales de voz

***Path Overhead***

Esta sección esta construida por nueve bytes, los cuales ocupan la primera columna de la STM-1, los mismos están destinados a manejar toda la información concerniente al camino por el cuál circulará la comunicación. Las funciones básicas de esta sección son las siguientes:

- Mensajes de la trayectoria de camino
- Chequeo de paridad
- Estructura del contenedor virtual
- Alarmas e información de presentación
- Indicación de multitrama para las unidades tributarias
- Conmutación por protección de camino

**1.5.2.13 Jerarquías de Multiplexación SDH.**

Las velocidades de bit para los niveles más altos de las jerarquías SDH van de acuerdo al nivel N del Modulo de Transporte Síncrono (STM). Según la recomendación G.707 del CCITT estas velocidades son:

| Nivel | Señal | Velocidad (Mbps) | Velocidad Real |
|---|---|---|---|
| 0 | STM_0 | 51.840 | 51.840 Mbps |
| 1 | STM_1 | 155.520 x 1 | 155.520 Mbps |
| 4 | STM_4 | 155.520 x 4 | 622.080 Mbps |
| 16 | STM_16 | 155.520 x 16 | 2.488 320 Gbps |
| 64 | STM_64 | 155.520 x 64 | 9.953 280 Gbps |
| 256 | STM_256 | 155.520 x 256 | 39.813 120 Gbps |

*Jerarquías SDH*

A diferencia de la jerarquía digital plesiocrona (PDH), aquí la velocidad del STM_N se obtiene multiplicando la velocidad del modulo básico STM_1, por N, donde N es un entero.

**1.5.3 ATM**

**1.5.3.1 Funcionamiento de ATM**

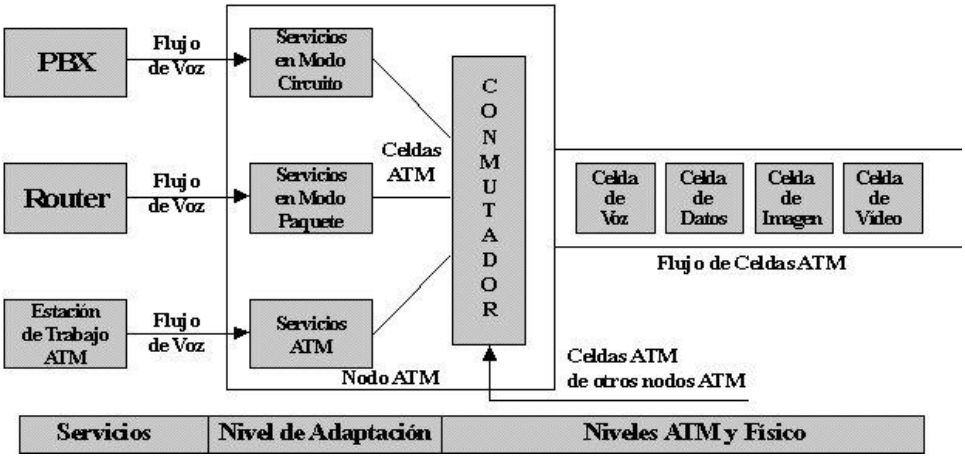
ATM (*Asynchronous Transfer Mode*) se basa en el concepto de Conmutación Rápida de Paquetes (*Fast Packet Switching*) en el que se supone una fiabilidad muy alta a la tecnología de transmisión digital, típicamente sobre fibra óptica, y por lo tanto no necesita recuperación de errores en cada nodo. Ya que no hay recuperación de errores, no son necesarios los contadores de número de secuencia de las redes de datos tradicionales, tampoco se utilizan direcciones de red ya que ATM es una tecnología orientada a conexión, en su lugar se utiliza el concepto de Identificador de Circuito o Conexión Virtual **VCI** (*Virtual Container Identifier*).

El tráfico con tasa de bits o velocidad binaria constante **CBR** (*Constant Bit Rate*), por ejemplo la voz o el vídeo no comprimido, tradicionalmente es transmitido y conmutado por redes de conmutación de circuitos o multiplexores por división en el tiempo (TDM), que utilizan el Modo de Transmisión Síncrono **STM**. En STM, los multiplexores por división en el tiempo dividen el ancho de banda, que conecta dos nodos, en contenedores temporales de tamaño pequeño y fijo llamados *Time Slots* (ranuras de tiempo). Cuando se establece una conexión, esta tiene estadísticamente asignado un *slot* (o varios) y el ancho de banda asociado con este *slot* está reservado para la conexión haya o no transmisión de información útil. Una pequeña cantidad de ancho de banda para control se utiliza para la comunicación entre los conmutadores, de forma que estos conocen los *slots* que tiene asignados la conexión. Esto se conoce como direccionamiento implícito. El conmutador receptor sabe a que canales corresponden los *slots* y por lo tanto no se requiere ningún

direccionamiento adicional. Este procedimiento garantiza la permanente asignación de un ancho de banda durante el tiempo que dura la llamada, así como un tiempo de retardo pequeño y constante, sin embargo implica un desperdicio de ancho de banda.

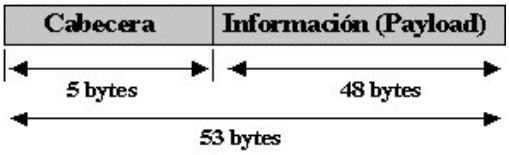
En contraste, los datos son normalmente transmitidos en forma de tramas o paquetes de longitud variable, lo que se adecua bien a la naturaleza de ráfagas de este tipo de información, ya que solo se transmiten paquetes cuando es necesario permitiendo que otros usuarios usen el ancho de banda cuando no se transmite información. Sin embargo, este mecanismo de transporte tiene retardos impredecibles, la latencia tiende a ser alta y en consecuencia la conmutación de paquetes no es adecuada para tráfico con tasa de bits constante como la voz. Tampoco la conmutación de circuitos se adecua para la transmisión de datos, ya que si se asigna un ancho de banda durante todo el tiempo para un tráfico en ráfagas se desperdicia mucho ancho de banda cuando este no se utiliza.

ATM ha sido definido para soportar de forma flexible, la conmutación y transmisión de tráfico multimedia como datos, voz, imágenes y vídeo. En este sentido, ATM soporta servicios en modo circuito, similar a la conmutación de circuitos, y servicios en modo paquete, para datos.




*Funcionamiento de un Nodo ATM*

Sin embargo, a diferencia de la conmutación de circuitos, ATM no reserva *slots* para la conexión. En su lugar, una conexión obtiene *slots* o celdas, solo cuando está transmitiendo información. Cuando una conexión está en silencio no utiliza *slots* o celdas, estando estas disponibles para otras conexiones. Con esta idea en mente, se decidió que la unidad de conmutación y transmisión fuese de tamaño fijo y longitud pequeña. Esta unidad es conocida como **Celda**, y tiene una longitud de **53 bytes** divididos en 5 de cabecera y 48 de información o carga útil. Esta celda sustituye al *time slot* de una red TDM



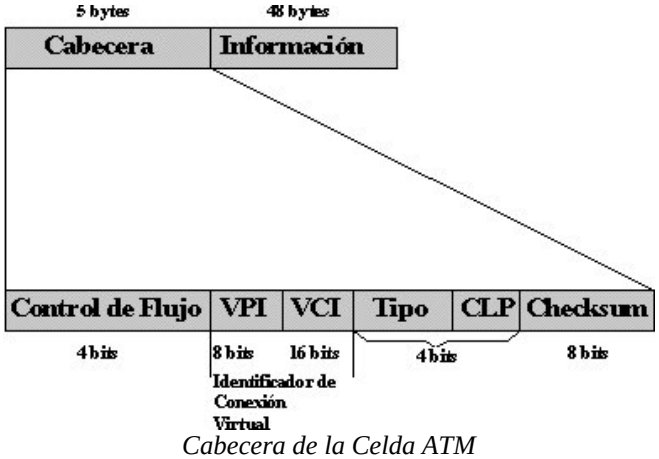

**Longitud fija: 53 bytes**
**Tamaño pequeño**

*Formato de Célula*

Las celdas pequeñas y de longitud constante son ventajosas para tráfico con tasa de bits constante (voz y vídeo por ejemplo) y son muy útiles en general ya que permiten un tiempo de latencia muy bajo, constante y predecible, así como una conmutación por hardware a velocidades muy elevadas. También, en el caso de pérdida de celdas por congestión o corrupción, la pérdida no es muy grande y en muchos casos es remediable o recuperable. De hecho, el tráfico de voz y vídeo, no es muy sensible a pequeñas pérdidas de información, pero si es muy sensible a retardos variables, sucediéndole lo contrario al tráfico de datos.

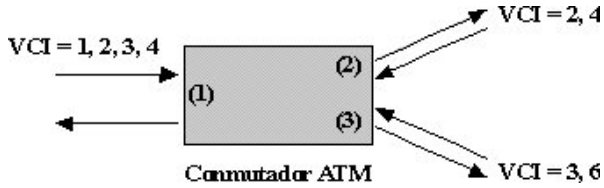
En una red ATM, donde las celdas no están reservadas sino asignadas bajo demanda, el conmutador receptor no puede determinar por adelantado a que canal corresponde cada celda. La Celda ATM a diferencia del *Time Slot* en TDM, debe transportar la identificación de la conexión a la que pertenece, de esta forma no existirán celdas vacías ya que serán utilizadas por conexiones pendientes. Esta es una diferencia fundamental de ATM frente TDM. La cabecera presente en cada celda, consume aproximadamente un 9.5% del ancho de banda, siendo este el precio que hay que pagar por la capacidad para disponer de ancho de banda bajo demanda, en lugar de tenerlo permanentemente reservado y eventualmente desperdiciado.

La adopción de una cabecera de 5 bytes ha sido posible, porque no se realiza recuperación de errores en los nodos intermedios, tampoco se emplean direcciones válidas a nivel de toda la red, tales como la dirección MAC en Ethernet o IP en redes tipo TCP/IP



*Cabecera de la Celda ATM*

Al igual que en las redes de conmutación de paquetes, la tecnología ATM está **Orientada a Conexión**. Esto significa que antes de que el usuario pueda enviar celdas a la red, es necesario realizar una llamada y que esta sea aceptada para establecer una **Conexión Virtual** a través de la red. Durante la fase de llamada un Identificador de Conexión Virtual **VCI** es asignado a la llamada en cada nodo de intercambio a lo largo de la ruta.



*Identificador de Conexión Virtual (VCI)*

El identificador asignado, sin embargo, solo tiene significado a nivel del enlace local, y cambia de un enlace al siguiente según las celdas pertenecientes a una conexión pasan a través de cada conmutador ATM. Esto significa, que la información de enrutamiento (*routing*) transportada por cada cabecera puede ser relativamente pequeña.

Asociado con cada enlace o puerto entrante del conmutador ATM, hay una tabla de enrutamiento que contiene el enlace o puerto de salida y el nuevo VCI que va a ser utilizado en correspondencia a cada VCI entrante.

| VCI-in | Enlace 1 R-T | |
|---|---|---|
| | Salida | VCI |
| 1 | 2 | 2 |
| 2 | 2 | 4 |
| 3 | 3 | 3 |
| 4 | 3 | 6 |
| . | . | . |
| . | . | . |
| . | . | . |

| VCI-in | Enlace 2 R-T | |
|---|---|---|
| | Salida | VCI |
| | . | . |
| | . | . |
| 2 | 1 | 1 |
| | . | . |
| | . | . |
| 4 | 1 | 2 |
| . | . | . |
| . | . | . |
| . | . | . |

| VCI-in | Enlace 3 R-T | |
|---|---|---|
| | Salida | VCI |
| | . | . |
| | . | . |
| 3 | 1 | 3 |
| | . | . |
| | . | . |
| 6 | 1 | 4 |
| . | . | . |
| . | . | . |
| . | . | . |

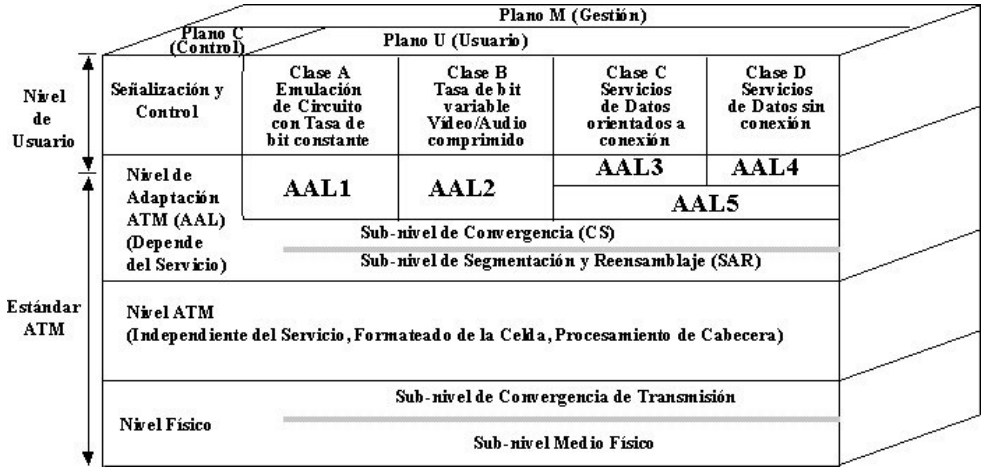
*Tablas de enrutamiento*

De este modo el enrutamiento de celdas en ambas direcciones a lo largo de la ruta es extremadamente rápido, ya que consiste en una simple operación de consulta en una tabla. Como resultado, las celdas procedentes de cada enlace pueden ser conmutadas independientemente a velocidades muy altas. Esto permite el uso de arquitecturas de conmutación paralelas y circuitos de alta velocidad hasta Gbps, cada uno operando a su máxima capacidad. Celdas procedentes de diferentes fuentes son multiplexadas juntas de forma estadística a efectos de conmutación y transmisión.

Un conmutador ATM podría describirse como una caja que mantiene en su interior una gran cantidad de ancho de banda, siendo este recurso cedido o recuperado dinámicamente según el aumento o disminución de las necesidades. En este sentido, se dice que ATM proporciona ancho de banda bajo demanda.

### 1.5.3.2 Modelo de Referencia ATM

El modelo de referencia está constituido por tres niveles: Nivel Físico, Nivel ATM y Nivel de Adaptación ATM (AAL)




*Modelo de Referencia ATM*

Las funciones han sido divididas en tres grupos conocidos como planos: El plano C de control y señalización, el plano U de usuario y el plano M de gestión. Los protocolos del plano C se encargan de la señalización, es decir, del establecimiento, mantenimiento y cancelación de conexiones virtuales. Los protocolos del plano U dependen de la aplicación y en general operan extremo a extremo (usuario a usuario). Los protocolos del plano M se encargan de la Operación, Administración y Mantenimiento (OAM). Los protocolos de los tres planos hacen uso de los servicios ofrecidos por los tres niveles ATM.

#### 1.5.3.2.1 Nivel Físico

Define las interfaces físicas, los protocolos de trama y codificación para la red ATM. Cada conexión física al conmutador ATM es un enlace dedicado y todos los enlaces pueden estar simultáneamente activos. Los

conmutadores ATM están diseñados para permitir a todos los puertos comunicarse transparentemente e independiente de la velocidad física. Esto permite que la conexión física esté acoplada con los requerimientos de ancho de banda del dispositivo conectado. La conversión de velocidad es una característica inherente de ATM, tampoco tiene restricciones topológicas de las redes clásicas tales como Ethernet.

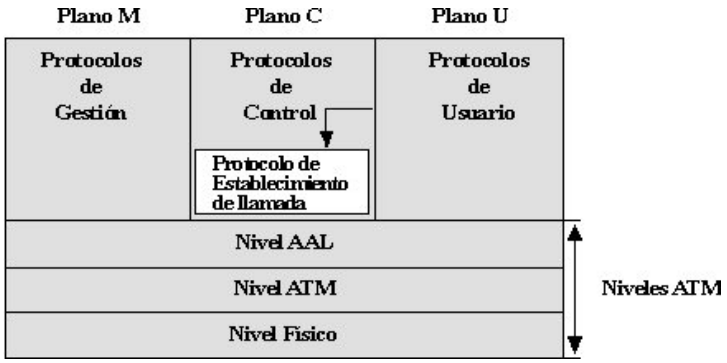
El nivel físico **PHY**, proporciona al nivel ATM los medios para transportar celdas ya configuradas. Este nivel está dividido en dos subniveles: el subnivel de Convergencia de Transmisión **TC**, y el subnivel dependiente del Medio Físico **PM**. La selección del medio físico determina la operación de ambos subniveles. El subnivel PM para cada medio, define cosas tales como formas de onda, ordenación de los bits, codificación en línea, recuperación del reloj, sincronización, etc. Además, para tráfico con temporización relacionada, proporciona información de temporización al nivel de Adaptación ATM **AAL**.

El subnivel TC es la clave para que la celda ATM viaje libremente sobre una amplia variedad de medios. El subnivel TC empaqueta las celdas ATM salientes en la estructura de trama del medio de transmisión, rellenando con celdas nulas según se necesite. A la recepción, el subnivel TC determina los contornos de las celdas, extrayéndolas del flujo de bits, descartando celdas nulas o erróneas y finalmente entregándolas al nivel ATM.

**1.5.3.2.2 Nivel ATM**

Este es el nivel de conmutación y transmisión de ATM. Define la estructura de la cabecera de la celda, y como las celdas fluyen sobre las conexiones lógicas en la red ATM. Realiza las funciones de multiplexación estadística de celdas procedentes de diferentes conexiones, y su enrutamiento sobre las conexiones virtuales. Las conexiones lógicas en el nivel ATM, están basadas en el concepto de Camino Virtual (*Virtual Path*) y Canal Virtual (*Virtual Channel*). Una Conexión de Camino Virtual **VPC** (*Virtual Path Connection*) es una colección de Conexiones de Canal Virtual **VCC** (*Virtual Channel Connection*) tributarios que son transportados a lo largo del mismo camino o ruta. Un conmutador de tránsito podría reaccionar únicamente a la información de camino (VPC), mientras que los conmutadores terminales reaccionarían a la información de fan-out (VCC), pudiéndose mapear diferentes sesiones contra VCIs sobre la misma conexión VPC.

Cada VPC o VCC puede estar establecido permanentemente, con lo que tendremos una Conexión Virtual Permanente (PVC), o establecido dinámicamente bajo demanda disponiéndose entonces, de una Conexión Virtual Conmutada **SVC** (*Switched VC*). Funciones de control y señalización asociadas con el plano C, y por lo tanto fuera del modelo de referencia ATM, permiten al usuario establecer y terminar dinámicamente VPCs y VCCs.

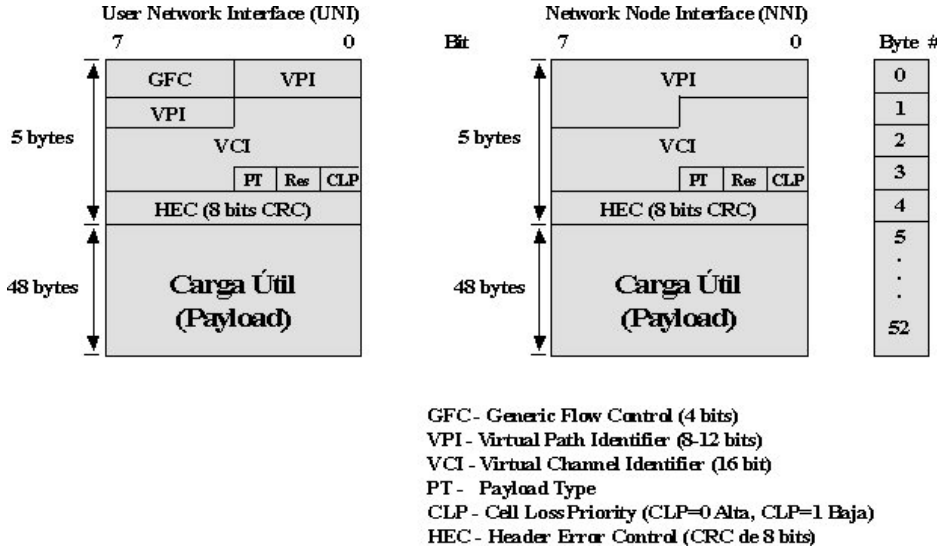



*Protocolos externos a ATM*

Dentro de una red ATM, el camino seguido por los mensajes de señalización es una conexión virtual específica conocida como Conexión de Canal Virtual para Señalización **SVCC**. Un descriptor de tráfico, o contrato usuario-red, define los parámetros y reglas de cada VPC y VCC. Están especificados descriptores de tráfico definiendo pico de tráfico **PCR**, longitud máxima de ráfagas **MBS**, tasa de bits media **SCR**, variación del retardo **CDVT**. El protocolo de control de la conexión negocia la clase de servicio específica y las características del ancho de banda de cada circuito virtual durante el establecimiento de la llamada. La red propaga esa petición internamente hasta su destino y verifica si los requerimientos exigidos se van a poder

cumplir. En caso afirmativo, la red acepta el circuito y a partir de ese momento, garantiza que el tráfico se va a tratar acorde a las condiciones negociadas en el establecimiento. Esto permite que cada circuito virtual sea adaptado para su uso específico, por ejemplo vídeo o paquetes de datos, siendo la calidad del servicio (**QoS**) una característica inherente de ATM.

Hay dos formatos diferentes para el encabezado o cabecera de las celdas




*Formatos UNI (User to Network Interface) y NNI( Network to Network Interface)*

El primero proporciona la conexión a la Red ATM desde un equipo terminal ATM o bien desde un sistema intermedio **IS** (*Intermediate System*) tal como un *hub*, un *gateway* (puente) o un enrutador que a su vez controla equipos de usuario final.

El segundo define la interfaz entre dos nodos ATM, cuando la NNI conecta nodos pertenecientes a distintas redes se denomina NNI-ICI (*NNI-Inter Carrier Interface*).

El campo Control de Flujo Genérico **GFC** (*Generic Flow Control*) tiene significado únicamente en este enlace y se incluye para asignar prioridades a las diferentes celdas, dependiendo del tipo de información que transportan, y que estas sean colocadas en diferentes colas de salida según su prioridad. No está presente dentro de la red, y en su lugar se amplia el campo VPI.

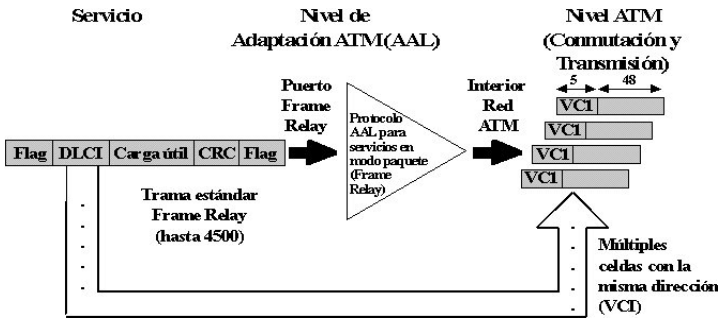
El campo Tipo de Carga útil **PT** (*Payload Type*) se utiliza para permitir que las celdas de los planos C y M, se distingan de las celdas conteniendo información de usuario, y también para informar de la existencia de congestión. El protocolo AAL5 utiliza un bit del campo PT para indicar el fin del mensaje **EOM** (*End of Message*) de una trama AAL5. El bit CLP permite que las celdas tengan una de dos prioridades: alta (CLP=0) y baja (CLP=1). Debido a que un conmutador ATM opera por multiplexación estadística de sus entradas, es posible que múltiples entradas compitan por una misma salida, dando lugar a que un buffer temporal se desborde en un enlace de salida de un nodo ATM. El bit CLP se utiliza para marcar aquellas celdas que en caso de congestión se puedan descartar primero. El campo HEC es un CRC de 8 bits solo para detección de errores en la cabecera, especialmente si el direccionamiento es correcto. Si falla, la celda es descartada. Si es correcto, se puede proceder inmediatamente a la conmutación. Celdas vacías también son descartadas y se caracterizan por que su VPI/VCI es cero.

**1.5.3.2.3 Nivel de Adaptación ATM (AAL)**

ATM ha sido definido para proporcionar un soporte de conmutación y transmisión flexible para tráfico multimedia. En consecuencia, es esencial que ATM soporte un rango de tipos de servicios alternativos. Excepto para aquellas aplicaciones que generan directamente celdas, el uso de la conmutación y transmisión

de celdas tiene que ser totalmente transparente al equipo del usuario. El nivel de Adaptación ATM, como su nombre indica, realiza las funciones de adaptación (convergencia) entre las clases de servicio proporcionadas al usuario, por ejemplo transportar tramas de datos entre dos LANs, y el servicio basado en celdas proporcionado por ATM.

Cuando una trama o flujo de bits, cualquiera que sea su origen (voz, datos, imagen o vídeo), entra en una red ATM, el nivel de Adaptación la segmenta en celdas. El proceso comienza inmediatamente cuando la primera parte de la trama entra en el conmutador de acceso a la red ATM, no hay que esperar hasta que la trama entera haya llegado.




*Servicios en modo paquete*

Las celdas generadas son enviadas a través de la red ATM a alta velocidad, por ejemplo a 622 Mbps. Durante la totalidad del proceso, hay únicamente un punto donde la trama completa podría estar almacenada: en el punto de salida de la red, sin embargo bastará que haya un número suficiente de celdas en el punto de salida para comenzar la entrega al usuario.

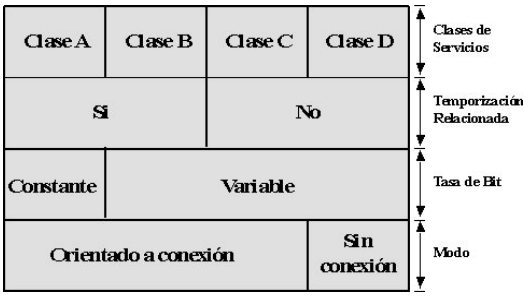
En los conmutadores intermedios, todas las celdas son despachadas tan rápidamente como llegan. De hecho, en el momento que la trama ha entrado totalmente en el conmutador de acceso a la red, la mayor parte de la trama estará ya en el puerto de destino, próxima a salir o saliendo de la red ATM. Esta tecnología evita el retardo de señalización causado por otras técnicas, que emplean la aproximación de almacenamiento de la trama y su posterior envío. También la utilización de celdas de tamaño pequeño y fijo, permite el intercalado y priorización de celdas en los *buffers* de salida de los conmutadores ATM, reduciéndose la sensibilidad a la congestión.

AAL soporta cuatro tipos de servicios: Clases A, B, C y D. Hay cuatro tipos de AAL: AAL1 y AAL2 que soportan las clases A y B respectivamente, mientras que las clases C y D están indistintamente soportadas por AAL3/4 ó AAL5. El protocolo AAL5 es una versión más sencilla y eficiente de la AAL 3/4, soportando las clases de servicio C y D para datos de alta velocidad. El nivel AAL realiza funciones de Segmentación y Reensamblado (SAR) para mapear la información de niveles superiores, al campo de Carga Útil del la celda. Otras funciones de AAL son el control y recuperación de la temporización para las clases de servicio A y B, así como la detección y manejo de celdas perdidas o fuera de secuencia.

**1.5.3.3 Clases de Servicios**

Los servicios han sido clasificados de acuerdo con tres criterios:

- La existencia de una temporización relacionada entre los usuarios origen y destino (por ejemplo voz).
- La tasa de bits, o velocidad binaria asociada con la transferencia (constante/CBR o variable/VBR).
- El modo de conexión (con conexión o sin conexión).




*Servicios proporcionados por ATM*

Los servicios en clase A y B están orientados a conexión y existe una temporización relacionada entre los usuarios origen y destino. La diferencia entre las dos clases, es que la clase A proporciona un servicio con tasa de bits constante, mientras que en la clase B la tasa de bits es variable. Un ejemplo del uso de la clase A, es la transferencia de un flujo constante de bits asociada con una llamada de voz, por ejemplo a 64 Kbps. La clase A es también conocida, como Emulación de Circuito Conmutado.

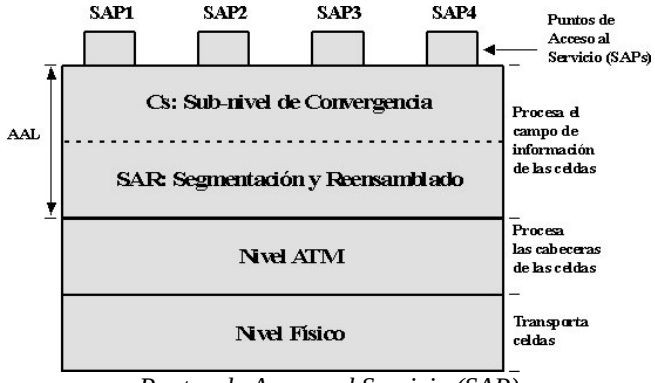
Un ejemplo de uso de la clase B, es la transmisión de un flujo de bits variable asociado con vídeo comprimido. Aunque el vídeo produce tramas a velocidad constante, un *codec* de vídeo produce tramas conteniendo una cantidad variable de datos comprimidos.

Las clases C y D no tienen temporización relacionada entre el origen y el destino. Ambas proporcionan servicios en modo paquete, con velocidad binaria variable entre origen y destino. La clase C está orientada a conexión y la clase D es sin conexión.

Para realizar las funciones anteriores, el nivel AAL está dividido en dos subniveles:

- El Subnivel de Convergencia (CS), que realiza las funciones de convergencia entre el servicio ofrecido al usuario y el proporcionado por el nivel ATM.
- El Subnivel de Segmentación y Reensamblado (SAR), que realiza las funciones de ensamblado/segmentación de los datos de origen para colocarlos en el campo de información de la celda y la correspondiente función de desensamblado/reensamblado en el destino.

Asociada con cada clase de servicio está un tipo de Punto de Acceso al Servicio (SAP) y un protocolo asociado. Clase A tiene un SAP de tipo 1, clase B de tipo 2 y así sucesivamente



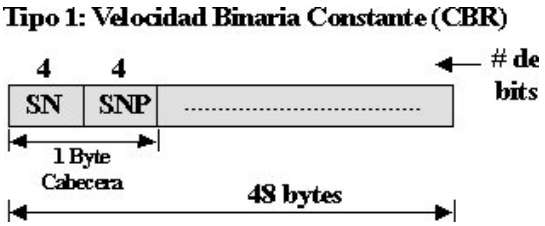

*Puntos de Acceso al Servicio (SAP)*

Los cuatro tipos o clases de servicios utilizan los 48 bytes del campo de carga útil en cada celda de forma diferente, pudiendo opcionalmente contener un campo de hasta 4 bytes para adaptación ATM.

**1.5.3.3.1 Tipo 1: Velocidad Binaria Constante (CBR)**

En este tipo de servicio, el protocolo de AAL1 se esfuerza en mantener un flujo con tasa de bits constante entre los SAPs de origen y destino (entrega sincronizada). La velocidad binaria está en el rango de pocos Kbps, por ejemplo para voz comprimida, a decenas de Mbps, por ejemplo en video no comprimido. Sin embargo, la velocidad binaria acordada debe ser mantenida, incluso con pérdidas ocasionales de celdas o variaciones en el tiempo de transferencia de las mismas. Este servicio se asemeja al proporcionado por el sistema telefónico existente, ya que garantiza un número fijo de celdas por unidad de tiempo para la aplicación.

El formato del campo de información de la celda, conocido como segmento, incluye un Número de Secuencia de 4 bits (SN) y un campo asociado de 4 bits utilizado para Proteger el Número de Secuencia (SNP) contra errores de un bit.



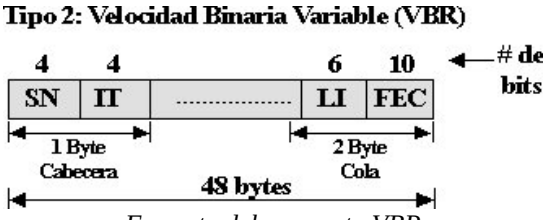

*Formato del segmento CBR*

De esta forma es posible detectar pérdidas de segmentos. Las pérdidas de celdas se superan de forma acordada, por ejemplo, insertando segmentos ficticios en el flujo entregado. Variaciones en el retardo de transferencia de celdas son compensadas mediante un buffer en la parte destino, la salida de segmentos correspondiente a una llamada por ejemplo, y únicamente se comienza después de que se hayan recibido un número predeterminado de segmentos. Este número viene determinado por la velocidad binaria del usuario. Valores típicos son 2 segmentos a velocidades de Kbps y 100 segmentos a velocidades de Mbps. Claramente este retardo se sumará al retardo de ensamblaje/desensamblaje ya identificado.

El uso de un buffer en destino también proporciona un modo sencillo de superar cualquier pequeña variación entre las velocidades binarias en origen y destino, por ejemplo si cada uno está basado en diferente reloj. Una solución mejor es que la red proporcione los relojes de entrada y salida, normalmente extraídos de la codificación en línea del flujo de bits transmitido.

**1.5.3.3.2 Tipo 2: Velocidad Binaria Variable (VBR)**

En este tipo de servicio, aunque exista una temporización relacionada entre los SAPs fuente y el destino, la velocidad de transferencia real de información, puede variar durante la conexión. Como con el tipo 1, el segmento contiene un Número de Secuencia **SN** de 4 bits para la recuperación de celdas pérdidas.




*Formato del segmento VBR*

El campo de Tipo de Información **IT** indica, o bien la posición relativa del segmento con relación al mensaje remitido, por ejemplo, una trama comprimida procedente de un codec de video por ejemplo, o si el segmento contiene información de temporización, o de otro tipo. Los tres tipos de segmento con relación a la información posicional son: comienzo de mensaje **BOM**, continuación de mensaje **COM** y fin de mensaje **EOM**. Debido al tamaño variable de las unidades de mensaje remitidas, un Indicador de Longitud **LI** en la cola del segmento indica el número de bytes útiles en el último segmento. Finalmente, el campo **FEC** habilita la detección y corrección de errores.

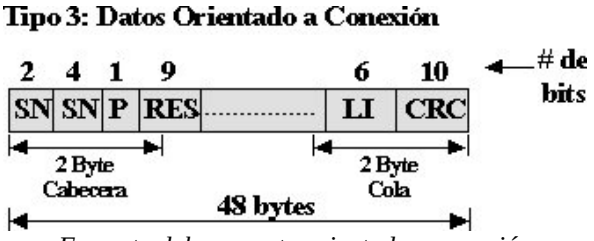
**1.5.3.3.3 Tipo 3: Datos Orientados a Conexión**

El protocolo AAL3/4 proporciona dos tipos de servicios para la transferencia de datos: uno Orientado a Conexión **CO** (*Connection Oriented*) y otro Sin Conexión **CLS**. La diferencia entre los dos es que con el primero, antes de que cualquier dato pueda ser transmitido, debe establecerse una Conexión Virtual.

El servicio orientado a conexión tiene dos modos operacionales: asegurado y no asegurado, cada uno soportando envíos de Unidades de Datos del Servicio **SDU** o mensajes de usuario, de tamaño fijo o variable. El modo asegurado proporciona un servicio fiable que garantiza que todas las SDUs son entregadas sin errores y en la misma secuencia con que fueron remitidas. Para proporcionar este servicio todos los segmentos generados por el sub-nivel CS están sujetos a procedimientos de control de flujo y recuperación de errores.

Para el modo no asegurado, los segmentos son transmitidos sobre la base del mejor esfuerzo (*best effort*), esto es, cualquier segmento corrompido es simplemente descartado y se deja a los niveles de protocolo de usuario superar esta eventualidad.

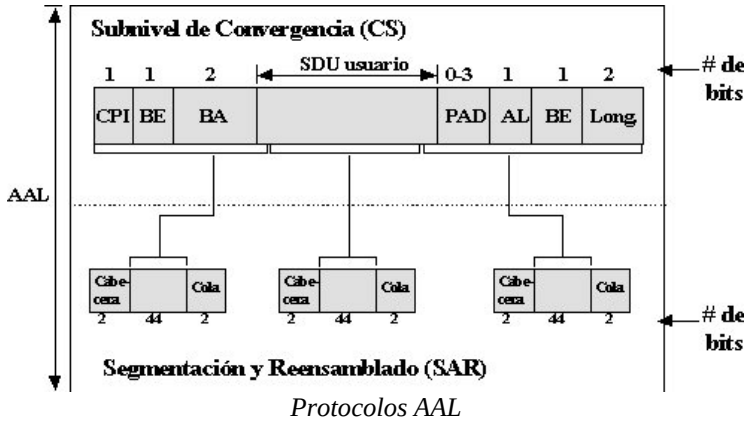
El Tipo de Segmento (ST) indica si es el primero (BOM), continuación (COM), último (EOM), o el único (SSM) de una SDU remitida.




*Formato del segmento orientado a conexión*

El Número de Secuencia **SN** se emplea para detectar segmentos perdidos o duplicados y también para control de flujo. Un único bit de Prioridad **P** permite que los segmentos tengan uno de dos niveles de prioridad. En la cola, el Indicador de Longitud **LI** indica el número de bytes útiles en el segmento y el CRC-10 está presente para la detección y eventual corrección de errores. Claramente LI solamente tiene significado en el último segmento de una SDU o si es el único segmento.

El funcionamiento del protocolo del Subnivel de Convergencia **CS** se puede describir mejor considerando el formato de los mensajes o Unidades de Datos del Protocolo **CS-PDU** que genera, en relación con la SDU remitida por el usuario, y el modo que esta es transportada por el subnivel SAR.




*Protocolos AAL*

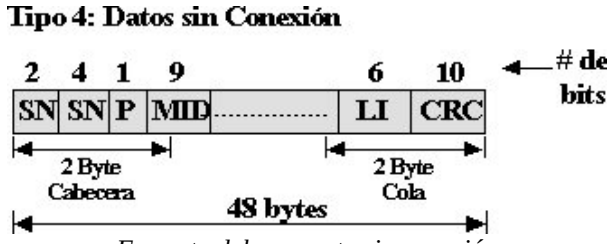
Los campos de cabecera y cola añadidos por el protocolo CS en origen a la SDU remitida se utilizan para habilitar al protocolo CS receptor para la detección de SDUs perdidas o malformadas. El Identificador de

Protocolo CS **CPI**, se utiliza para identificar el tipo de protocolo CS que está siendo utilizado. El identificador comienzo-fin **BE** (*Begin-End*) es un número de secuencia que se repite en la cola para añadir capacidad de reacción. Se utiliza para asegurarse que las SDUs son entregadas en la misma secuencia en la que se remitieron. El campo de Asignación de Buffer **BA** se inserta en la cabecera para ayudar al protocolo CS receptor a reservar una cantidad de memoria suficiente (*buffer*) para contener una SDU completa.

En la cola, el campo de relleno **PAD** se utiliza para hacer que el número de bytes de la unidad de datos del protocolo CS sea un múltiplo de 4 bytes. De forma similar el byte de alineamiento **AL** es un byte de relleno para hacer que la cola tenga 4 bytes. El campo de longitud (*Length*) indica la longitud total de la unidad de datos del protocolo completa y entonces ayuda al receptor a detectar cualquier SDU malformada.

#### 1.5.3.3.4 Tipo 4: Datos sin Conexión

El servicio de datos sin conexión está pensado, por ejemplo, para la interconexión de LANs a alta velocidad. A diferencia del tipo 3 no hay señalización de llamada ni terminación, en su lugar conexiones permanentes o semi-permanentes están siempre establecidas entre cada par de SAPs origen y destino. Aparte de esto, los dos servicios utilizan los mismos formatos en el Subnivel de Convergencia CS y segmento.




*Formato del segmento sin conexión*

Sin embargo, con los servicios sin conexión, el campo **RES** (reservado) está sustituido por el Identificador del Mensaje **MID**. Normalmente celdas relacionadas con diferentes tramas estarán en tránsito en cualquier instante, el campo MID se utiliza para habilitar al subnivel SAR de destino relacionar cada celda recibida a su SDU específica. La utilización del MID permite la multiplexación de múltiples sesiones en una misma conexión virtual VPI/VCI.

#### 1.5.3.3.5 Servicios sin Conexión ATM

Usualmente esta información será introducida por el gestor de la red y para minimizar la sobrecarga se deben utilizar varios de estos nodos. Estos son conocidos como Servidores de la Función Sin Conexión (**CLSF**). Otro tema con este tipo de servicio se relaciona con el asignamiento de MIDs. Si dos nodos fuente utilizan simultáneamente el mismo MID y las tramas son para el mismo destino, el procedimiento de reensamblado no funcionará. En consecuencia, para superar esta eventualidad, el CLSF puede también cambiar el MID durante su operación de retransmisión, si este ya está en uso en un nodo de destino dado.

#### 1.5.3.3.6 Comunicaciones de Datos sobre ATM - AAL5 (SEAL)

AAL5 es un protocolo para soportar transmisiones de datos con o sin conexión. Elimina parte de la complejidad y sobrecarga introducida por AAL3/4, proporcionando un nivel de adaptación simple y eficiente para la transmisión de tramas de datos entre dispositivos tales como enrutadores, sobre una red ATM.

AAL5 define un formato de trama de longitud variable, así como los procedimientos para segmentar la trama en celdas para su transmisión sobre la red ATM, y el reensamblado en destino. El subnivel de convergencia **CS**, para realizar sus funciones, añade 8 bytes por trama: Un CRC para detectar errores de trama y celdas perdidas, 2 bytes para especificar la longitud de la trama (0-65.535 bytes), 2 bytes de control reservados. Hay un campo de relleno (**PAD**) conteniendo de 0 a 47 bytes con el fin de el número total de bytes sea múltiplo de 48. La unidad de datos del protocolo así generada (CS-PDU), es transportada al subnivel SAR para su segmentación.

El subnivel SAR utiliza un bit del campo PT de la cabecera de la celda ATM, para indicar que es la última celda (EOM) perteneciente a la trama (PT = 0x1), o no es la última (not EOM, PT = 0x0). No consume ninguna parte de la carga útil de la celda para realizar esta función, obteniéndose una mejora de 4 bytes por celda frente a AAL3/4.

AAL5, a diferencia de AAL3/4, no permite la multiplexación de mensajes de diferentes usuarios (diferentes SDUs) dentro de un mismo VPI/VCI ya que no contiene el IDentificador de Mensaje (MID), así que requiere un VPI/VCI dedicado.

### 1.6 Otros Servicios de las Redes Telefónicas

El rápido crecimiento de la redes de datos y de Internet y la creciente demanda de servicios orientados a satisfacer necesidades de comunicación avanzadas, han provocado que las redes telefónicas actuales brinden otros servicios como el transporte de datos, fax y servicios suplementarios.

#### 1.6.1 Fax

Utilizando la red telefónica, pueden ser transmitidos documentos impresos o escritos, mediante lo que se conoce como facsímil o **fax**. Para su transmisión, un equipo de fax hace un recorrido por medio de un haz a través de todo el documento que será transmitido, identificando para cada punto del mismo la intensidad del color y asignándole una señal eléctrica. En este caso, se realiza la conversión de una señal óptica en una señal eléctrica, esta última puede entonces ser transmitida a través de la red telefónica, como si fuera una señal de voz. En este proceso, el protocolo que tienen que realizar los equipos terminales consiste en intercambiar señales para acordar, entre otros factores, el tiempo de inicio de la transmisión y la velocidad de la misma. Una vez que ésta ha sido iniciada, el equipo receptor realiza el mismo recorrido sobre la hoja de papel, a la misma velocidad, y va imprimiendo las señales ópticas que, a su vez, están basadas en las señales eléctricas que recibe.

#### 1.6.2 Modems

Considerando la amplia cobertura de la red telefónica y los desarrollos tecnológicos de las últimas décadas, muchos esfuerzos se han dirigido hacia la posibilidad de transmitir señales digitales de audio, voz, vídeo y datos sobre la misma infraestructura, lo cual aumentaría de manera considerable la cantidad de servicios que podrían ser ofrecidos por medio de esta red.
En un principio, para lograr lo anterior, se utilizó el siguiente razonamiento: Si a través de la red telefónica se pueden transmitir señales eléctricas que corresponden al rango de frecuencias que genera el hombre al producir sonidos hablados, entonces, si se generan tonos en este mismo rango que correspondan a los símbolos binarios "1" y "0" se podrían realizar transmisiones digitales binarias. Este proceso se conoce como modulación, y el proceso inverso, es decir, extraer del canal o de la red los tonos para generar nuevamente los símbolos binarios, es la demodulación. Con base en estos dos términos, los equipos que realizan estas operaciones para transmisión de datos, se denominan módems.
A través de los módems se puede tener acceso a redes de datos como Internet, aunque se tiene la limitante de que se usa un enlace de muy baja velocidad diseñado para manejar un ancho de banda de 4 kHz y que esta muy propenso a interferencias y atenuaciones. Actualmente con algunas variaciones de esta técnica se pueden lograr velocidades de 56 kbps (estándar V.90) y hasta de varios Mbps mediante la tecnología XDSL (X *Digital Subscriber Line*) que utiliza algoritmos de codificación de línea avanzados para dividir el espectro de frecuencias entre la voz y los datos, de tal manera que las transmisiones de voz residen en la banda base (4 kHz o inferior) mientras que los canales de datos de salida y de entrada están en un espectro más alto (300 kHz o superior). El resultado final es que los proveedores de servicio pueden proporcionar velocidades de datos de múltiples Mbps mientras dejan intactos los servicios de voz, todo sobre la misma línea de cobre.

#### 1.6.3 Servicios Suplementarios

La utilización de centrales telefónicas digitales ha permitido la implementación de una serie de servicios llamados suplementarios con la finalidad de satisfacer las crecientes necesidades de comunicación de los

usuarios y para brindarles una serie de beneficios adicionales a los de la telefonía tradicional. Algunos de estos servicios se mencionan a continuación:

**Transferencia Variable Incondicional**: El usuario puede programar su teléfono para que desvíe las llamadas destinadas a él hacia otro número telefónico.

**Transferencia Variable por Abonado Ocupado**: El usuario puede programar su teléfono para que desvíe las llamadas destinadas a él hacia otro número telefónico, siempre y cuando su teléfono se encuentre ocupado.

**Transferencia por no Respuesta**: El usuario puede programar su teléfono para que desvíe las llamadas destinadas a él hacia otro número telefónico, cuando el teléfono no es contestado después de cierto tiempo.

**Restricción Permanente de Llamadas Salientes**: El usuario puede restringir su teléfono para realizar llamadas salientes locales, locales extendidas, larga distancia, celulares, internacionales etc. según lo solicite.

**Código Secreto:** El usuario puede restringir desde su teléfono y por medio de una clave, la salida de llamadas locales, locales extendidas, larga distancia, celulares, internacionales etc. según lo haya solicitado y según sea su restricción permanente de llamadas salientes.

**Línea Directa:** El servicio consiste en establecer una llamada a un número preestablecido con solo levantar el auricular del teléfono.

**Despertador Automático:** El usuario puede programar la hora deseada en la central por medio de su aparato telefónico.

**Conferencia Tripartita:** El usuario puede establecer llamadas simultáneamente con dos teléfonos más y realizar control sobre ellas dejándolas en espera o liberándolas.

**No Molestar:** El usuario puede hacer llamadas pero no recibirá ninguna. Quien llama al abonado, recibe un tono de congestión.

**Identificador de Llamada:** La central envía al dispositivo de identificación de llamadas del usuario el número telefónico desde el cual esta siendo llamado.

**Restricción de Identificación de Llamada:** El número telefónico del usuario no será presentado en los identificadores de llamadas de otros usuarios.

**Suspensión Temporal:** A petición del usuario, su número teléfono quedará bloqueado para hacer y recibir llamadas.

**Timbre Distintivo:** El usuario puede dar una lista de números telefónicos cada uno de los cuales, cuando llamen, timbrarán de forma diferente para facilitar su identificación.

**Rechazo Selectivo de Llamadas:** El usuario puede dar una lista de números telefónicos cada uno de los cuales, cuando uno de estos llame, recibirán un tono de congestión. El usuario también podrá activar o desactivar el rechazo selectivo desde su teléfono, cuando el rechazo este activado, el tono de invitación a marcar será diferente.

**Transferencia Selectiva de Llamadas:** El usuario puede dar una lista de números telefónicos cada uno de los cuales, cuando llame, serán transferidos a un número telefónico dado.

**Aceptación Selectiva de Llamadas:** El usuario puede dar una lista de números telefónicos cada uno de los cuales, cuando llame, serán comunicado con el número del usuario mientras los teléfonos que llamen que no se encuentran en la lista recibirán tono de congestión.

**Remarcado Automático:** Permite al usuario establecer comunicación con un abonado que se encuentre ocupado en el mismo instante en que el abonado llamado se libere.

Varias de las funciones que realizan las centrales, también pueden ser efectuadas por conmutadores privados PBX, que en realidad son pequeñas centrales telefónicas. Entre ellas están la búsqueda de personas, la selección y la configuración de grupos, la disponibilidad de distintos modos de operación para diferentes horarios, la restricción de llamadas de larga distancia y la asignación de privilegios en general a cada una de las extensiones, el almacenamiento de información sobre llamadas y de las extensiones que las originaron, la puesta en espera de llamadas, la disponibilidad de directorios en línea, etcétera.

### 1.6.4 Transporte de Datos

Uno de la mayores y más importantes servicios que brindan las red telefónicas actuales es la de brindar servicios de transporte de datos, usando tecnologías de multiplexación y transporte como PDH y SDH principalmente. Mediante estos servicios los usuarios rentan enlaces dedicados o compartidos, tales como E1s E2s, etc. para transportar sus datos sobre la infraestructura de las compañías telefónicas, de esta manera pueden interconectar sus redes de datos sin la necesidad de instalar su propia red de transporte, que en algunos casos es imposible para las empresas por los elevados costos de instalación y mantenimiento que implica.

# Capitulo 2

# Redes IP

## 2.1 Fundamentos y Definiciones

La creciente necesidad de intercambio de información a nivel global así como el uso masivo de sistemas de cómputo ha llevado a un vertiginoso desarrollo de las redes de datos. Una red de datos es una colección de dispositivos lógicos, interconectados entre sí a través de un medio de transmisión, capaces de intercambiar algún tipo de información digital mediante un conjunto de reglas bien definidas llamadas protocolos.

Las redes de datos permiten compartir recursos tales como capacidad de procesamiento en potentes computadoras, programas de cómputo, almacenamiento de datos, bases de datos, impresoras, etc. Permitiendo considerables ahorros al no tener que proporcionar esos recursos a cada uno de los usuarios. Pero la principal ventaja de las redes de datos es que permiten el acceso eficiente a la información que sirve a los usuarios para realizar su trabajo, para tomar decisiones, para comunicarse entre ellos, para divertirse, etc. independientemente del lugar del mundo donde se localicen.

El tipo de información que viaja por las redes de datos va desde mensajes de texto (correo electrónico por ejemplo), imágenes, archivos de audio, archivos de vídeo, videoconferencias, y otras aplicaciones que cada vez demandan un mayor ancho de banda.

Las redes de datos se basan en la conmutación de paquetes para comunicarse, en este tipo de comunicación la información es fragmentada en paquetes que incluyen información de control que es utilizada por los dispositivos de red para llevar el mensaje a su destino, con este sistema no es necesaria la creación de un circuito antes de enviar la información, sino que los paquetes son enviados y el equipo de red se encarga de llevarlos a su destino, pudiendo viajar por diferentes trayectorias, esto permite que un enlace pueda transportar información generada por diversas fuentes, lo que ocasiona que los paquetes compitan entre ellos para alcanzar sus destinos, originando así en algunos casos un retardo variable.

Algunas ventajas que presentan son:

1. La eficiencia de los enlaces aumentan, pues se puede compartir el medio de transmisión con varias fuentes.
2. Se puede variar la velocidad de transmisión entre cada nodo.
3. Pueden entregar paquetes aun cuando haya más paquetes usando el mismo medio de transmisión, pero con cierto retardo.
4. Se pueden dar prioridades a los paquetes, para obtener menor retardo en los paquetes que así lo necesiten.

Las redes de área local **LAN** (*Local Area Network*) son las que proporcionan un mayor ancho de banda al usuario final, estas se caracterizan por brindar servicios de red en áreas relativamente pequeñas que van desde unos cuantos metros, en pequeñas salas, hasta grandes edificios o grupos de edificios que se distribuyen a lo largo de varios kilómetros mediante los nuevos sistemas basados en fibra óptica. Para este tipo de redes el estándar o tecnología más empleado es Ethernet.

El desarrollo de las Redes de Área Amplia **WAN** (*Wide Area Network*) se ha dado principalmente por la necesidad de interconectar redes LAN separadas geográficamente por grandes distancias, este tipo de redes permiten la comunicación prácticamente instantánea entre sistemas localizados en diferentes ciudades, países o continentes, el ejemplo más representativo de este tipo de redes es Internet que permite comunicar redes y sistemas, que pueden ser diferentes, en todo el mundo.

La popularidad y éxito de Internet se deben al desarrollo del Protocolo Internet **IP** (*Internet Protocol*) que ha permitido la interconexión de sistemas desarrollados con diferentes tecnologías, que antes impedían su

interconexión, dando origen a las redes IP, que son las que utilizan este protocolo. Las redes IP han permitido el desarrollo de una gran variedad de aplicaciones que han revolucionado el intercambio de información.

### 2.1.1 Componentes de una Red de Datos

Los elementos que componen una red de datos son:

**Software de Red:** Se trata del software de comunicación que trabaja apoyado sobre el sistema operativo de la computadora y que permite la interacción de las computadoras con la red.
**Servidores:** Son computadoras que permiten la administración de memoria, el almacenamiento de archivos, que brindan servicios, como el de correo electrónico (*mail*), que permiten la comunicación entre sistemas remotos y bases de datos y directorios, y que además pueden realizan la administración de dispositivos como impresoras.
**Clientes** (Nodos y *Workstations*): Se trata de las computadoras que se conectan a la red y que completan el concepto cliente/servidor. Es decir, computadoras que hacen uso de los servidores de una manera remota a través de las redes de datos, pudiendo varios clientes utilizar el servidor de manera simultánea.
**Interfaz de red NIC** (*Network Interface Cards o Network Board*): Estas son los dispositivos que permiten conectar las computadoras a la red de datos, se trata de circuitos que se conectan a un puerto de la computadora y que interpretan las señales eléctricas y las convierten en datos para la computadora de acuerdo a un protocolo y viceversa, son las que permiten la conexión al medio físico.
***Hub/Bridge/Switch/Router/Gateway*:** Son sistemas que permiten la interconexión de los elementos de la red. Se trata de componentes activos que regeneran las señales de datos, direccionan paquetes, evalúan protocolos y pueden tener funciones de supervisión remota.

### 2.1.2 Funciones de los Protocolos de Red

Un protocolo de red es normalmente un software que realiza un conjunto de funciones que definen las acciones que debe cumplir cada capa de la red de datos. Las funciones de un protocolo de red son las siguientes:

- Segmentación, encapsulado y ensamble en la transmisión y recepción de secuencias extensas de datos.
- Multiplexación e identificación de tramas de distintos usuarios de capas superiores.
- Control de conexión (inicio y final de llamada) y control de flujo de datos.
- Control para la detección de errores, el descarte de tramas y el pedido de retransmisión de las mismas.
- Selección de ruta (conmutación) o filtrado de direcciones cuando corresponde.
- El control de flujo de datos para detener la emisión cuando el receptor no está disponible.

**Segmentación y Ensamble de Datos:** Las razones para efectuar la segmentación de los datos a transmitir incluyen:

- La distribución del medio de transmisión en forma más equitativa entre los usuarios.
- La segmentación permite disminuir el retardo de acceso e impide la monopolización del medio de enlace.
- Permite que el tamaño del buffer requerido para los datos sea más pequeño.
- Se logra un control de errores más eficiente cuando los segmentos son pequeños.
- Permite la retransmisión de tramas más cortas.

Sin embargo, una segmentación en paquetes pequeños tiene las siguientes desventajas:

- Reduce la eficiencia de datos al involucrar un encabezado proporcionalmente mayor.
- Los bloques pequeños pueden involucrar también un número mayor de interrupciones.
- Se requiere un tiempo mayor de procesamiento.

**Control de Flujo de Datos:** Este concepto se refiere a la capacidad del receptor de controlar la emisión de datos desde el otro extremo. Los métodos usados son varios, dependiendo de la capa involucrada. Puede ser un control eléctrico (hardware) o se puede realizar en forma de secuencia de datos (software).

**Control de Errores:** Se involucra un campo de bits de paridad (*checksum*) que permite determinar las tramas con error. En este caso se puede efectuar el descarte de la trama de datos afectada (Frame Relay o ATM) o pedir la repetición automática **ARQ** (protocolos X.25 y redes LAN). El *checksum* se calcula como la suma binaria de los datos transmitidos y es menos eficaz que el chequeo de redundancia cíclica CRC.

**Control de Conexión:** El tipo de servicio ofrecido por la red es orientado a conexión (*Connection-Oriented*) u orientado a no-conexión (*Connection-less Oriented*). El Servicio **orientado a conexión** se establece inicialmente una conexión (canal virtual) y se mantiene hasta la desconexión. En el servicio **orientado a no-conexión** cada mensaje lleva la dirección completa del destino y el origen, y el enrutamiento es independiente para cada mensaje. Esto puede producir que el arribo de los mensajes esté fuera de orden. En el primero es más fácil el control de flujo para la congestión y se usa un encabezado más corto. El servicio sin conexión es usado por los usuarios de redes de datos debido a que permite el arribo de las tramas aún con interrupción de ciertos enlaces en una red. En tanto el servicio con conexión es el generalmente es usado por la simplicidad de la funciones de enrutamiento.

**Direccionamiento:** En una red de datos se requiere la identificación de los usuarios que participan en la conexión mediante las direcciones de origen y destino. Estas direcciones pueden ser físicas (mediante *hardware* o en una memoria) o lógicas (establecida mediante el sistema operativo de la red).

### 2.2 Modelo de Referencia OSI

El modelo de interconexión de sistemas abiertos **OSI** (*Open Systems Interconnection*) fue adoptado por la Organización Internacional de Normas **ISO** (*International Standard Organization*) para proporcionar a los fabricantes un conjunto de estándares que aseguraran una mayor compatibilidad e interoperabilidad entre los distintos tipos de tecnología de red utilizados en el ámbito mundial.

La finalidad del modelo ISO es permitir la cooperación entre sistemas abiertos. Un sistema abierto es aquel conjunto de computadoras, dispositivos lógicos, dispositivos periféricos, terminales, etc., que forma un todo autónomo capaz de procesar y/o transferir información. Cada sistema abierto se considera constituido por un conjunto de 7 capas o estratos representados en forma vertical. Se trata de un modelo teórico de referencia que se utiliza para explicar lo que debe realizar cada componente de la red sin entrar en los detalles de implementación.

El modelo de referencia OSI es un marco que se puede utilizar para comprender cómo viaja la información a través de una red y para visualizar cómo la información o los paquetes de datos viajan desde los programas de aplicación a través de un entorno de red hasta otro programa de aplicación ubicado en otra computadora de la red, aún cuando el remitente y el receptor tengan distintos tipos de red.

Se realiza una división en capas para entender el funcionamiento de la red, obteniéndose las siguientes ventajas:

- Divide la comunicación de red en partes más pequeñas y sencillas.
- Normaliza los componentes de red para permitir el desarrollo y el soporte de los productos de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Impide que los cambios en una capa puedan afectar las demás capas, de manera que se puedan desarrollar con más rapidez.
- Divide la comunicación de red en partes más pequeñas para simplificar su comprensión.

Cada capa tiene una función bien definida y se relaciona con sus capas inmediatas mediante unas interfaces bien definidas. Esto permite la sustitución de una de las capas sin afectar al resto, siempre y cuando no se varíen las interfaces que la relacionan con sus capas superior e inferior.

#### 2.2.1 Funciones de las Capas

Cada capa individual del modelo OSI tiene un conjunto de funciones que debe realizar para que los paquetes de datos puedan viajar en la red desde el origen hasta el destino.


*Capas del Modelo OSI*

#### 2.2.1.1 Capa 7. Aplicación

La capa de aplicación es la capa del modelo OSI más cercana al usuario. Suministra servicios de red a las aplicaciones del usuario. Difiere de las demás capas debido a que no proporciona servicios a ninguna otra capa del modelo OSI, sino solamente a aplicaciones que se encuentran fuera del modelo. Algunos ejemplos de dichos procesos de aplicación son los navegadores *web*, las hojas de cálculo, los procesadores de texto, etc. La capa de aplicación establece la disponibilidad de los socios de comunicación, sincroniza y establece acuerdos sobre los procedimientos de recuperación de errores y control de la integridad de los datos.

#### 2.2.1.2 Capa 6. Presentación

La capa de presentación garantiza que la información que envía la capa de aplicación de un sistema pueda ser leída por la capa de aplicación de otro. De ser necesario, la capa de presentación traduce entre varios formatos de datos utilizando un formato común. También son interpretados los códigos dentro de los datos, como tabuladores y caracteres especiales. Asimismo es en este nivel donde se lleva a cabo el cifrado de datos y traducción desde otros juegos de caracteres.

#### 2.2.1.3 Capa 5. Sesión

La capa de sesión establece, administra y finaliza las sesiones entre dos *hosts* (equipos de red como computadoras) que se están comunicando. La capa de sesión proporciona sus servicios a la capa de presentación. También sincroniza el diálogo entre las capas de presentación de los dos *hosts* y administra su intercambio de datos. Además de regular la sesión, esta capa ofrece disposiciones para una eficiente transferencia de datos, clase de servicio y un registro de excepciones acerca de los problemas de la capa de sesión, presentación y aplicación.

#### 2.2.1.4 Capa 4. Transporte

La capa de transporte segmenta los datos originados en el *host* emisor y los reensambla en un flujo de datos dentro del sistema del *host* receptor. Mientras que las capas de aplicación, presentación y sesión están relacionadas con aspectos de las aplicaciones, las tres capas inferiores se encargan del transporte de datos. La capa de transporte intenta suministrar un servicio de transporte de datos que aísla las capas superiores de los detalles de implementación del transporte. Específicamente, temas como la confiabilidad del transporte entre dos *hosts* es responsabilidad de la capa de transporte. Al proporcionar un servicio de comunicaciones, la capa de transporte establece, mantiene y termina adecuadamente los circuitos virtuales. Al proporcionar un servicio confiable, se utilizan dispositivos de detección y recuperación de errores de transporte. Si se pierden datos del paquete, el protocolo del nivel de transporte se coordina con el nivel de transporte de origen para la retransmisión del paquete. Este nivel asegura que se reciban los datos en el orden apropiado.

Los siguientes protocolos pueden estar en este nivel:

- *Transport Control Protocol* (TCP)
- *User Datagram Protocol* (UDP)
- *Sequenced Packed Exchange* (SPX)
- NetBios/NetBEUI

#### 2.2.1.5 Capa 3. Red

La capa de red es una capa compleja que proporciona conectividad y selección de ruta entre dos sistemas de *hosts* que pueden estar ubicados en redes geográficamente distintas. Está relacionado con los procedimientos de conmutación y transmisión de datos y oculta dichos procedimientos a los niveles superiores. Los enrutadores actúan en este nivel. Este nivel se encarga de que los paquetes sean dirigidos a su destino en la red. Si está dirigido a un segmento de la red, este nivel lo envía a un dispositivo de enrutamiento el cual lo reenvía a su destino. Esta capa se ocupa de la selección de ruta, conmutación, direccionamiento lógico y enrutamiento.

Algunos protocolos que ocupan este nivel:

- *Internet Protocol* (IP)
- Protocolo X.25
- *Internetwork Packet Exchange* (IPX) de Novell

#### 2.2.1.6 Capa 2. Enlace

La capa de enlace de datos proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la notificación de errores, entrega ordenada de tramas y control de flujo. Los *switches* actúan en este nivel en el grupo de protocolos.

Algunos protocolos que ocupan este nivel:

- Control de enlace de datos de alto nivel HDLC(*High-level Data Link Control*)
- Manejadores y métodos de acceso de LAN, como Ethernet o Token Ring.
- ATM para redes de área extensa WAN de transmisión rápida.

#### 2.2.1.7 Capa 1. Física

La capa física define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales. Las características tales como niveles de voltaje, temporización de cambios de voltaje, velocidad de datos físicos, distancias de transmisión máximas, conectores físicos y otros atributos similares se definen a través de las especificaciones de la capa física.

### 2.2.2 Comunicación entre Capas

El modelo prevé una **comunicación vertical** entre capas (capa N+1 con N y N con N-1) denominado **servicio** y una **comunicación horizontal** (capa N con N) entre distintos sistemas abiertos denominado **protocolo** (protocolo entre entidades pares o iguales *peer to peer*). Cada capa N ofrece un servicio a la capa inmediatamente superior N+1 y requiere los servicios de la inferior N-1.

Para la comunicación se definen los puntos de conexión **SAP** (*Service Access Point*) que funcionan como direcciones de la capa superior, una entidad puede tener activas varias direcciones SAP simultáneamente.

La comunicación que procede de una capa del modelo, generalmente se da con otras tres capas: la capa inmediata superior, la capa inmediata inferior y la capa análoga (*peer*) en la computadora a la que se comunicará.

Las siete capas del modelo, usan varias formas de controlar la información para comunicarse con su respectivo *peer* en otros sistemas. Esta información de control consiste de peticiones específicas e instrucciones que son intercambiadas entre *peers* del modelo de referencia OSI. La información de control consiste principalmente de encabezados. Así los datos serán encapsulados por encabezados y serán pasados a la siguiente capa según corresponda.

Los datos y la información de control que viaja a través de una red toman varios nombres dependiendo de la capa en que se encuentre:

- **Frame o Trama:** Cuando está en la Capa de Enlace de Datos
- **Datagrama o Paquete:** Cuando está en la Capa de Red
- **Segmento:** Cuando está en la Capa de Transporte.
- **Mensaje:** Unidad de información cuyo origen y destino se encuentra arriba de la Capa de Red y a veces hasta la Capa de Aplicación.

### 2.3 Modelo TCP/IP

Aunque el modelo de referencia OSI sea universalmente reconocido, el estándar de Internet desde el punto de vista histórico y técnico es el Protocolo de Control de Transmisión/Protocolo Internet **TCP/IP** *(Transfer Control Protocol/Internet Protocol.)*

El modelo de referencia TCP/IP y la pila de protocolo TCP/IP hacen que sea posible la comunicación entre dos maquinas, desde cualquier parte del mundo a través de redes que pueden ser diferentes. El Departamento de Defensa de E.U. creó el modelo TCP/IP por la necesidad de una red que pudiera funcionar ante cualquier circunstancia. La idea es que a través de un sistema de comunicaciones con diferentes tipos de conexiones (cables, microondas, fibras ópticas y enlaces satelitales), se pudiera mantener una comunicación de los equipos de red aun cuando alguna o más de las conexiones estuvieran rotas o indisponibles.

El modelo TCP/IP tiene cuatro capas: la capa de Aplicación, la capa de Transporte, la capa de Internet y la capa de Acceso de Red. Algunas de las capas del modelo TCP/IP poseen el mismo nombre que las capas del modelo OSI pero tienen diferentes funciones en cada modelo.

*Capas del Modelo TCP/IP*

#### 2.3.1 Capa de Aplicación

La capa de aplicación contiene protocolos de nivel superior que incluyen los detalles de las capas de sesión y presentación que incluyen aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y garantiza que estos datos estén correctamente empaquetados para la siguiente capa. En la capa de aplicación, aparecen distintas tareas comunes de Internet desarrolladas por aplicaciones que incluyen las siguientes:

- FTP: Protocolo de Transferencia de Archivos (*File Transfer Protocol* )
- HTTP: Protocolo de Transferencia de Hipertexto (*Hypertext Transfer Protocol* )

- SMTP: Protocolo de Transferencia de Correo Simple (*Simple Mail Transfer Protocol* )
- DNS: Sistema de Nombres de Dominio (*Domain Name System* )
- TFTP: Protocolo de transferencia de Archivos Trivial (*Trivial File Transfer Protocol* )

El modelo TCP/IP enfatiza la máxima flexibilidad, en la capa de aplicación, para los creadores de software.

### 2.3.2 Capa de Transporte

La capa de transporte se refiere a los aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores. Uno de sus protocolos, el protocolo TCP, ofrece maneras flexibles y de alta calidad para crear comunicaciones de red confiables, sin problemas de flujo y con un nivel de error bajo. TCP es un protocolo orientado a la conexión. Mantiene un diálogo entre el origen y el destino mientras empaqueta la información de la capa de aplicación en unidades denominadas segmentos. La capa de transporte involucra dos protocolos: el protocolo de control de transmisión **TCP** (*Transfer Control Protocol*) y el protocolo de datagrama de usuario **UDP** (*User Datagram Protocol*).

### 2.3.3 Capa de Internet

El propósito de la capa de Internet es enviar paquetes origen desde cualquier red en Internet y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que recorrieron para llegar hasta allí. El protocolo específico que rige esta capa se denomina **Protocolo Internet IP** (*Internet Protocol*). En esta capa se produce la determinación de la mejor ruta y la conmutación de paquetes. En el modelo TCP/IP existe solamente un protocolo de red: el Protocolo Internet o IP, independientemente de la aplicación que solicita servicios de red o del protocolo de transporte que se utilice. Esta es una decisión de diseño deliberada. IP sirve como protocolo universal que permite que cualquier maquina en cualquier parte del mundo pueda comunicarse en cualquier momento.

### 2.3.4 Capa de Acceso de Red

También se denomina capa de *host* a red. Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico. Esta capa incluye los detalles de tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI. La capa de acceso de red, se relaciona con la tecnología específica de LAN o WAN que se utiliza.

A continuación se muestran algunas de los protocolos de cada capa:

**Capa de aplicación** (HTTP, SMTP, FTP, TFTP, DNS)
**Capa de transporte** (UDP, TCP)
**Capa de red** (IP)
**Capa de acceso a la red** (Ethernet, Token Ring, etc.)
**Capa física** (Cable Coaxial, UTP, Fibra Óptica, etc.)

## 2.4 Comparación del Modelo OSI y el Modelo TCP/IP

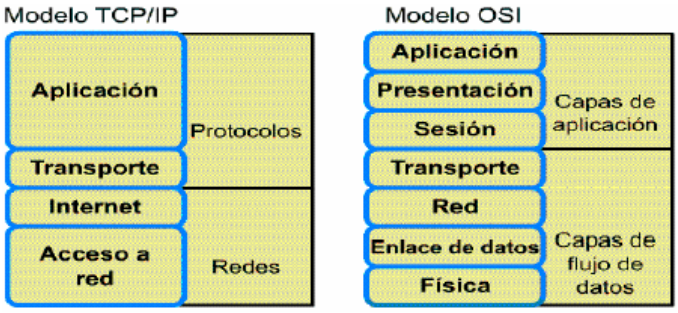
Similitudes:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- La tecnología es de conmutación por paquetes.

Diferencias

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en una sola capa

- TCP/IP parece ser más simple porque tiene menos capas
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló Internet. Las redes típicas no se desarrollan normalmente a partir del protocolo OSI, aunque el modelo OSI se usa como guía de referencia.




*Diferencias entre los Modelos OSI y TCP/IP*

**2.5 Elementos de la Capa de Acceso a Red (TCP/IP)**

A continuación se describen los elementos que integran una red IP en la capa de acceso a red de acuerdo al modelo TCP/IP, aunque también se hace referencia al modelo OSI para un mejor entendimiento del funcionamiento de las redes IP.
La capa de acceso a red (TCP/IP) incluye a las funciones de la capa física y de la capa de enlace del modelo OSI que se describen a continuación

**2.5.1 Capa Física (OSI)**

La capa física determina la interfaz entre el sistema y el medio de enlace. Se ocupa de los siguientes aspectos:

- Propiedades de la interfaz de red (topología, tamaño o extensión, configuración, longitud, etc).
- Propiedades de conexión (conector, tipo de cable, etc).
- Propiedades eléctricas (nivel de tensión, impedancia, tipo de conductor, código, velocidad de bit, etc).
- Protocolo de acceso al medio de enlace (en redes LAN).

**2.5.1.1 Medios de Transmisión**

La capa física determina el soporte físico o medio de transmisión por el cual se transmiten los datos. Estos **medios de transmisión** se clasifican en **guiados** y **no guiados**. Los primeros son aquellos que utilizan un medio sólido (un cable) para la transmisión. Los medios no guiados utilizan el aire para transportar los datos, son los medios inalámbricos.

Entre los medios no guiados se encuentran:

- **Ondas de Radio**: Son capaces de recorrer grandes distancias, atravesando incluso edificios. Son ondas electromagnéticas que se propagan en todas las direcciones (omnidireccionales). Su mayor problema son las interferencias entre usuarios.
- **Microondas**: Estas ondas viajan en línea recta, por lo que emisor y receptor deben estar alineados cuidadosamente (línea de vista). Tienen dificultades para atravesar edificios. Debido a la propia curvatura de la tierra, la distancia entre dos repetidores no debe exceder de unos 80 Km de distancia. Es una forma económica para comunicar dos zonas geográficas mediante dos torres suficientemente altas para que sus extremos sean visibles.
- **Infrarrojos**: Son ondas direccionales incapaces de atravesar objetos sólidos (paredes, por ejemplo) que son usadas para transmisiones de distancia corta. Las tarjetas de red inalámbricas utilizadas en algunas redes locales emplean esta tecnología (WLAN), resultan muy cómodas para computadoras portátiles, sin embargo, su velocidad es inferior a la conseguida mediante un cable de par trenzado.

- **Ondas de Luz**: Las ondas láser son unidireccionales y se pueden utilizar para comunicar dos edificios próximos instalando en cada uno de ellos un emisor láser y un fotodetector.

Entre los medios guiados se encuentran:

- **Cable Coaxial**: Es un hilo de cobre en la parte central rodeado por una maya y separados ambos elementos conductores por un cilindro de plástico. Las redes que utilizan este cable requieren que los adaptadores tengan un conector apropiado: los ordenadores forman una fila y se coloca un segmento de cable entre cada ordenador y el siguiente. En los extremos hay que colocar un terminador, una resistencia de 50 Ohms. La velocidad máxima que se puede alcanzar es de 10Mbps.
- **Cable de Par Trenzado**: Consta de 4 pares de hilos y utiliza conectores RJ-45. Dependiendo del número de trenzas por unidad de longitud, los cables de par trenzado se clasifican en categorías. A mayor número de trenzas, se obtiene una mayor velocidad de transferencia.
  - Categoría 3, hasta 16 Mbps
  - Categoría 4, hasta 20 Mbps
  - Categoría 5, hasta 100 Mbps
  - Categoría 6, hasta 1Gbps

  Los cables par trenzado pueden ser a su vez de dos tipos:
  - UTP (*Unshielded Twisted Pair*, par trenzado no enmallado)
  - STP (*Shielded Twisted Pair*, par trenzado enmallado)

  Los cables UTP son los más utilizados debido a su bajo costo y facilidad de instalación. Los cables STP están cubiertos por una malla metálica que reduce las interferencias y mejora las características de la transmisión. Sin embargo, tienen un costo elevado y al ser más gruesos son más complicados de instalar.
  Los cables STP se utilizan únicamente para instalaciones muy puntuales que requieran una calidad de transmisión muy alta. Anteriormente los segmentos de cable iban desde cada una de las estaciones o nodos de red hasta un *hub* o concentrador, formando una topología de estrella. Actualmente se utilizan métodos de cableado estructurado, que permiten una estandarización en el uso de cableado para distintos sistemas de comunicación, por ejemplo el cable empleado por las redes telefónica y de datos puede ser el mismo, de tal manera que el cableado que se extiende desde los nodos de cualquier servicio hasta el cuarto de telecomunicaciones se concentren en un panel de parcheo, a partir del cual los nodos de red son interconectados al servicio correspondiente mediante un conector adecuado. Esta filosofía de cableado permite que el cable usado, por ejemplo, para conectar un teléfono de conmutación de circuitos mediante un conector RJ-11, pueda ser usado después para conectar un teléfono IP o una computadora mediante un conector RJ-45, evitando la costosa instalación de nuevo cableado, en el panel de parcheo lo que se hace es cambiar el conector destinado a la RTC por uno para la red de datos.
- **Cable de Fibra Óptica**: En los cables de fibra óptica la información se transmite en forma de pulsos de luz. En un extremo del cable se coloca un diodo luminoso (LED) o bien un láser, que puede emitir luz. Y en el otro extremo se sitúa un detector de luz. Mediante los cables de fibra óptica se llegan a alcanzar velocidades de varios Gbps. Sin embargo, su instalación y mantenimiento tiene un costo elevado y solamente son utilizados para redes troncales con mucho tráfico.

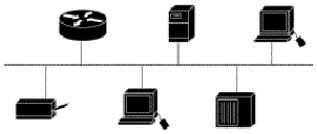
#### 2.5.1.2 Tipos de Comunicación

- ***Simplex*:** En una comunicación *simplex* existe un solo canal unidireccional, el origen puede transmitir al destino pero el destino no puede comunicarse con el origen. Por ejemplo, la radio y la televisión.
- ***Half-Duplex*:** En una comunicación *half-duplex* existe un solo canal que puede transmitir en los dos sentidos pero no simultáneamente, las estaciones se tienen que turnar. Esto es lo que ocurre con las emisoras de radioaficionados.
- ***Full-Duplex*:** En una comunicación *full-duplex* existen dos canales, uno para cada sentido, ambas estaciones pueden transmitir y recibir a la vez. Por ejemplo, el teléfono.

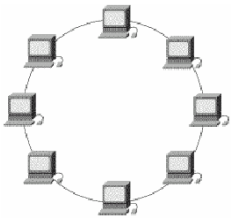
#### 2.5.1.3 Topologías de Red

En redes de datos existen las siguientes configuraciones básicas para la interconexión de dispositivos (ya sea de manera lógica o física).

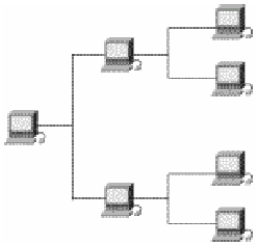
**Bus:** Todos los dispositivos se encuentran conectados a un medio de transmisión de manera plana, es decir la transmisión de uno es escuchada por los demás al mismo tiempo.



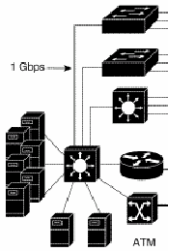
**Anillo:** Los dispositivos se conectan uno tras otro en cadena para formar un anillo. Si un dispositivo quiere transmitir información a otro no directamente conectado, los dispositivos intermedios tendrán que retransmitir la información generada por el primer dispositivo hasta que llegar a su destino final.



**Jerárquica o árbol:** En esta topología varios dispositivos son concentrados en uno para su comunicación, el cual a su vez puede estar concentrado en otro dispositivo de mayor jerarquía para su comunicación.



**Estrella:** Es el tipo más común de topología física, y está formada de un dispositivo central conectado a todos los demás dispositivos para su comunicación.




### 2.5.2 Capa de Enlace (OSI)

La capa de enlace proporciona un tránsito de datos confiable a través de un enlace físico. Al hacerlo, la capa de enlace de datos se ocupa del direccionamiento físico, la topología de red, el acceso a la red, la notificación

de errores, entrega ordenada de tramas y control de flujo. El principal estándar usado en esta capa es el IEEE 802.3 o Ethernet.

#### 2.5.2.1 Funcionamiento de Ethernet (IEEE 802.3)

Las redes Ethernet son actualmente las redes más utilizadas en entornos LAN. El estándar 802.3 fue diseñado originalmente para funcionar a 10 Mbps, aunque posteriormente ha sido perfeccionado para trabajar a 100 Mbps a 1 Gbps y actualmente hasta 10 Gbps.

Una red Ethernet tiene las siguientes características:

- **Utiliza un Canal Único:** Todas las estaciones comparten el mismo canal de comunicación por lo que sólo una puede utilizarlo en cada momento, físicamente esto se implementa mediante una topología de estrella, pero lógicamente se tiene una topología de bus.
- **Es una Red de Difusión:** Debido a que todas las transmisiones llegan a todas las estaciones pero sólo su destinatario acepta el mensaje y el resto lo descartan.
- **Tiene un Control de Acceso Distribuido:** No existe una autoridad central que garantice los accesos. Es decir, no hay ninguna estación que supervise y asigne los turnos al resto de estaciones. Todas las estaciones tienen la misma prioridad para transmitir.

En Ethernet cualquier estación puede transmitir siempre que el cable o medio de transmisión se encuentre libre, se utiliza un canal único de difusión y ninguna estación tiene mayor autoridad que otra. Por lo que Ethernet se comporta mejor en redes con poco tráfico.

En las redes Ethernet, cuando una estación envía un mensaje a otra, no recibe confirmación de que la estación destino haya recibido su mensaje. Una estación puede estar enviando paquetes Ethernet a otra que está desconectada y no advertirá que los paquetes se están perdiendo. Las capas superiores (y más concretamente, TCP) son las encargadas de asegurar que la transmisión se haya realizado de forma correcta.

El protocolo de comunicación que utilizan estas redes es el de Acceso Múltiple con Detección de Portadora y Detección de Colisiones **CSMA/CD** (*Carrier Sense Multiple Access/Collision Detect*). Esta técnica de control de acceso a la red ha sido normalizada en el estándar IEEE 802.3.

Cuando una estación quiere transmitir, primero escucha el canal (detección de portadora). Si está libre, transmite, pero si está ocupado, espera un tiempo y vuelve a intentarlo. Sin embargo, una vez que una estación ha decidido comenzar la transmisión puede darse el caso de que otra estación haya tomado la misma decisión, basándose en que el canal estaba libre cuando ambas lo comprobaron. Debido a los retardos de propagación en el cable, ambas señales sufrirán una **colisión** y no se podrá completar la transmisión de ninguna de las dos estaciones. Las estaciones que están transmitiendo lo advierten (detección de colisiones) e interrumpen inmediatamente la transmisión. Después esperan un tiempo aleatorio y vuelven a intentarlo. Si se produce una nueva colisión, esperarán el doble del tiempo anterior y lo intentan de nuevo. De esta manera, se va reduciendo la probabilidad de nuevas colisiones.

El canal es único y por lo tanto todas las estaciones tienen que compartirlo. Sólo una estación puede estar transmitiendo en cada momento, sin embargo pueden estar recibiendo el mismo mensaje más de una. La existencia de colisiones en una red no indica que exista un mal funcionamiento. Las colisiones están definidas dentro del protocolo Ethernet y no son consideradas como una situación anómala. Sin embargo, cuando se produce una colisión el canal se desaprovecha porque ninguna estación logra transmitir en ese momento. Para reducir el número de colisiones que se producen en una red se separa en grupos de computadoras mediante un *switch* o un *router*.

##### 2.5.2.1.1 Direcciones Físicas (MAC)

Para distinguir unas estaciones de otras se utilizan las direcciones físicas o Direcciones de Control de Acceso al Medio **MAC** (*Medium Access Control*), que son direcciones de 48 bits asignadas de fábrica, que no se pueden variar, a las tarjetas de interfaz de red **NIC** (*Network Interface Card*). Los fabricantes garantizan que

no puede haber dos tarjetas de red con la misma dirección física. Si esto llegase a ocurrir dentro de una misma red la comunicación se volvería imposible.

Los tres primeros bytes corresponden a un identificador del fabricante (no puede haber dos fabricantes con el mismo identificador) y los tres últimos al número de serie (no puede haber dos tarjetas del mismo fabricante con el mismo número de serie).

Por ejemplo en la dirección MAC: 5D:1E:23:10:9F:A3

Los bytes 5D:1E:23 identifican al fabricante y los bytes 10:9F:A3 al número de serie de la NIC

No todas las direcciones representan a máquinas aisladas, algunas de ellas se utilizan para enviar mensajes de multidifusión (***multicast***). Esto es, enviar un mensaje a varias máquinas a la vez o a todas las máquinas de la red (***broadcas***t). Ethernet permite que el mismo mensaje pueda ser escuchado por más de una máquina a la vez.

**2.5.2.1.2 Formato de la Trama**

La comunicación entre una estación y otra a través de una red Ethernet se realiza enviando tramas Ethernet. El mensaje que se quiere transmitir se descompone en una o más tramas que puede tener el siguiente formato:

| 8 bytes | 6 bytes | 6 bytes | 2 bytes | 64-1500 bytes | 4 bytes |
|---|---|---|---|---|---|
| Preámbulo | Dirección física destino | Dirección física origen | Tipo de trama | Datos de la trama | CRC |

*Formato de la Trama Ethernet*

**Preámbulo:** Este campo tiene una extensión de 7 bytes que siguen la secuencia <10101010>, Cuando esta secuencia de bits se codifica en Manchester diferencial, se genera una onda cuadrada (y digital, discreta) cuya frecuencia es utilizada por el receptor para sincronizarse con el reloj del emisor.
**Inicio:** Es un campo de 1 byte con la secuencia <10101011> que indica el comienzo de la trama.
**Dirección de Destino:** Es un campo de 6 bytes que contiene la dirección del destinatario, esta dirección puede ser local o global. Es local cuando la dirección sólo tiene sentido dentro de la propia red, suele estar asignada por el administrador de red. Una dirección global es la dirección MAC o dirección Ethernet. El bit de mayor orden de este campo, que ocupa el lugar 47, codifica si la dirección de destino es un único destinatario (bit puesto a 0) o si representa una dirección de grupo (bit puesto a 1). Una dirección de grupo es la dirección a la que varias estaciones tienen derecho de escuchar (transmisión de uno a varios). Cuando todos los bits del campo dirección están a 1, se codifica un *broadcast*, es decir, codifica una trama para todas las estaciones de la red. El sistema sabe si se trata de una dirección local o global analizando el valor del bit 46.
**Dirección de origen:** Es semejante al campo de dirección de destino, pero codifica la dirección MAC de la tarjeta que originó la trama.
**Tipo de Trama:** Indica el formato de los datos que se transfieren en el campo y se utiliza para permitir el uso de diferentes protocolos en la misma red (TCP/IP por ejemplo).
**Datos:** Es un campo que puede codificar entre 0 y 1500 bytes. Incluye la información de usuario procedente de la capa de la red.
**Relleno:** La IEEE 802.3 especifica que una trama no puede tener un tamaño inferior a 64 bytes, por tanto, cuando la longitud del campo de datos es muy pequeña es necesario rellenar este campo para completar una trama mínima de 64 bytes. Es un campo que puede, por tanto, tener una longitud entre 0 y 64 bytes.
**CRC:** Es el campo en donde se codifica el control de errores de trama por el método de redundancia cíclica.

El formato del frame y el medio de transmisión (coaxial, UTP, fibra óptica) es lo que difiere entre las diferentes tecnologías Ethernet (FastEthernet, GigabitEthernet, etc).

**2.5.2.1.3 Elementos de Interconexión**

***Hub*** **o Concentrador:** Es el punto central desde el cual parten los cables de par trenzado hasta los distintos puntos de la red, siguiendo una topología de estrella, pero brindando una topología lógica de bus, ya que los

*hubs* difunden la información que reciben desde un puerto por todos los demás, es decir que funcionan como un repetidor de señales eléctricas, por esto se dice que es un dispositivo que funciona dentro de la capa 1 del modelo OSI. Todas sus ramas funcionan a la misma velocidad por lo que si se mezclan tarjetas de red de 10/100 Mbps y 10 Mbps en un mismo *hub*, por ejemplo, todas las ramas del *hub* funcionarán a la velocidad menor (10 Mbps).

***Switch* o Conmutador:** Es una especie de *hub* mejorado, tiene las mismas posibilidades de interconexión que un *hub* (al igual que un *hub*, no impone ninguna restricción de acceso entre los ordenadores conectados a sus puertos). Sin embargo se comporta de un modo más eficiente reduciendo el tráfico en las redes y el número de colisiones. Un *switch* no difunde las tramas Ethernet por todos los puertos, sino que las retransmite sólo por los puertos necesarios, cada puerto tiene un *buffer* o memoria intermedia para almacenar tramas Ethernet. Otra ventaja es que puede trabajar con velocidades distintas en sus ramas (*autosensing*), unas ramas pueden ir a 10 Mbps y otras a 100 Mbps, por ejemplo.

Para realizar su trabajo los *switches* contienen una tabla dinámica de direcciones físicas y números de puerto. Un procesador analiza las tramas Ethernet entrantes y busca la dirección física de destino en su tabla. Si la encuentra, únicamente reenvía la trama por el puerto indicado. Si por el contrario no la encuentra, no le quedar más remedio que actuar como un *hub* y difundirla por todas sus ramas.
El campo con la dirección física de origen de las tramas Ethernet es utilizado por el *switch* para agregar una entrada a su tabla basándose en el número de puerto por el que ha recibido la trama. A medida que el tráfico se incrementa en la red, la tabla se va construyendo de forma dinámica. Para evitar que la información quede desactualizada las entradas de la tabla desaparecen cuando agotan su tiempo de vida (TTL), expresado en segundos. Por las tareas que realizan los *switches* se dice que son dispositivos de capa 2.

#### 2.5.2.1.4 Dominios de Colisión

Un dominio de colisión es un segmento del cableado de la red que comparte las mismas colisiones. Cada vez que se produzca una colisión dentro de un mismo dominio de colisión, afectará a todos los ordenadores conectados a ese segmento pero no a los ordenadores pertenecientes a otros dominios de colisión.
Todas las ramas de un *hub* forman un mismo dominio de colisión (las colisiones se retransmiten por todos los puertos del *hub*). Cada rama de un *switch* constituye un dominio de colisiones distinto (las colisiones no se retransmiten por los puertos del *switch*). Este es el motivo por el cual la utilización de *switches* reduce el número de colisiones y mejora la eficiencia de las redes. El ancho de banda disponible se reparte entre todos los ordenadores conectados a un mismo dominio de colisión.

#### 2.5.2.1.5 Velocidades

Ethernet puede funcionar a diferentes velocidades: 10 Mbps, 100 Mbps (*FastEthernet*), 1 Gbps (1000 Mbps) y a 10 Gbps. 10 Mbps es la velocidad para la que se diseñó originalmente el estándar Ethernet. Sin embargo, esta velocidad se ha mejorado para adaptarse a las crecientes exigencias de las redes locales. La velocidad de 100 Mbps es actualmente la más utilizada en las empresas.

Una buena opción para redes nuevas es *FastEthernet*. Para conseguir velocidades de 100 Mbps es necesario utilizar cable par trenzado con una categoría mínima de 5, un concentrador que soporte esta velocidad y tarjetas de red de 100 Mbps. Generalmente, los cables UTP cumplen bien con su función pero en situaciones concretas que requieran el máximo rendimiento de la red o existan muchas interferencias, puede ser necesario un cableado STP. En el nivel físico, las redes IEEE 802.3 utilizan codificación Manchester diferencial

### 2.6 Elementos de la Capa Internet

A continuación se describen los elementos que conforman a la capa Internet del modelo TCP/IP

#### 2.6.1 Protocolo IP

Los estándares **MIL-STD-1777** (*Militar Standard*) y **RFC-791** (*Request For Comments*) determinan el protocolo IPv4 para la interconexión de redes Internet o IP (redes que usan el protocolo IP). En Internet se

conectan redes individuales mediante **enrutadores** (r*outers)* (algunas veces denominados *gateway*s de red), el *router* realiza la operación de enrutar o determinar la ruta que debe seguir un paquete, mediante el uso de las direcciones IP (4 bytes), para llegar a su destino.

La identificación de un punto en la red requiere de vías simultáneas: direcciones MAC en capa 2, IP en la capa 3 y puerto en la capa 4, adicionalmente de la identificación de usuario de un servicio en particular.

#### 2.6.1.1 Direcciones IP

En el caso de redes IP que utilizan la versión cuatro, es necesario que cada sistema conectado a la red tenga asignada una dirección única de 32 bits, esta son las direcciones IP, esta es una dirección lógica que sirve para identificar a los equipos dentro de toda la red, sin importar a que tipo de red pertenezcan, estas direcciones sirven para determinar la ruta que deben seguir los datagramas o paquetes dentro de la red para llegar a su destino. Algunos sistemas, como los enrutadores que tienen interfaces con más de una red, requieren tener asignada una dirección IP a cada puerto o interfaz de red.

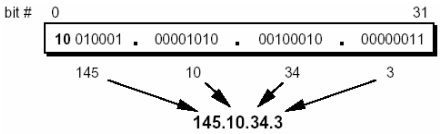
La primera parte de una dirección IP identifica la red a la cual pertenece el sistema (***host***), mientras que la segunda parte identifica al *host* o sistema que pertenece a dicha red

| Numero de Red | Numero de *Host* |
|---|---|

*Formato de Dirección IP*

El número de red también es conocido como prefijo de red, todos los *hosts* de una misma red comparten el mismo número de red o prefijo de red, pero tienen diferente números de *host*. De similar manera dos redes diferentes tienen diferentes números de red, pero pueden tener los mismos números de *host*.

Para hacer las direcciones IP más fáciles de leer y escribir, usualmente se expresan como cuatro números decimales, cada uno separado por un punto. Este formato divide las direcciones de 32 bits en 4 campos de 8 bits cada uno, separado por un punto, donde el valor de cada campo esta especificado por un numero decimal entre 0 y 255.




*Notación IP Decimal*

La gestión de direcciones la realiza la **IANA** (*Internet Assigned Numbers Authority*) que se encarga de asignar los número de red, dejando al usuario la asignación de los números de *host*, donde a cada nodo de red le corresponde un numero de *host* que debe ser único. El registro de las direcciones IP se opera desde el **DDN/NIC** (*Department of Defense Network/Network Information Center*).

##### 2.6.1.1.1 Clases de direcciones IP (*Classful Addressing*)

Para poder soportar diferentes tamaños de red, los diseñadores del protocolo IP inicialmente decidieron dividir las direcciones IP en clases, donde cada clase limita el número de *hosts* que puede tener cada red, mediante el tamaño del prefijo. Las clases son las siguientes:

| Prefijo (bits) | Numero Red | | Clase |
|---|---|---|---|
| 8 | 0xxxxxxx.z.z.z | 1.0.0.0 a 126.155.155.155 | A |
| 16 | 10xxxxxx.z.z.z | 128.0.0.0 a 191.255.255.255 | B |
| 24 | 110xxxxx.z.z.z | 192.0.0.0 a 223.255.255.255 | C |

*Classful Adressing*

#### 2.6.1.1.2 Direccionamiento IP sin Clase (*Classless Adressing*)

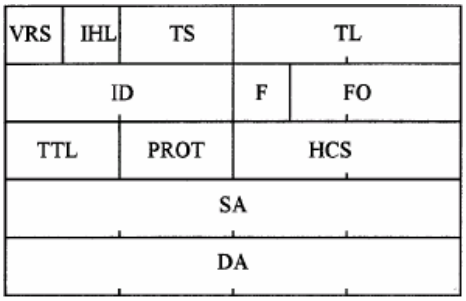
Debido a al naturaleza del esquema de direccionamiento *classful* se hace un uso ineficaz del limitado numero de direcciones IP, algunas redes son muy pequeñas (clase C) y solo pueden tener 256 *hosts*, por lo que, por ejemplo, una empresa pequeña que requiriera una red un poco más grande tenia que solicitar una o varias direcciones IP tipo C, por otro lado las empresas medianas y grandes solicitaban direcciones tipo B que puede alojar hasta 65536 *hosts*, desperdiciándose muchos números de *host* en muchos casos, algo peor ocurría con las direcciones IP de tipo C que pueden alojar hasta 16 777 216 *hosts*.

Conforme se fue agotando el espacio de direccionamiento IP ante el crecimiento desbordado de las redes IP y sobre todo de Internet, se empezó a idear un esquema para hacer más eficiente la asignación de direcciones IP, este consiste en un esquema en el que no hay clases de red, sino que se usan redes con un tamaño de prefijo de *host* que puede ser diferente a los del esquema *classful*.

El número de mascara determina el tamaño del prefijo de *host* de cada red, este tiene un formato similar al de las direcciones IP, por ejemplo el número de mascara: 11111111.11111111.11110000.00000000 que también se puede escribir como 255.255.240.0 significa que la red tiene un prefijo de *host* de 12 bits (igual al número de unos), con lo cual dicha red puede direccionar hasta 4096 *hosts*, usualmente la mascara de red se expresa por ejemplo 132.295.128.0/20 que también significa que esta red tiene un prefijo de *host* de 12 bits.

### 2.6.1.2 Formato de la Trama de IPv4

El formato de la trama (denominado datagrama) contiene los campos que se muestran a continuación para el protocolo IPv4. El protocolo IP no tiene previsto el control de flujo, la protección de la secuencia de datos u otros servicios ofrecidos del tipo *host* a *host*.




*Campos del Datagrama del protocolo IPv4.*

A continuación se describen estos campos y se clasifican de acuerdo a las funciones que realizan.

#### 2.6.1.2.1 Campos de Información General

**VRS:** (4 bits) Indica la versión del protocolo IP, la versión más usada es la IPv4.
**IHL** (*Internet Header Lenght*)**:** (4 bits) Indica la longitud del encabezado en unidades de 4 Bytes. El valor típico es 5 (que corresponde a 20 Bytes sin campo opcional).
**ToS** (*Type of Service*): (1 Bytes) Contiene información que permite gestionar la calidad de servicio **QoS** (*Quality of Service*) dentro de una red IP:

- **PROC** (*Procedence*): (3 bits) Permite designar a los datagramas una prioridad con 8 niveles que son: Control de red, control de interconexión de redes, crítico, pasaje rápido, *flash*, inmediato, prioritario y de rutina.
- **D:** (1 bit) Retardo admitido sobre el datagrama, que pueden ser el estado normal o el estado bajo.
- **T:** (1 bit) Conectividad admitida (normal o alto).
- **R:** (1 bit) Pérdida de datagramas (probabilidad para descarte de datagrama: normal o bajo).

#### 2.6.1.2.2 Campos de Información Para la Segmentación

**TL** (*Total Length*): (2 Bytes) Indica la longitud total del datagrama, incluyendo el encabezado, en unidades de Bytes. Por razones de fragmentación se usa un valor muy inferior al máximo permitido de 65535 Bytes. Por ejemplo se puede programar a los *routers* para aceptar datagramas de 576 Bytes como máximo. Es conveniente que la longitud total del datagrama no supere la utilizada en la red de transporte (por ejemplo: 1492 Bytes en IEEE 802.3). Con esto se logra reducir los problemas de fragmentación en capas inferiores.
**ID:** (2 Bytes) Identificador de dirección de origen, destino y protocolo de usuario. La identificación es única mientras dura el datagrama en la Internet.
**Flags:** (3 bits) Para informar de la segmentación y facilitar el ensamble de datagramas en el destino. Contiene la siguiente información mediante 2 de los 3 bits:

- **MF** (*More Flag*). (1 bit) Indica si es el final de la segmentación final o si existen más datagramas.
- **DF** (*Do not Fragment*): (1 bit) Indica si se ha efectuado o no una fragmentación de datos y si ella es autorizada para los *routers*.

**FO** (*Fragment Offset*): (13 bits) Indica la posición del datagrama en el mensaje original en unidades de 8 Bytes. En los segmentos sucesivos señala la cantidad de Bytes transmitidos hasta el momento. La longitud máxima del mensaje recibido desde TCP y segmentado por IP es 8x213 Bytes.
**TTL** (*Time To Live*): (1 Bytes) Tiempo de vida medido en intervalos de 1 segundo. En muchos casos es configurable y el valor recomendado es de 32 seg. Permite liberar la red de datagramas que no llegan a destino y que ocupan reservas de memoria.
**PROT** (*Protocol*): (1 Bytes) Indica el protocolo de capa superior que transporta, actúa como dirección de servicio SAP (*Service Access Point*). Puede tomar los valores decimales del 0 al 255), por ejemplo TCP tiene asignado el valor 6, UDP el 17, ICMP el 0, EGP el 08 y OSPF el 89.
**HCS** (*Header Checksum*): (2 Bytes) Sirve para realzar la detección de errores en el encabezado. El campo HCS cambia en cada *router* debido al cambio de TTL y Flags. Si se detecta un error en el encabezado el datagrama se descarta. TCP detecta falta de datos y solicita la retransmisión. Cabe recordar que IP no detecta errores en los datos, esto lo hacen TCP y UDP.

#### 2.6.1.2.3 Campos de Direcciones y Opcional

**SA** (*Source Address*): (4 Bytes) Dirección de origen del datagrama.
**DA** (*Destine Address*): (4 Bytes) Dirección de destino del datagrama.
**PAD** (*Padding*): (N Bytes) Para el final de encabezado (completa el número de Bytes minimos).
**Data:** Campo de datos del datagrama (mensaje segmentado desde la capa superior).
**OPT**: Campo de información opcional.

### 2.6.2 Funcionamiento del Protocolo IP

La operación de redes como X.25 o Frame Relay es en el modo orientado a conexión, lo cual corresponde a un circuito virtual (conexión lógica permanente establecida entre dos puntos en una red de paquetes), minetras que una red IP basa su operación en modo orientado a no conexión, que corresponde a el uso de datagramas que llevan toda la información necesaria para el enrutamiento en la red. La operación sin conexión requiere del análisis del nivel de protocolo Internet IP (función del *router*), en tanto en la operación con conexión una vez establecido el circuito virtual no requiere dicho tratamiento.

Un datagrama IP puede ser direccionado o enrutado mediante una tabla de ruta estática en la que se especifica la ruta que debe tomar el datagrama de acuerdo a los criterios del administrador de la red, estas rutas son fijas y no responden a los cambios en la topología de la red, los datagramas solo disponen de alternativas en caso de indisponibilidad de un enlace o *router,* a esto se le llama **enrutamiento estático,** por otro lado el **enrutamiento dinámico** responde a la topología de la red permitiendo que los enrutadores decidan la ruta de cada paquete considerando la congestión de la red, el número de saltos o enrutadores que tiene que atravesar un datagrama para llegar a su destino , el costo y el retardo de un enlace, entre otras cosas. Estos aspectos pueden demorar a un datagrama en la red, consumiendo buffer de memoria y capacidad de transporte e incluso puede mantenerlo en un ciclo entre *routers* indefinidamente (por ello se requiere el tiempo de vida TTL).

A continuación se describen los elementos funcionales más importantes del protocolo IP:

**Tiempo de Vida.** Para reducir el riesgo de demora o pérdida del datagrama se define el **TTL** (*Time To Live*), que indica el tiempo que el datagrama puede permanecer en la Internet. Como el datagrama consume memoria y recursos en la red, al transcurrir este tiempo (indicado en el campo TTL en segundos) el mismo se descarta. Cada ingreso de un datagrama a un *router* le descuenta una unidad de TTL, además en tanto el datagrama permanece en el buffer de un nodo se descuenta el valor de TTL en una unidad por seg.

El protocolo de capa 3 no se ocupa de la retransmisión, el encargado es el protocolo de capa 4 (TCP). El protocolo de destino debe detectar la ausencia de un datagrama correlativo mediante la información TL, Flag y FO, con lo que se interrumpe el ensamble. Un *router* intermedio no está autorizado a efectuar ensamble ya que no posee la seguridad que los distintos segmentos pasan por dicho *router*. El protocolo IP dispone del protocolo ICMP para enviar reportes cuando se produce un descarte debido a finalización de TTL. Un datagrama puede ser descartado por varias razones: final del tiempo de vida, congestión de la red y errores de bits en el encabezado.

**Calidad de Servicio.** En IP se tiene la oportunidad de definir la Calidad del Servicio o **ToS** (*Type of Service*) en los siguientes términos:

- Precedencia (importancia relativa del datagrama, 8 niveles).
- Retardo admitido del datagrama (2 niveles).
- Importancia para la seguridad del datagrama (2 niveles).

**Ensamble de Datos Fragmentados.** Mediante la información de longitud y offset del datagrama se realiza el ensamble de datos fragmentados para su transporte. Para este proposito se utilizan los siguientes recursos: La longitud de datos TL, *Offset* (desplazamiento) de fragmentación FO y la MF que indica si se trata del último datagrama. IP es responsable por la ruta de los datos pero no lo es por la integridad de los mismos. De esto se ocupa la capa 4 (TCP requiere la retransmisión automática). IP no permite el secuenciamiento, el control de flujo, la apertura y cierre de la conexión ni el reconocimiento del servicio. TCP se encarga de reconocer cuando un datagrama se ha perdido (por tiempo de vida o errores) en la Internet.

**Comandos IP.** El protocolo IP permite entre muchos otros los siguientes comandos:

**Add:** Añade interfaces, servidores, *hostnames*, *routers*, etc.
**Change:** Modifica la tabla programada mediante el comando Add.
**Delete:** Elimina las configuraciones realizadas mediante el comando Add.
**Cache:** Muestra la tabla de destinos enrutados recientemente.
**Counter:** Diversos contadores pueden ser configurados para obtener estadísticas (paquetes con error, etc).
**Dump:** Enlista el contenido de la tabla de rutas del enrutador.
**Enable:** Habilita diversas facilidades (*routing* ARP, *broadcast*, información RIP, etc).
**Interface:** Enlista las direcciones IP de las interfaces del *router*.
**Show ARP:** Muestra la lista de direcciones IP y las direcciones MAC asociadas.
**List:** Muestra la lista de comandos que permiten la configuración de IP.
**Ping:** Emite un comando ICMP *Echo Request* para verificar el estado del elemento con IP *Address* requerida. La respuesta es un comando ICMP *Echo Replay*.
**Route/Trace:** Enlista la ruta seguida por los datagramas en la red hacia un destino específico. Se envían datagramas con TTL sucesivamente creciente para que sean descartados e informados mediante ICMP.
**Static:** Muestra las rutas estáticas especificadas mediante configuración.
**Security:** Permite la configuración de seguridad (*keyword*, *password*, etc).

### 2.6.3 Enrutadores *(Routers)*

La interconexión (*internetworking*) de redes se efectúa de distintas formas dependiendo de los objetivos y tipos de redes involucradas. Los elementos usados para la extensión o comunicación de una red son*: hubs, switches, routers y gateways*.

Los *routers* funcionan en el ámbito de la capa 3 y por ello realizan un análisis del Protocolo Internet IP. Deben soportar distintos tipos de protocolos, por ejemplo TCP/IP, DECnet, IPX (Novell), AppleTalk, XNS

(Xerox). Interconectan redes LAN entre sí o una LAN con una WAN (X.25, Frame Relay, ATM). Permiten mejorar la eficiencia de la red ya que toleran distintos caminos dentro de la red. El *router* puede segmentar datagramas muy largos en caso de congestión, pero no pueden ensamblar datagramas. Un *router* se utiliza muchas veces como conversor de interfaz.

En conexiones de datos de baja velocidad el *router* puede ser colocado en el extremo del circuito de acceso al usuario para obtener supervisión de línea. En este caso, mediante el protocolo SNMP asociado a UDP/IP se puede gestionar el punto de acceso de usuario (función PING por ejemplo).

Los *routers* se pueden interconectar a alta velocidad mediante interfaces de 100 Mbps (mediante UTP o fibra óptica), a 1000 Mbps (mediante Gigabit Ethernet) y a otras velocidades más altas dependiendo de la tecnología e interfaces a que se conectan, por ejemplo, para formar redes de alta velocidad, existe una gran variedad de interfaces para inteconectar los *routers* con otros *routers* o con otros dispositivos, como pueden ser aquellos que se utilizan en redes WAN, switches y *routers* ATM por ejemplo, y conforme avanza la tecnología los *routers* son capaces de soportar mayores velocidades, del orden de Gbps. Usualmente el medio de transporte entre *routers* es una conexión LAN extendida (MAN). Normalmente el protocolo IP usado en una LAN puede ser transportado mediante una red SDH, una red ATM o directamente sobre interfaz LAN por fibra óptica.

Algunas ventajas de los *switches* (de capa 2) frente a los *routers* han determinado la idea de difundir el *switch* y usar el *router* solo cuando sea necesario. El *switch* tiene una menor latencia (retardo), una mayor capacidad de tráfico (*throughput*), una más fácil administración (concepto de gestión *plug and play*) y menor costo por puerto. Los *switches* de capa 2 crean redes planas. Ademas existen *switches* de capa 3 que simulan totalmente las operaciones de enrutamiento (*routing*). Se entiende por *switch* de capa 3 al equipo que realiza la operación de enrutamiento mediante acciones de hardware, en tanto que es un *router* cuando las mismas se realizan mediante acciones de software.

Una diferencia de importancia entre un *switch* y un *router* es que el *router* permite optimizar rutas cuando la red es muy grande, permite además disponer de caminos alternativos y reconfigurar la tabla de enrutamiento dinámicamente.

#### 2.6.3.1 Características de Selección de los Enrutadores

- **Eficiencia:** La eficiencia es la habilidad para seleccionar la mejor ruta con una utilización del CPU mínima.
- **Sumarización:** La sumarización de rutas se refiere a la posibilidad de estructurar la tabla de enrutamiento con grupos de rutas sobre un mismo enlace, es decir que en lugar de tener un registro para asociar cada ruta con su propio enlace, se asocian los enlaces a grupos de rutas. Esto permite reducir sustancialmente la capacidad de memoria utilizada por la tabla de enrutamiento.
- **Simplicidad:** Se refiere al software mínimo requerido y al *overhead* producido por los paquetes requeridos para la actualización de las tablas de enrutamiento. Por ejemplo, protocolos como RIP utilizan una parte del ancho de banda del enlace para realiza actualizaciones periódicas de las tablas de enrutamiento, mientras que OSPF o IS-IS lo hacen solo en caso de falla. Son más complejos pero solo ocupan al CPU solo en caso necesario, lo que en condiciones de funcionamiento normal minimiza la ocupación del ancho de banda.
- **Robustez:** La robustez se refiere a la habilidad para reponerse a fallas de hardware, condiciones de pérdidas de paquetes e implementaciones incorrectas.
- **Flexibilidad:** Se refiere a la adaptación a diversas circunstancias.
- **Convergencia:** Es la velocidad de actualización de la tabla de enrutamiento cuando se requiere una actualización (recálculo de las rutas). El **tiempo de convergencia** depende de la velocidad de detección de cambios en la red, selección de la ruta y propagación de los cambios. Los cambios realizados en un *router* y que por el momento no generan cambios en otros *routers*, pueden provocar *loops* de *routing*. Algunos problemas son detectados rápidamente como la interrupción (pérdida de portadora) de una línea serial. En cambio sobre una red Ethernet no existe indicación de interrupción (semejante a la pérdida de *carrier*). Si sobre un *router* se efectúa un *reset* tampoco se dispone de una indicación inmediata.

- **Escalabilidad:** Se refiere a la posibilidad de crecimiento. Normalmente la escalabilidad se encuentra limitada por razones operacionales más que técnicas.
- **Seguridad:** Referido al uso de medios para protección de la información de enrutamiento. El mecanismo de autentificación reduce potenciales inestabilidades.

### 2.6.4 Protocolos de Enrutamiento (*Routing Protocols*)

Se entiende por enrutamiento (*routing)* al proceso que permite determinar la mejor ruta para que un paquete llegue a su destino. Se puede efectuar mediante *switches* (capa 2 o 3) o *routers* de acuerdo con el tipo de redes involucradas. El *switch* se prefiere por el mínimo retardo que introduce, su bajo costo, sus pocas conexiones y su mínimo planeamiento, aunque usualmente el s*witch* solo se usa para interconectar redes LAN. Mientras que los *routers* se usan para interconectar redes LAN y redes WAN, por lo que requieren un mayor grado de configuración para interpretar correctamente la información de enrutamiento, ya que varias tecnologías y protocolos pueden estar involucrados.

El *switch* y *router* son elementos que aprenden de la red, analizan la dirección de cada paquete y pueden formar una tabla de direcciones (tabla de enrutamiento) que les permiten determinar la ruta que debe seguir cada datagrama para llegar a su destino.

Los *routers* tienen la capacidad de optimizar el camino del paquete de datos mediante el análisis del costo, el retardo de tránsito, la congestión de la red y la distancia medida como número de *routers* que tiene que atravesar el paquete en su trayecto. La tabla de enrutamiento (*Routing Table*) contiene solo el próximo paso en la red, en cada enrutador en particular, por lo que las rutas que van de un punto hacia un mismo destino pueden ser diferentes, dependiendo de las condiciones de la red.

Se han definido 2 tipos de protocolos de enrutamiento: los interiores y los exteriores al sistema autónomo **AS** (*Autonomous System*). Se denomina sistema autónomo **AS** (sistema interior o dominio) a un conjunto de subredes y *routers* que utilizan el mismo protocolo o el mismo control administrativo.

Los *routers* siguen el principio de **Mínima Acción** para determinar el mejor camino para los paquetes, esto significa que los enrutadores escogen las rutas basándose en diversos parámetros llamados métricas de tal manera que eligen las rutas más convenientes de acuerdo a esas métricas, por ejemplo, el menor número de saltos. Los algoritmos para determinar esta mínima acción son diversos.

La **métrica** es un estándar de medida que permite efectuar las operaciones de *routing*. Cada protocolo utiliza diferentes métricas o un conjunto de ellas para seleccionar las mejores rutas, entre las métricas se encuentra por ejemplo, la longitud del trayecto en número de *routers* utilizado en RIP (el primer protocolo de enrutamiento).

La **tabla de enrutamiento** es la responsable del enrutamiento del paquete en la red, esta tabla realiza un mapa de la topología de la red para determinar el próximo paso hacia el destino final. La métrica para una ruta particular es el agregado de varias características asignadas a un enlace, existen diversos tipos de métricas, algunos protocolos de enrutamiento utilizan solo una de ellas mientras que otros usan varias alternativas. Algunas posibles métricas de los protocolos de enrutamiento son las siguientes:

- **Calidad del enlace:** Referido a la existencia de errores en el trayecto.
- **Longitud del trayecto:** Referido al número de saltos o *routers* intermedios en la red.
- **Retardo de tránsito:** Referido al tiempo de propagación (medible mediante un *Ping* de ICMP).
- **Ancho de banda del enlace:** Referido a la capacidad de tráfico disponible entre *routers*.
- **Disponibilidad:** Referido al grado de ocupación del CPU del *router*.
- **Costo:** Toma en cuenta el valor de conexión de la ruta.

#### 2.6.4.1 Clasificación de los Protocolos de Enrutamiento

A continuación se indican los criterios de clasificación de los protocolos de enrutamiento:

**Estático/Dinámico:** Esta característica se refiere a la posibilidad de fijar una ruta determinada en el caso estático (*route of last resort*) o rutas variable o dinámicas para una adaptación de las rutas en tiempo real.

**Simple/Múltiple:** Referido a la posibilidad de permitir la multiplexación por varias líneas. Cuando es posible el múltiple trayecto las vías para distribuir los paquetes son dos: balanceo por paquete (distribuidos de acuerdo con la métrica) y balanceo por destino (se asignan rutas por cada nuevo destino).
El **balanceo por paquete** es similar al esquema *round-robin* (todos contra todos con el mismo nivel de métrica frente a los demás), para rutas de igual costo. El **balanceo por destino** tiende a preservar el orden de los paquetes. TCP acomoda en orden los paquetes pero puede degradarse el desempeño. Si bien IP es un protocolo orientado sin-conexión (*connectionless*) los *routers* preservan en lo posible la ruta.

**Plano/Jerárquico:** En la topología plana todos los enrutadores tienen igual jerarquía, en la jerárquica los enrutadores forman un *backbone* para el tráfico principal. Los protocolos OSPF y IS-IS son ejemplos de protocolos de enrutamiento que utilizan estructura jerárquica.

**Domain:** Los protocolos de enrutamiento son distintos si trabajan en el mismo dominio (intra-dominio) o entre dominios (inter-dominio).

**Algoritmo:** Se disponen de dos tipos de algoritmos para obtener las tablas de enrutamiento:

- ***Distance Vector***: El algoritmo vector-distancia desarrollado por Bellman-Ford. Este algoritmo requiere de datos sobre el número de saltos y el costo para definir las rutas. El costo puede indicar un valor en $/min o bien por preferencia (ponderación definida por el retardo, por ejemplo, un peso de 1 para 128 kbps y de 10 para 64 kbps). Es usado por protocolos como RIP, Hello y BGP.
- ***Dijkstra Algorithm***: Este es un protocolo de estado de enlace **LSA** (***Link State Advertisements***) que acumula información acerca de las rutas y enlaces de la red, verificando cual es su estado a cada momento, de tal modo que cuando ocurre algún cambio en la topología de la red, las tablas de enrutamiento se actualicen inmediatamente, esta información es usada para reconocer el camino más corto a cada nodo. Es usado por OSPF e IS-IS.

#### 2.6.4.2 Protocolos de Enrutamiento de Capa 2

Para que los enrutadores se puedan comunicar con los *switches* o segmentos de red que están conectados a él necesitan un conjunto de protocolos y procesos. El más simple de los procesos que permiten definir direcciones y rutas es el de resolución de direcciones MAC en una red LAN, que se realiza con alguno de los protocolos que se indican a continuación:

**Resolución de direcciones MAC**

**ARP** (*Address Resolution Protocol*) RFC-0826: Este protocolo es usado para anunciarse mediante direcciones de capa IP. Permite comunicarse con un usuario IP sin conocer la dirección MAC del mismo. ARP envía un mensaje *ARP Request* para solicitar la dirección MAC correspondiente a una dirección IP para todas las direcciones MAC en la red LAN (*broadcast*). La respuesta es un paquete *ARP Respond* con la dirección MAC que corresponde a la dirección IP indicada.

Un datagrama ARP es un paquete de corta longitud que contiene los siguientes campos:

- Identificador del tipo de hardware (2 Bytes): Para identificar que tipo de dispositivo de red envía el paquete.
- Identificador de protocolo (2 Bytes): Para identificar el protocolo de red usado por el dispositivo de red, por ejemplo al protocolo IP le corresponde el 0800
- HLEN/PLEN (2 Bytes): Indica la longitud de la dirección MAC y de la dirección IP (la longitud normal es 6 y 4 Bytes respectivamente)
- Identificador de mensaje (2 Bytes): Para indicar si es un ARP *request* o un ARP *response*
- Direcciones MAC e IP de origen y de destino.

Cada nodo mantiene una memoria denominada *ARP Cache* con las direcciones de las puertas IP y las correspondientes direcciones MAC, esta memoria es actualizada cada 15 minutos. Se entiende por *cache* una memoria que contiene los datos utilizados recurrentemente, en este caso referido a direcciones y rutas.

**Proxy ARP** RFC-1027: Un *router* utiliza el proxy ARP para ayudar a un *host* en el reconocimiento de direcciones de otras redes y subredes vecinas.

**RARP** (*Reverse ARP*) RFC-0903: Funciona con estaciones sin disco duro que no pueden guardar las direcciones IP. Su función es requerir la dirección IP cuando se conoce la dirección MAC. Los protocolos ARP y RARP no utilizan paquetes IP en forma directa, sin embargo generan un datagrama propio de características similares.

**Hello:** Este protocolo habilita a los elementos de red para reconocer las direcciones MAC mediante paquetes pequeños de presentación. Cuando un nuevo elemento se conecta a la red genera un mensaje Hello en forma de *broadcast*, el mismo es emitido en forma periódica para indicar que continúa activo. Para cada *Hello message* se responde con un *Hello replies* para configurar la tabla de direcciones.

**STP** (*Spanning Tree Protocol*): En las redes construidas mediante *switches* Ethernet se debe cuidar que no ocurran *loops*, que se originan cuando se tienen caminos y rutas duplicadas (redundantes) y se generan paquetes duplicados para uno o más destinos. El uso de STP permite eliminar el problema de los *loops* y mantener las ventajas (redundancia de enlaces). STP fue desarrollado originalmente en Digital DEC y luego fue incorporado al estándar **IEEE 802.1d**. Este protocolo permite identificar los *loops* y mantener activo solo un puerto del *switch*, se asigna a cada puerto un identificador (la dirección MAC y una prioridad), la prioridad de la puerta se puede asignar en términos de costo.
El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg), para que cuando se detecte un cambio en la configuración de la red se recalcule la distancia (suma de costos) para asignar una nueva puerta activa. Las decisiones se toman en el propio *switch*. Los mensajes son *Configuration* y *Topology-change*, los campos del mensaje de configuración incluyen 35 Bytes y el de cambio de topología solo 4 Bytes iniciales.

El mensaje de configuración contiene:

- 2 Bytes para indicar el Identificador de Protocolo y 1 Byte para la Versión.
- 1 Byte para identificar el Tipo de Mensaje (Un valor de 0 para configuración y de 128 para cambio de topología).
- 1 Byte de Flag para indicar el cambio de configuración de la red.
- 8 Bytes para identificar la raíz (*Root*) y 4 Bytes para identificar el costo de la ruta.
- 8 Bytes para identificar el *switch* y 2 Bytes para identificar el puerto del mismo.
- 2 Bytes para identificar el tiempo de emisión del mensaje (*Age*) y 2 Byte para indicar el tiempo máximo de vida.
- 2 Bytes para indicar el período de intercambio de mensajes de configuración *Hello*.
- 2 Bytes para indicar el tiempo de espera para emitir un mensaje en caso de detectar un cambio de configuración.

#### 2.6.4.3 Protocolos de Enrutamiento de Capa 3

La mayor jerarquía de enrutamiento es el **AS** (*Autonomous System*) que es una colección de redes bajo una administración de dominio común. Los protocolos de resolución interior **IGP** (*Interior Gateway Protocol*) permiten la comunicación interna del dominio AS, en tanto que, los de resolución exterior **BGP** (*Border Gateway Protocol*) lo hacen entre dominios distintos. Así un AS es un grupo de *routers* que utilizan un mismo protocolo de enrutamiento. Cada AS puede ser dividido en un número de áreas y un *router* con múltiples interfaces puede participar de múltiples áreas, estos *routers* se denominan *routers* de borde y mantienen separadas las bases de datos topológicas de cada área.
Un área puede contener a todos los *router*s que inician con la misma dirección IP, por ejemplo, 150.98.05.x, en este caso el uso de la mascara de red 255.255.255.0 puede ser de utilidad para separar las áreas. La

expresión dominio se refiere a la porción de red donde los *routers* poseen la misma base de datos topológica. La topología del área es invisible a elementos fuera del área. El dominio es usado para intercambios con AS. Para resolución interior se utilizan los protocolos RIP, IGRP y OSPF y para resolución exterior EGP y BGP.

#### 2.6.4.3.1 Protocolo RIP (*Routing Information Protocol*)

El protocolo RIP es del tipo de resolución interior IGP indicado como inter-AS y esta definido en la RFC-1058. La métrica utilizada es del tipo número de saltos (vector distancia de 4 bits), donde un número de saltos superior a 15 se entiende como inalcanzable. Por ello el RIP es válido para redes pequeñas.
Desde el punto de vista del modelo de capas, RIP trabaja sobre UDP con el número de puerto 520 (decimal), en cambio que BGP trabaja sobre TCP (realiza una conexión con control de errores y de flujo). El máximo tamaño del mensaje es de 512 Bytes (sin contar UDP/IP). Los mensajes son de *Request* (pedido de transferencia de la tabla de rutas) y de *Response* (respuesta al pedido). Normalmente el *request* es un mensaje con dirección *broadcast*. RIP no puede manejar direcciones con máscara de subred variable.

El paquete del protocolo RIP permite la actualización de las tablas de enrutamiento en los *routers*, el contenido en la dirección IP y el valor de la métrica (el número de saltos desde 1 a 15). La tabla de enrutamiento formada por RIP contiene la siguiente información: Dirección de destino, próximo paso, distancia, *Timer* y *Flag*.

La tabla de enrutamiento solo mantiene la mejor ruta al destino, por lo que cuando una ruta mejor es detectada se reemplaza la anterior. Cada *router* actualiza un cambio y lo propaga a los demás, por lo que el tiempo de convergencia es alto. RIP requiere datos de ruta para actualizar las tablas y periódicamente anuncia la presencia y difunde los cambios que detecta en la red. RIP utiliza el algoritmo *distance vector*.

Los paquetes de RIP son intercambiados en forma periódica cada 30 seg. (*Upgrade*). Este mecanismo de transmisión periódica carga la red con información de *routing*. Si el tiempo de *upgrade* supera el valor de 90 seg. la ruta de salida se considera inválida, si se supera el tiempo de 270 seg (denominado *Flush Timer*) la ruta se elimina de la tabla de rutas. El campo de métrica permite un máximo de 15 saltos (*Count Hop*), por lo que si es mayor se considera un destino inalcanzable. Se utiliza un mecanismo denominado *Split Horizont* que permite evitar información sobre rutas que retornan al origen generando *loops* de *routing* entre 2 nodos.

##### 2.6.4.3.1.1 Campos del Protocolo RIP

- **Command:** (1 Byte) Identifica si se trata de un requerimiento o una respuesta. Se solicita el envío de la tabla de rutas y se responde con toda o parte de la misma.
- **Version:** (1 Byte) Identifica la versión del protocolo RIP.
- **Reserved:** (2 Bytes) No utilizados.
- **Address:** (2 Bytes) Identifica la dirección de familia de protocolo (para IP el valor decimal es 2).
- **Address IP:** (4 Bytes) Dirección IP del destino a la que corresponde la métrica inferior. En un mensaje RIP de respuesta pueden reportarse un máximo de 25 destinos por paquete. Las tablas de enrutamiento más grandes requieren múltiples paquetes.
- **Metric:** (4 Bytes) Indica el número de saltos al *router* de destino. El valor 16 corresponde a inalcanzable.

#### 2.6.4.3.2 Protocolo IGRP (*Interior Gateway Routing Protocol*)

Este protocolo es para enrutamiento en AS. Es un protocolo que usa el vector distancia como RIP. Emite la totalidad de la tabla de rutas al inicio y solo los cambios en períodos preestablecidos como actualización. Mientras RIP usa solo una métrica (con un número de saltos máximo de 16) IGRP utiliza una combinación de métricas: retardo, ancho de banda, confiabilidad y carga del enlace (estos dos últimos se evalúan mediante un número desde 1 a 255).
Todos los *routers* mantienen la tabla de rutas de los vecinos para usarlo en el algoritmo de convergencia. Los tipos de paquetes involucrados se denominan: *Hello* (paquete *multicast* emitido para indicar la presencia)*; acknowledgment* (paquete de reconocimiento)*; update* (paquete emitido en forma *unicast* a un nuevo *router* en la red)*; querry; replay and request* (para solicitar información en forma *unicast*).

#### 2.6.4.3.3 Protocolo OSPF (*Open Shortest Path First*)

OSPF es desarrollado para IP como protocolo de *gateway* interior **IGP**. Este protocolo se creó para mejorar al protocolo **RIP**. OSPF es un protocolo abierto (especificación de dominio público) y se encuentra especificado en la RFC-1583. El algoritmo utilizado es el *Dijkstra Algorithm*. Es un protocolo de estado de enlace **LSA** (*Link State Advertisements*) que acumula información usada por el algoritmo **SPF** (*Shortest Path First*) para reconocer el camino más corto a cada nodo. OSPF es un protocolo intra-AS que dispone de una base de datos topológica que contiene la información recibida mediante LSA (Avisos del estado de los enlaces).

Cuando se inicia el algoritmo SPF espera que las capas inferiores informen de la operabilidad del enlace, cuando las interfaces están operacionales utiliza el mensaje *Hello* para adquirir información de los *routers* vecinos. En una red pequeña la dirección de los *routers* vecinos puede ser configurada manualmente, sobre una red mayor se utiliza la dirección *multicast* 224.0.0.5 reservada para esta aplicación de Hello. Los *routers* reconocen esta dirección y también las redes LAN, por lo que no puede ser usada para dirección de usuarios.

Cada *router* en operación normal emite los mensajes de LSA en forma periódica (valor típico 5 seg). OSPF soporta *routing* del tipo *multi-path* y **ToS** (*Type-of-Service*). El ToS permite efectuar operaciones de prioridad para datos urgentes sobre protocolo IP. Soporta además diferentes métricas (requiere el número de saltos, la velocidad de comunicación, la congestión de tráfico, el costo de la ruta y la prioridad). La métrica por default de OSPF está basado en el ancho de banda (el valor de métrica es inverso al ancho de banda).

El protocolo OSPF se adapta mejor a redes jerárquicas. La principal decisión es indicar que *router* se incluyen en el *backbone* y cuales en cada área. Una topología jerárquica incluye:

- Nivel de **acceso** (conexión a usuarios mediante *routers* o *switches* de capa 2).
- Nivel de **distribución** (que conecta a los *routers* de borde de área e implementa mecanismos de seguridad y DNS).
- Nivel ***Core*** para formar el *backbone* de la red (este nivel dispone de acceso a la Internet mediante *routers* de Borde).

Los dos aspectos más críticos respecto de las áreas son la determinación de la dirección y la conexión al *backbone*. Una forma de asignar direcciones IP en un medio ambiente OSPF es asignar números de red separados por áreas. Se asignan direcciones de red por área y de subred y *hosts* en el interior del área. El *router* que conecta al área con el *backbone* se denomina *router* de borde (*Bourder*). Es conveniente tener más de un *router* por borde de área. La redundancia permite prevenir la partición de redes y además permite obtener ancho de banda adicional en caso de tráfico elevado.

El tiempo de convergencia depende del número de *routers* y el tamaño del área (típicamente entre 6 y 46 seg). La convergencia en OSPF es mejor que en otros protocolos y se logra mediante dos componentes:

- La detección de cambios de la topología de la red (por detección de falla del enlace o por ausencia del paquete *Hello* luego de un tiempo denominado *dead time*).
- El recálculo de *routers* (el *router* que detecta la falla del enlace emite a los otros un paquete de estado de enlace).

El paquete OSPF trabaja sobre IP (protocol=89) y contiene 24 bytes de encabezado de longitud. A continuación se describen sus campos.

##### 2.6.4.3.3.1 Campos del Protocolo OSPF

**Version:** (1 Byte) Indica la versión de OSPF utilizada.
**Type:** (1 Byte) Especifica uno de los 5 tipos de paquetes OSPF:
- *Hello:* Emitido en forma regular para establecer relaciones con *routers* vecinos.
- *Database Description*: Describe la base de datos topológica y se intercambia con *routers* adyacentes.
- *Link State Request*: Para solicitar partes de la base de datos topológica cuando se descubren cambios.

- *Link State Update*: Responde al mensaje anterior. Existen 4 tipos de campos del tipo LSA:
  - *Router Link Advertisements:* Describe el estado de enlace entre *routers* de una área.
  - *Network LA*: Describe todos los *routers* que se conectan a la red multiacceso.
  - *Summary LA*: Resume las rutas y destinos de salida del área.
  - *AS External LA*: Describe las rutas de destino al exterior de la AS.
- *Link State Acknowledgment*: Reconoce el mensaje anterior para confirmar la recepción.

**Length:** (2 Bytes) Especifica la longitud total del paquete, incluido el encabezado.
**Router ID:** (4 Bytes) Identifica el *router* que emite el paquete.
**Area ID:** (4 Bytes) Identifica el área. En OSPF los paquetes se asocian a un área solamente.
**Checksum:** (2 Bytes) Que realiza un chequeo del paquete completo.
**Authen Type:** (2 Bytes) Indica el tipo de autentificación. Es obligatoria y configurable.
**Authen:** (8 Bytes) Información de autentificación.

#### 2.6.4.3.4 Protocolo EGP (*Exterior Gateway Protocol*)

Este protocolo es del tipo interdominio (RFC-0904). Ha sido reemplazado en la práctica por el BGP que se indica a continuación. Inicialmente determina los *routers* vecinos, verifica luego la presencia *on-line* y envía periódicamente información de actualización de la red. Los campos de este protocolo involucran 10 Bytes fijos y una carga útil de datos variable. Los bytes fijos indican la versión del protocolo (1 Byte), el tipo y subtipo de mensaje (2 Bytes), información de estado (1 Byte e indica problemas, violaciones, etc), información de *checksum* (2 Bytes para detección de error), número de sistema AS (2 Bytes), numeración secuencial de paquete (2 Bytes) y datos (longitud variable).

#### 2.6.4.3.5 Protocolo BGP (*Bourder Gateway Protocol*)

El protocolo BGP (RFC-1771) reemplaza al EGP en Internet y trabaja sobre TCP. Este tipo de protocolo permite el tráfico sin *loops* entre sistemas autónomos **AS**. Permite el tráfico dentro de un AS entre *routers* pares (**IBGP** para *Interior*) o entre sistemas autónomos (**EBGP** para *External*) y el pasaje por un sistema autónomo que no opera con BGP. Normalmente es usado entre operadores ISP (*Internet Service Provider*). La versión IBGP es más flexible, entrega varias vías de conexión en el interior del AS y dispone de una vista del exterior gracias a EBGP.

Cuando un *router* se conecta a la red BGP permite intercambiar las tablas de enrutamiento completas. Pero las mismas se intercambian en forma parcial cuando existen modificaciones. BGP utiliza como protocolo de transporte a TCP (utilizando el puerto 179). Cuando dos *routers* intercambian información de *routing* (con el puerto TCP activo) se denominan *Peers* o *Neighbors*. Una actualización de la tabla de rutas se propaga a los *routers* pares vecinos. El mapa de rutas es usado en BGP para controlar y modificar la información de *routing* y para definir las condiciones de redistribución de rutas entre dominios de *routing*.

BGP utiliza la información de *routing* intercambiada para generar un mapa de rutas AS libre de *loops*, solo un camino es conservado en la tabla de rutas y es el que se propagada a otros *routers*. La decisión entre distintos caminos al mismo destino se realiza mediante los siguientes atributos:
- El próximo paso (*Next Hop*).
- La ponderación de peso (por lista de acceso o mapa de ruta, se prefiere el camino de mayor peso ponderativo).
- La preferencia de ponderación local asignada por el operador (para selección de caminos con igual ponderación).
- El origen de la ruta y la longitud del camino.

BGP v4 soporta el *routing* interdominio del tipo *classless*, es decir con una máscara de red variable. En BGP se utiliza también el concepto de *routers Cluster* (grupo) que consiste en una secuencia route-reflector-cliente. El *router* intermedio refleja los paquetes entre *route* y cliente. El encabezado del paquete ocupa 19 Bytes y el mensaje tiene longitud variable.

##### 2.6.4.3.5.1 Campos del Protocolo BGP

**Marker:** (16 Bytes) Mensaje de autentificación que el receptor puede reconocer.
**Length:** (2 Bytes) Longitud total del paquete en número de bytes.
**Type:** (1 Byte) Identifica el tipo de mensaje de datos que sigue a continuación.
**Data:** Mensaje de longitud variable con los siguientes casos.

- *Open Message*: *(*14 Bytes) Provee los criterios para el intercambio entre *routers*. Contiene el tiempo en seg. que se espera para declarar un enlace no-funcional, este tiempo se conoce como *hold-time*. Contiene una lista de parámetros opcionales como la información de autentificación.
- *Update Message*: Sirve para actualizar las tablas de enrutamiento, su longitud es variable. Algunos tipos de mensajes de *update* son: longitud total de un trayecto, atributos de un trayecto (origen, próximo paso, grado de preferencia, etc), rutas agregadas, etc.
- *Notification Message*: Indica condiciones de error a otros equipos. Por ejemplo: error en el encabezado del mensaje, finalización del tiempo (*Hold Time*), evento no esperado, error de datos (error en la lista de atributos, próximo paso inválido, etc).
- *Keep-alive Message*: Se utiliza para informar que el equipo está activo.

#### 2.6.4.3.6 Protocolo IS-IS (*Intermediate System*)

Este protocolo permite el intercambio de información de *routing* entre sistemas intermedios (*intradomain*) (ISO-10747), está basado en un desarrollo original de DECnet. Desde el punto de vista de las funciones es similar a OSPF (pero no son compatibles), ambos son del tipo estado de enlace (*Link State*). Permite funciones no soportadas en RIP, como son jerarquías de *routing*, separación de trayectos, tipo de servicio ToS, soporta la autentificación, soporta una máscara de subred de longitud variable.

IS-IS utiliza una métrica con valor máximo de 1024, es arbitraria y es asignada por el administrador de red, un enlace simple puede tener un valor máximo de 64. La longitud del enlace es calculada por la suma de las ponderaciones individuales. Otras métricas adicionales son: el retardo del enlace, los costos asociados al enlace y errores en el enlace. Un mapa de estos 4 tipos de métrica permite formar la QoS en el encabezado del paquete **CLNP** (protocolo de capa 3 en el modelo ISO) y calcular la tabla de enrutamiento de la red.

Existen 3 tipos básicos de paquetes en IS-IS: el *Hello*, el paquete de *Link State* y el paquete de número secuencial. El formato de los paquetes es complejo y contiene en esencia 3 diferentes partes lógicas.

#### 2.6.4.3.6.1 Campos del Protocolo IS-IS

**OH:** (8 Bytes) de *OverHead.* Encabezado común que contiene un byte para cada uno de los siguientes mensajes:

- **IDE:** Identificador del protocolo IS-IS (corresponde a 1 Byte con valor 131).
- **LEN:** Longitud del encabezado (corresponde a los 8 Bytes de longitud).
- **PRO:** Versión del protocolo.
- **ID:** Identifica la longitud de la porción de dominio ID en la dirección NSAP.
- **PAC:** Identifica el tipo de paquete: *Hello*, *link state* o de numeración secuencial.
- **VRS:** Versión del protocolo.
- **RSV: (**1 Byte) Reservado (todos ceros).
- **AR:** Dirección de área máxima, número máximo de direcciones en el área.

#### 2.6.4.3.7 *Tag Switching* y MPLS

Es un diseño de Cisco para el *Backbone* de una red IP cuando se trabaja a alta velocidad (por ejemplo, Gigabit Ethernet). Es un avance de la técnica **MPLS** (*Multiprotocol Layer Switching*). La arquitectura *Tag Switch* se encuentra en la RFC-2105

Luego de que las tablas de enrutamiento convergen (usando protocolos de *routing*) los distintos *routers* asignan una etiqueta (*tag)* para cada ruta posible (dicha *tag* se encuentra como *header* de capa 2 o 3). El *tag* es corto y de longitud fija que es mejor manejado que la tabla de enrutamiento (se puede asimilar al identificador de trayecto virtual VPI de ATM). Las *tags* generados localmente en el *router* se intercambian con los otros mediante el protocolo **TDP** (*Tag Distribution Protocol*). Este protocolo permite distribuir, requerir y actualizar la información de *tag.*

El *tag switching* consiste de dos componentes: el *forwarding* (responsable de la transferencia de paquetes) y el control. La información de *tag* se memoriza en una base de datos de información realizada a tal efecto y denominada **TIB** (*Tag Information Base*). Los paquetes que circulan en la red llevan el *tag* de identificación y no requieren de acciones de tabla de rutas. El *tag* puede ser una simple ruta *unicast* o *multicast*, o un identificador de flujo de tráfico (por ejemplo, para el caso de *Netflow* donde se identifica el flujo mediante direcciones IP, puertos y políticas administrativas). Por otro lado, *tag switching* puede trabajar con QoS mediante información de prioridades.

## 2.7 Elementos de la Capa de Transporte

### 2.7.1 Protocolo TCP

Los protocolos de la capa de trasporte permiten efectuar las siguientes funciones generales:

**Segmentación y Ensamble:** El proceso de segmentación se aplica para tener una mayor eficiencia en el control de errores, para lograr un acceso más equitativo al medio de transporte y para requerir un tamaño de memoria buffer inferior. Sin embargo, la segmentación en paquetes de corta longitud genera un incremento en el tiempo de procesamiento y una menor eficiencia de datos. Se entiende por eficiencia la relación entre Bytes de datos **PDU** (*Protocol Data Unit*) y Bytes de encabezado. La relación entre la velocidad y el tamaño del datagrama determina la eficiencia y el acceso equitativo.

**Control de Errores y de Flujo:** Mediante campos de control apropiados se pueden detectar la ausencia o errores de datos y requerir la retransmisión. El protocolo IP detecta errores en el encabezado y descarta el datagrama. El protocolo TCP detecta errores en el encabezado y falta de segmentos de datos y solicita la retransmisión. El protocolo UDP no realiza la retransmisión de datos.

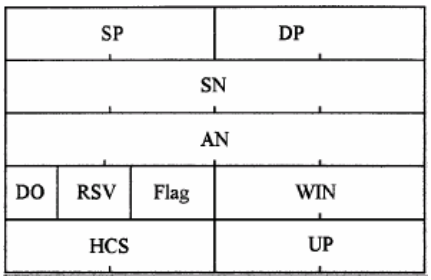
**Control de Conexión:** Se trata de servicios orientados a conexión en TCP y a no conexión en IP. En el primer caso se establece una conexión virtual con 3 fases: Establecimiento de conexión, transferencia de datos y terminación de conexión.

#### 2.7.1.1 Trama TCP Para Internet

El protocolo TCP puede entregar los siguientes servicios:

- Multiplexación para varios puertos de usuario.
- Gestión de la conexión (Inicio, mantenimiento y terminación).
- Transporte de datos (full-dúplex, ordenamiento, control de flujo, chequeo de errores).

Tratándose el protocolo TCP de un servicio orientado a conexión el funcionamiento incluye el establecimiento y finalización de la llamada. La estrategia de transferencia de datos incluye la retransmisión, la detección de duplicación y el control de flujo.



*Trama TCP*

**2.7.1.2 Campos de TCP**

**SP** (2 Bytes): Identifica el puerto (*Port TCP*) de acceso al servicio origen en TCP. Se trata de direcciones TSAP que se numeran desde 1 a 225 para los protocolos más conocidos (Echo:7, SMTP:25, FTP:21, Telnet:23, Gopher:70, y Web:80). Desde la puerta 256 a la 1023 se reserva para aplicaciones UNIX. Las aplicaciones propietarias llevan la dirección de puerto desde la 1024 hasta la 49151, las direcciones superiores a 40152 se asignan en forma dinámica. La combinación de la dirección IP y el puerto TCP/UDP es conocida como ***socket*** cuya asignación puede estar predeterminada (para protocolos conocidos) o se asigna entre los valores no utilizados (para las aplicaciones nuevas).
**DP** (2 Bytes): Identifica la puerta de acceso al servicio de destino. Tiene una estructura igual a la de SP.
**SN** (*Sequence Number*): (4 Bytes) Número secuencial del primer octeto de datos en el segmento para la puerta correspondiente. Permite el proceso de requerimiento de retransmisión automática **ARQ**. La longitud máxima del mensaje de capas superiores que puede segmentar TCP es de 232 Bytes, la longitud máxima del segmento que puede entregar a IP es de 216 Bytes.
**AN** (4 Bytes): Contiene el número de secuencia del próximo Byte que TCP espera recibir. Es un reconocimiento ACK de los Bytes recibidos.
**DO** (*Data Offset*): (4 bits) Número de palabras de 4 Bytes del encabezado.
**RSV** (6 bits): Reservados.
**Flags** (6 bits): Son bits utilizados para señalar la validez de otros campos y para el control de conexión:

- **URG:** (1 bit) Indica la existencia del puntero urgente en los datos (UP al final del *header*). Se trata de la función *Break* que notifica a la aplicación del TCP receptora que los datos son urgentes y deben ser presentados de inmediato en pantalla.
- **ACK:** (1 bit) Indica la existencia del campo de reconocimiento (AN al inicio del *header*).
- **PSH:** (1 bit) Función *push* que envía los datos desde un usuario (login remoto) cuando se presiona *Return*. Los datos son transferidos por TCP y presentados en la aplicación del otro extremo.
- **RST:** (1 bit) Indica que se debe realizar un *Reset* de conexión debido a un error grave.
- **SYN:** (1 bit) Usado para iniciar la conexión entre nodos. Se usa solo en el primer paquete de la conexión, en éste el primer byte de datos se numera como SN+1. El valor SN es un número de 4 bytes
- **FIN:** (1 bit) No más datos desde el emisor. Usado para iniciar la desconexión del enlace TCP.

**WIN** (*Window*): (2 Bytes) Crédito para control de flujo. Una PC tiene una capacidad de buffer limitada (4 kBytes) equivalente a 4 tramas de Ethernet de 1 kByte. Un crédito 0 detiene la emisión de datos.
**CS** (*Checksum*): (2 Bytes) Control de error sobre el encabezado y la carga útil. Permite la detección de errores para realizar la retransmisión.
**UP** (*Urgent Pointer*): (2 Bytes) Puntero que indica la cantidad de datos urgentes (identifica el final de los datos urgentes en el campo de datos que deben tratarse con prioridad).
**OPT:** Opcional de longitud variable.
**Data:** Datos de capas superiores.

Si la conexión al medio de enlace se supone mediante una LAN del tipo IEEE 802.3, se dispone de los campos de dirección **SAP** dentro del protocolo LLC y **SNAP** adicional. Las direcciones son:

- En Ethernet IEEE 802.3: IP=0800, ARP=0806 y RARP=8035.
- En SNAP (*Sub-Network Address Point*). Consta de 2 campos: 3 Bytes para el identificador de versión de protocolo **IP** y 2 Bytes para identificador de SAP (0800 para TCP/IP y 0600 para XNS).

– La dirección SAP en la capa IP se determina mediante el campo *Protocol* y en TCP/UDP se identifican mediante dos Bytes de *Port*.

#### 2.7.1.3 Funcionamiento de TCP

A continuación se describen los elementos funcionales de TCP:

**Inicio de Conexión:** Se trata de un saludo de 3 pasos. Cada extremo informa el número secuencial SN que pretende utilizar. El primer paquete lleva la bandera SYN=1 y el número secuencial SN=X (se genera mediante un contador de 32 bits que se incrementa cada 4 µseg y de período 5 horas). La respuesta a este paquete consiste en SYN=1 y ACK=1 más el propio número secuencial SN=Y y el acuse de recibo AN=X+1 (acuse de recibo del valor X). El tercer paso es responder al paquete anterior con ACK=1 y el acuse de recibo AN=Y+1.

**Retransmisión:** Mediante el mecanismo de reconocimiento se puede pedir la retransmisión de segmentos cuando estos llegan corrompidos por errores o les faltan segmentos intermedios. Es de fundamental importancia cuando las capas inferiores de la red no prevén la retransmisión (tal es el caso de Frame Relay y ATM). Las redes Ethernet (IEEE 802.3) y el protocolo PPP tienen desactivado el mecanismo de control en el protocolo LLC (tampoco corrigen errores). La capa 3 (Internet) no se ocupa de la confirmación de datagramas. Es TCP quien confirma, para cada puerta individual, los segmentos recibidos. La combinación de los campos AN y WIN permite el reconocimiento y el control de flujo.
Cuando se requiere emitir una secuencia de N bytes de datos, TCP coloca la bandera PSH=1 (empujando la emisión inmediata) y SYN=1, en tanto que la numeración secuencial es SN=X. El receptor retorna un mensaje con ACK=1 y la confirmación AN en el valor X+N+1 y el valor de la ventana WIN. Cuando existe un error se envía las banderas RST, SYN, ACK=1.

**Control de Flujo:** El mismo mecanismo de reconocimiento permite regular el flujo de datos en el protocolo TCP. El control de flujo de datos se complica debido al retardo entre entidades TCP y por la pérdida de segmentos. Además debe considerarse la posibilidad de arribo de segmentos fuera de orden y a la pérdida de segmentos con información de crédito. Sin el control de flujo los datos pueden superar la capacidad del buffer de recepción antes de ser procesados.

Se hace uso de dos elementos, AN y el crédito o ventana (*Window*):

– AN=H reconoce hasta la secuencia (H-1) e indica que espera la secuencia H
– El crédito WIN=K autoriza la transmisión hasta la secuencia (H-1)+K.
– La capa 2 en Frame Relay y ATM implementan alarmas para desencadenar un control de flujo de los extremos.
– En la capa 4 en TCP implementa un control de flujo mediante **WIN** que indica el buffer disponible para la recepción. Cuando TCP detecta errores o falta de datos y realiza la retransmisión reduce el tamaño de la ventana para descongestionar la red (posteriormente la incrementa en forma sucesiva).

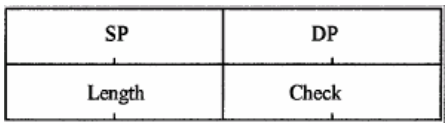
**Time-Out:** El valor de time-out de retransmisión es crítico. Si es muy corto incrementa el tráfico inútilmente y si es muy largo genera largos períodos de espera. Existen formas de realizar un tiempo time-out dinámico, en otros casos el mismo es configurable y fijo.

**Cierre de Conexión:** Se trata de un proceso de 3 pasos. Cuando la aplicación se cierra (*Close*) TCP envía un mensaje con la bandera FIN=1. Se envían 2 mensajes de respuesta, el primero confirma mediante ACK=1 y el segundo cierra la conexión mediante SYN=FIN=1. A esto se responde con un mensaje de reconocimiento ACK=1 y otro de terminación.

### 2.7.2 Protocolo UDP

El protocolo **UDP** (*User Datagram Protocol*) se ubica en la capa de transporte. El encabezado UDP ocupa 4 campos de 2 Bytes cada uno. UDP es un protocolo muy similar a TCP en el que muchas de las funciones de TCP han sido eliminadas. Dispone de los campos de puerto para identificar a los usuarios de UDP (protocolos

como SNMP, RTP, etc.), indica además la longitud del paquete y realiza un chequeo de errores sobre todo el paquete. Sin embargo no retransmite en caso de falta de datos, lo cual es útil en el caso de servicios de tiempo-real (voz y vídeo) donde esta función no es deseada.




*Trama de UDP*

**2.7.2.1 Campos de UDP**

**SP:** (2 Bytes) Identifica al número de puerto (*Port*) de origen del mensaje.
**DP:** (2 Bytes) Identifica al número de puerta de destino del mensaje.
**Length:** (2 Bytes) Determina la longitud total del datagrama UDP (incluyendo el encabezado y datos).
**Check:** (2 Bytes) Es un *Checksum* para control de errores del mensaje completo.

**2.8 Elementos de la Capa de Aplicación**

Además de los elementos de red antes descritos, es muy común la utilización de otros elementos en las redes IP destinados a brindar servicios de seguridad, de comunicaciones, de almacenamiento, etc. y que forman parte de la capa de aplicaciones.

**2.8.1 Servidor de 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 los recursos corporativos. Acepta, rechaza y controla el flujo de paquetes basado en identificadores de capa 3 o aplicaciones. El principio de funcionamiento es que todas las conexiones son denegadas a menos que estén expresamente autorizadas.
- ***Loggin*:** 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 sistema NAT permite aliviar la escasez de direcciones IP y eliminar la necesidad de renumeración cuando se realiza un cambio de **ISP** (*Internet Service Provider*).
- **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 el sistema (*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 páginas *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 un servidor de FTP, por ejemplo.

**2.8.2 Servidor de Autentificación**

El proceso de autentificar a un cliente puede ser realizado durante 4 etapas posibles: la conectividad del cliente, cuando se accede al software de autentificación del *switch*, mediante un servidor o cuando se autoriza a trabajar en una VLAN. Existen diversos métodos de autentificación de clientes. Se utilizan diversas herramientas como son: *username*, *password*, claves (*key*), **RADIUS** (*Remote Access Dial In User Service*), **PIN** (*Personal Identification Number*), Kerberos, LDAPv3, etc.

### 2.8.3 Servidor Web

Estos son los servidores que almacenan los datos e información de las páginas de Internet y que permiten el funcionamiento de la *World Wide Web*. En la WWW se desarrolla el protocolo de hipertexto, por hipertexto se entienden enlaces entre datos, mediante el cual con la selección de palabras y textos resaltados se accede a una otra página adicional. El salto entre páginas es independiente al lugar de almacenamiento (un servidor o varios en todo el mundo). Este proceso se denomina **navegación** (*Browsing, Cruising o Surfing*) en el ciberespacio.

No existe una RFC para la WWW, se trata de diferentes mecanismos como son URL, HTTP, HTML, CGI y Cookies entre otros. Se indican varios detalles de los mismos a continuación.

**URL** (*Uniform Resource Locators*). RFC-1630: El URL es una forma de identificador de recursos en los servidores web. Una URL puede administrar a varios servidores web desde un punto al que se dirige el usuario.
**HTTP** (*Hypertext Transfer Protocol*). RFC 2068: Se trata de un protocolo basado en un arquitectura cliente-servidor, donde el cliente utiliza un visualizador (*Browser Web*) para consultar información almacenada en un equipo remoto o servidor *web*. El servidor *web* es uno o más *servers* que entregan texto, gráficos, imagen y sonido que utilizan el protocolo de hipertexto HTTP para indicarle al cliente como mostrar la información. La forma de identificación de un servidor *web* inicia con el formato *http://www*. El servidor se denomina *HTTP server* en el ambiente Windows NT o *HTTP Daemon* en el Unix.
**HTML** (*Hypertext Markup Language*): Los enlaces de hipertexto se crean mediante el lenguaje HTML (RFC-1866). Es una variante de **SGML** (*Standard Generalized Markup Language*) de ISO-8879
**CGI** (*Common Gateway Interface*): Esta interfaz define como se comunica el *server* de HTTP con el programa ejecutable mediante un *browser*.
***Cookies*:** Se trata de información que el servidor *web* almacena en el cliente para ser utilizada en una próxima sesión. Puede ser usada para memorizar información de configuración o *passwords* de subscripción (acceso) al servidor. Esto produce un consumo de memoria y una intromisión que puede ser considerada inaceptable por el cliente. Algunos *cookies* son utilizados para tomar información del cliente y enviarlas al servidor. Los navegadores de Internet permiten configurar la aceptación de *cookies* en el cliente.

### 2.8.4 Servidor de Dominios

La gestión de direcciones IP requiere de una serie de elementos interrelacionados: el servidor DNS permite asociar un nombre de usuario con la dirección IP, el servidor/*router* NAT permite asignar direcciones IP no públicas en el interior de una red privada, el servidor DHCP permite asignar direcciones IP en forma dinámica a usuarios intermitentes y el *Dynamic DNS* permite actualizar el servidor de DNS cuando se asigna la dirección mediante DHCP. A continuación se describen algunos detalles de estos elementos.

**DNS** (*Domain Name System*): Este sistema permite traducir la información de enrutamiento entre un seudónimo o palabra simple de recordar y el número de dirección IP verdadera (se denomina resolución de nombres). Hasta 1980 un solo computador realizaba esta función para Internet, pero el tráfico hacia la misma se tornó inmanejable. Entonces se introdujo un sistema distribuido mediante el cual se realiza la resolución de nombres con varios servidores distribuidos en todo el mundo. El nombre o seudónimo completo tiene como máximo 63 caracteres. De ellos 3 caracteres indican el domino (edu-educación, com-comercial, gov-gubernamental, org-organización, mil-militar, etc) y 2 el país (ar-Argentina, it-Italia, etc). La tabla de dominios memorizada en el servidor se denomina *DNS Cache*.

**NAT** (*Network Address Translation*)**:** El problema más complejo de Internet es el reducido número de direcciones IP. La solución a largo plazo es IPv6 que cuenta con un mayor número de bytes por dirección y por lo tanto proporciona un mayor espacio de direccionamiento. Las soluciones usadas sobre IPv4 son dos: el **CIDR** (*Classless InterDomain Routing*) y el **NAT**. El proceso NAT propone reducir el número de direcciones IP mediante el re-uso de direcciones privadas en todas las redes. De esta forma una red privada utiliza un direccionamiento propio y el *router* en el borde (*Stub Router*) de la red realiza la función de traducción y direccionamiento hacia la red pública (llamadas dirección local y dirección global).

**DHCP (*Dynamic Host Configuration Protocol*):** Cuando un nuevo usuario se agrega a la red o se cambia de posición se requiere asignar una dirección IP y actualizar la base de datos del servidor DNS. El protocolo DHCP fue diseñado por el IETF (RFC-2131) para reducir los requerimientos de configuración. Además de asignar la dirección IP realiza una configuración automática de los parámetros necesarios para que el equipo de red pueda funcionar en cualquier lugar de la red donde se encuentre. DHCP trabaja sobre TCP y está basado en el protocolo **BOOTP** (*Bootstrap Protocol*) de RFC-0951, con algunas diferencias. El BOOTP permite que clientes sin capacidad de memoria (disco duro) puedan funcionar en TCP/IP.
Se utiliza un modelo *Client/Server* por lo que se dispone de uno o varios servidores DHCP. No se requiere de un servidor por subred, por lo que el protocolo DHCP puede trabajar a través de *routers*. Más de un servidor pueden realizar las tareas de asignación de direcciones con el propósito de mejorar la eficiencia del sistema.

**DNS *Update*:** Asociado a DHCP se encuentra el mecanismo *Dynamic DNS Update* que permite la actualización automática del servidor DNS con el nombre y la dirección IP asignada en forma dinámica por el protocolo DHCP. Se refiere a la RFC-2136. Este protocolo trabaja sobre TCP o UDP mediante peticiones (*requests*). El formato del mensaje de actualización (*update*) contiene un encabezado de 12 Bytes que identifica al que efectúa el requerimiento y diversos campos.

**DHCP *Failover*:** También en sociedad con DHCP se dispone de la técnica *DHCP Failover* que consiste en disponer de servidores duplicados funcionando como pares redundantes. Se dispone de un protocolo de comunicación simplificado para la operación en régimen normal, de interrupción de comunicación entre servidores y de falla del servidor asociado.

### 2.9 Calidad de Servicio QoS *(Quality of Service)*

Se entiende por calidad de servicio la posibilidad de asegurar una tasa de datos en la red (ancho de banda), un retardo y una variación de retardo (*jitter*) acotados a valores acordados con el usuario de una red. Por ejemplo en las redes Frame Relay o ATM la calidad de servicio se garantiza mediante un contrato de **CIR** (*Commited Information Rate*) con el usuario.

Para disponer de una calidad de servicio aceptable en redes soportadas en protocolo IP se han diseñado herramientas como son los protocolos de tiempo-real RTP y el de reservación RSVP.

Un problema es que cuando se soporta un servicio de voz sobre IP (VoIP) por ejemplo, los paquetes son cortos y el encabezado es largo comparativamente. En este caso se requiere un encabezado reducido y un proceso de fragmentación e intercalado **LFI**. Mediante **QoS** (*Quality os Service*) se tiende a preservar los datos con estas características.

Los servicios tradicionales de Internet disponen de una calidad denominada *best effort*, es decir que la red ofrece el mejor esfuerzo posible para satisfacer los retardos mínimos, lo cual no es mucho, pero que es suficiente para servicios que no requieren transmisión en tiempo real. Para servicios del tipo *real time* (voz y vídeo por ejemplo) se requiere una latencia mínima.

Se denomina **latencia** a la suma de los retardos en la red. Los retardos están constituidos por el retardo de propagación y el de transmisión (dependiente del tamaño del paquete), el retardo producido por el procesamiento *store and forward* (debido a que los *switches* o *routers* emiten el paquete luego de haber sido recibido completamente en una memoria buffer) y el retardo de procesamiento (necesario para el reconocimiento de encabezados, errores, direcciones, etc).

Una recepción de latencia variable (*jitter*) se define como una fluctuación del retardo sobre los datos de recepción, es decir que los datos llegan al receptor con diferentes retardos, con lo cual los datos de aplicaciones de tiempo real se ven afectados. La solución al *jitter* es almacenar los datos en memorias buffer, lo cual introduce un retardo aun mayor, y entregarlos con un retardo constante. Se han implementado diversos métodos de almacenamiento en el buffer de una manera garantizada mediante software, algunas de estos son mediante el uso de:

- Colas Prioritarias: Donde el administrador de la red define varios niveles (hasta 4) de prioridad de tráfico.
- Cola Definida: Donde el administrador reserva un ancho de banda para cada tipo de protocolo específico.
- Cola Ponderada: Mediante un algoritmo se identifica cada tipo de tráfico priorizando al de bajo ancho de banda. Esto permite estabilizar la red en los momentos de congestión.

### 2.9.1 Variantes de Servicios

Los servicios de datos y de multimedia tienen distintos requerimientos de calidad referido a la latencia y el *jitter*. Para satisfacer los requerimientos de calidad se acude al manejo de las colas de paquetes, la reservación de ancho de banda y la gestión del tráfico.

Para obtener estos objetivos en diversos ámbitos se han definido variantes de servicios.

**CoS** (*Class of Service*): El servicio CoS se logra mediante 3 bits que se ingresan en un campo adicional de 4 Bytes (etiqueta denominada *Tag* o *Label*) dentro del protocolo MAC. Estos 3 bits permiten definir prioridades desde 0 (máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del *switch* LAN para la descarga de paquetes.

**ToS** (*Type of Service*): Es similar al servicio de CoS pero este se realiza en la capa 3. Sobre el protocolo IP se define el campo ToS con 3 bits (del segundo byte del encabezado IP) para asignar prioridades. Se denomina señal de precedencia.

**QoS** (*Quality of Service*). En redes IP se define la tasa de acceso contratada **CAR** (*Committed Access Rate*) en forma similar al CIR de Frame Relay y ATM. La calidad QoS se ve garantizada mediante protocolos de reservación **RSVP** y de tiempo real **RTP.**

### 2.9.2 Clasificación de la QoS

***Guaranteed*:** El servicio garantizado es utilizado para garantizar un retardo máximo de extremo a extremo. Se trata de un servicio análogo al CBR (*Constant Bit Rate*) en ATM. Para esto se puede aplicar el concepto de reservación de tasa de bits (mediante el protocolo RSVP) o el método *Leaky-bucket*. Al usuario se le reserva un ancho de banda dentro de la red para su uso exclusivo aún en momentos de congestión. Se lo conoce como **Hard QoS**.

***Differentiared*:** El servicio diferenciado utiliza la capacidad separar el tráfico en la red con múltiples prioridades o **ToS** (*Type of Service*). Se dispone de 3 bits de precedencia para diferenciar las aplicaciones sensibles a la congestión (se brindan mediante el encabezado del protocolo IPv4). Es por lo tanto es un **Soft QoS**. El control de aplicación es del tipo *leaky-bucket*. Se puede soportar la función CAR que permite una administración del ancho de banda (política de tráfico). Su primera línea de defensa frente a la congestión es el uso de buffer de datos, lo cual implica el uso de una cola de espera y un retardo que depende de la prioridad asignada para los paquetes en dicha cola.

***Best-effort*:** Este es un servicio por *default* que no tiene en cuenta las modificaciones por la QoS. Se trata de una memoria buffer del tipo FIFO (*First Input-First Output*).

Existen 3 herramientas que utiliza un *router* para mejorar la eficiencia de la red reduciendo el tráfico que circula por la misma:

- Un manejo de nombres y direcciones mediante DNS.

– Los servicios *proxy* (se entiende por *proxy* a un elemento de la red que actúa en representación de otro).
– El *cache* local.

Un **cache** es un bloque de memoria para mantener disponibles los datos requeridos frecuentemente por varios procesos. Cuando un proceso requiere información primero consulta el cache, si la información se encuentra allí se produce una mejora de funcionamiento reduciendo el retardo de procesamiento. Si no se la encuentra en el cache se buscará en otras alternativas de memoria y luego se lo encontrará disponible en el cache para una próxima oportunidad.

Una ventaja adicional de ciertos caches es la posibilidad de reducir el dialogo para transferencia de información. Por ejemplo una consulta *web* lleva una sesión de innumerable cantidad de objetos que son transferidos mediante un HTTP *Get-Request*. Puede reducirse la cantidad de paquetes transferidos mediante una sesión en paralelo de objetos.

Algunos tipos de memoria cache son:

– Cache del Procesador: Es parte del procesador y es de más fácil acceso que la memoria RAM y a una velocidad mayor.
– Disco Cache: Pertenece a la memoria RAM y contiene información del disco. En algunos casos se mueve en forma anticipada la información desde el disco al cache en la RAM.
– Cache Cliente-Servidor: Se trata de un banco de memoria ubicado en el cliente para agilizar el movimiento de datos.
– Cache Remoto: Permite reducir los retardos cuando se accede a información de un sistema remoto en una WAN. Se resuelve mediante un *caching* de información del terminal remoto ubicado en el sistema local.
– Cache de Servidor Intermedio: Entrega información a un grupo de clientes (*Local Workgroup*) en un sistema cliente-servidor.

**Web-Caching:** Para un proveedor de servicio de Internet ISP *(Internet Service Provider)* el uso de cache en el punto de presencia POP puede reducir el tráfico en su red (aumentando la velocidad de respuesta al usuario y el costo de la conexión WAN). Un tráfico muy común y apropiado para el cache es la Web. El cache se conecta directamente al *router*, el cual deriva todos los paquetes de requerimiento al cache (por ejemplo los paquetes con puerto-TCP de destino 80 indican el protocolo HTTP), de esta forma puede verificar si la información está disponible. Su ventaja se incrementa en la medida que el número de usuarios es mayor.

### 2.9.3 Herramientas Para Proporcionar QoS

#### 2.9.3.1 Manejo de Congestión y Tráfico

Las herramientas de que se dispone para asegurar una QoS dentro de una red IP se tratan de mecanismos que previenen o manejan una congestión, distribuyen el tráfico o incrementan la eficiencia de la red.

Los protocolos involucrados en asegurar la calidad de servicio son los indicados a continuación, a los mismos se refiere como mecanismos de señalización.

#### 2.9.3.2 Control de Congestión en el Buffer de Datos

**FIFO** (*First In, First Out*): El primer mensaje en entrar es el primero en salir. Este es el mecanismo de QoS por *default* en las redes IP. Es válido solo en redes con mínima congestión. No provee protección, no analiza el ancho de banda ni la posición en la cola de espera.

**PQ** (*Priority Queuing*): Este mecanismo de control de congestión se basa en la prioridad de tráfico de varios niveles que puede aportar el encabezado del datagrama IP (ToS**:** *Type of Service*). Se trata de 3 bits disponibles en el Byte 2 del encabezado de IPv4 (bits de precedencia).

**CQ** (*Custom Queuing*): Este mecanismo se basa en garantizar el ancho de banda mediante una cola de espera programada. El operador reserva un espacio de buffer y una asignación temporal a cada tipo de servicio. Es una reservación estática.

**WFQ** (*Weighted Fair Queuing*): Este mecanismo asigna una ponderación a cada flujo de forma que determina el orden de tránsito en la cola de paquetes. La ponderación se realiza mediante discriminadores disponibles en TCP/IP (dirección de origen y destino y tipo de protocolo en IP, número de *socket* de TCP/UDP) y por el ToS en el protocolo IP. En este esquema la menor ponderación es servida primero. Con igual ponderación es transferido con prioridad el servicio de menor ancho de banda. El protocolo de reservación RSVP utiliza a WFQ para localizar espacios de buffer y garantizar el ancho de banda.

#### 2.9.3.3 Control de Tráfico

**WRED** (*Weighted Random Early Detection*): Trabaja monitoreando la carga de tráfico en algunas partes de las redes y descarta paquetes en forma aleatoria 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 desecho de paquetes de forma que no afecta al tráfico de tipo RSVP.

**GTS** (*Generic Traffic Shaping*): Provee un mecanismo para el control del flujo de tráfico en una interfaz en particular. Trabaja reduciendo el tráfico saliente limitando el ancho de banda de cada tráfico específico y enviándolo a una cola de espera. De esta forma permite un mejor desempeño en topologías con tasa de bits diferentes. Este control de tráfico se relaciona con **CAR**.

#### 2.9.3.4 Incremento de la Eficiencia (Señalización)

**LFI** (*Link Fragmentation and Interleaving*): El tráfico interactivo como Telnet y VoIP es susceptible de sufrir *jitter* con grandes paquetes en la red o largas colas en enlaces de baja velocidad. Se basa en la fragmentación de datagramas y el intercalado de los paquetes de tráfico.

**RSVP** (*Resource Reservation Protocol*): Se trata de implementar el concepto de señalización. Se dispone de dos tipos de señalización: en banda, por ejemplo los bits de precedencia para ToS, y fuera de banda, mediante un protocolo de comunicación como el RSVP. Este protocolo permite que un *host* o un *router* aseguren la reservación de ancho de banda a lo largo de la red IP.

**RTP-HC** (*Real-Time Protocol - Header Compression*): La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas.

No todas las herramientas disponibles son usadas en los mismos *routers*. Por ejemplo, la clasificación de paquetes, el control de admisión y el manejo de la configuración se usan en los *routers* de borde (*edge*), en tanto que en los centrales (*backbone*) se gestiona la congestión. El tratamiento de la congestión se fundamenta en el manejo de las colas en buffer mediante diferentes técnicas. El buffer es la primera línea de defensa frente a la congestión. El manejo correcto (mediante **políticas de calidad** de servicio) del mismo permite determinar el servicio de calidad diferenciada. Una segunda defensa es el control de flujo. El problema del control de flujo en TCP es que se ha planeado de extremo a extremo y no considera pasos intermedios.

En TCP cada paquete de reconocimiento (*Acknowledgment*) lleva un crédito (*Window*) con el tamaño del buffer disponible por el receptor. Un sobreflujo de datos en los *routers* de la red se reporta mediante el mensaje *Source Quench* en el protocolo ICMP. Estos mecanismos son ineficientes y causan severos retardos en la conexión.

#### 2.9.3.5 Priorización de Tráfico

**ToS/IEEE 802.1Q:** Los estándares IEEE 802.10 y 802.1Q fueron propuestos para el manejo de las redes VLAN, este último es el utilizado con regularidad. En el estándar 802.1Q se define el VLAN *Tagging Switch* que permite una identificación de la VLAN y la posibilidad de la priorización del servicio. La trama del paquete en la capa MAC incluye 4 Bytes adicionales al IEEE 802.3 que se colocan luego de las direcciones MAC y antes del *Type/Length.*

Los 4 Bytes son:

**TPID** (*Tag Protocol Identifier*): 2 Bytes usados para la identificación del protocolo. En Ethernet es hexa=8100.
**TCI** (*Tag Control Information*): 2 Bytes usados para las siguientes funciones:

- **UP:** 3 bits para determinar la prioridad del usuario (*User Priority*). Se trata de CoS desde 0 a 7. Esta información permite poner en práctica la CoS definida en IEEE 802.1p.
- **CFI** (*Canonical Format Indicator*): 1 bit para ser usado por Token Ring.
- **VLANI** (*VLAN Identifier*): Este campo de 12 bits permite identificar la VLAN (válido desde 1 a 1005). Permite la interoperación entre diferentes redes.

**QoS:** El campo de precedencia en el encabezado de IPv4 permite definir varios tipos de servicio ToS. Se trata de 3 bits que por razones históricas tienen diferentes nombres (*routing*, *priority*, etc) y que pueden ser usados para asignar prioridad. Se aplica un control de acceso extendido EACL para definir la política de la red en términos de congestión. En redes heterogéneas se debe mapear este tipo de servicio en equivalentes (*tag switch*, Frame Relay y ATM).
Con los bits de precedencia se pueden realizar 3 tipos de acciones: *routing* basado en políticas **PBR** (*Policy Based Routing*) (por ejemplo direcciones IP, puerto de TCP, protocolo, tamaño de paquetes, etc), propagar la política de QoS mediante el protocolo de enrutamiento BGP-4 y desarrollar una política de tasa de acceso contratada CAR.

**CAR** (*Committed Access Rate*): Se ofrece especificando políticas de tráfico y ancho de banda. El umbral de CAR se aplica a la puerta de acceso para cada puerta IP o por flujo de aplicación individual. Algunas opciones de política de CAR son la de prioridad y la asignación:

**Políticas de prioridad CAR**:

- CAR máximo: El exceso de ancho de banda es descartado.
- CAR premium: El exceso es señalado con un nivel de preferencia más bajo.
- CAR *best effort*: Por encima de un umbral se cambia la preferencia y sobre otro los paquetes son eliminados.

**Políticas de asignación CAR**:

- CAR por aplicación: Diferentes políticas son usadas en distintas aplicaciones, por ejemplo bajo nivel para HTTP.
- CAR por puerto: Los paquetes que ingresan a los puertos son clasificados con diferentes niveles de prioridad.
- CAR por dirección: Puede diferenciarse entre la dirección IP de origen y destino y asignar la prioridad en cada caso.

**Formación de Anillos:** Se trata de configurar la red de *switch* con enlaces en *loops* para incrementar la redundancia. Los *loops* están prohibidos en Ethernet pero mediante el protocolo STP se puede configurar la red en forma automática para detectar los *loops* e interrumpirlos hasta que una falla los habilite como necesarios. Las posibles configuraciones son:

- STP se puede habilitar para cada VLAN en particular.
- A los puertos se les asigna una prioridad y un costo para que STP determine el mejor camino.
- Se puede determinar el estado de los puertos (bloqueado, deshabilitado, *forwarding*, etc).
- *PortFast* es una función que habilita a pasar desde el bloqueo a *forward* sin pasar por los estados intermedios.

– *UplinkFast* permite una rápida convergencia para cambios con enlaces redundantes. Otra variante es *BackboneFast*.

El puerto que utiliza la función STP se encuentra en algunos de los siguientes estados: bloqueado (no participa de la transmisión), *listening* (es un estado transitorio luego del bloqueo y hacia el *forwarding*), *learning* (es otro estado transitorio antes de pasar al *forwarding*), *forwarding* (transmite las tramas en forma efectiva) y deshabilitado (se trata del estado no operacional). Si todos los puertos tienen la misma prioridad el *forward* lo realiza el puerto de menor número.

Este protocolo permite identificar los *loops* y mantener activa solo una puerta del *switch*. Por otro lado, utiliza un algoritmo que permite identificar el mejor camino libre de *loops* en la red de *switch*. Para lograr este objetivo, se asigna a cada puerta un identificador consistente en la dirección MAC y una prioridad. La selección de la puerta se puede asignar en términos de prioridad (valor entre 0 y 63, por default es 32) y costo (0 a 65535).

El STP consiste en un intercambio de mensajes de configuración en forma periódica (entre 1 y 4 seg). Cuando se detecta un cambio en la configuración de la red (por falla o cambio de costo del puerto) se recalcula la distancia (suma de costos) para asignar un nuevo puerto. Las decisiones se toman en el propio *switch*. En condiciones normales se selecciona un *switch* para que trabaje como *Root Switch* para determinar una topología de red estable (es el centro lógico de la topología en *Tree*). Por *default* el *switch* que posee la dirección MAC más baja es el seleccionado como root.

Los mensajes disponibles se denominan *Bridge-PDU* y son de dos tipos: *Configuration* y *Topology-change*. Los campos del mensaje de configuración incluyen 35 Bytes y el de cambio de topología solo los 4 Bytes iniciales. Por ejemplo, el mensaje de configuración contiene los siguientes campos de información.

### 2.9.4 Protocolos para Asegurar la QoS para Aplicaciones de Tiempo Real

**RSVP** (*Resource Reservation Protocol*): Este protocolo permite que un *host* o un *router* asegure la reservación de ancho de banda a lo largo de la red IP. Es del tipo orientado al receptor (el receptor solicita la reservación) y es útil para aplicaciones de tipo *símplex* (unidireccional). Puede funcionar como *unicast* o *multicast.*
**RTP** (*Real-time Transport Protocol*): Se utiliza sobre el protocolo UDP para aplicaciones como H.323 o VoIP.
**RTCP** (*Real-Time Transport Control Protocol*): Este protocolo se utiliza para control de la calidad de servicio sobre aplicaciones que trabajan sobre RTP.
**IGMP** (*Internet Group Management Protocol*): Este protocolo se utiliza para aplicaciones del tipo *multicast* cuando se requiere distribuir la misma información sobre un grupo (*multicast*) de usuarios y reduciendo el ancho de banda ocupado. Se emite un mismo paquete con dirección *multicast* en lugar de uno para cada dirección *unicast*.

#### 2.9.4.1 Protocolo de Reservación de Ancho de Banda (RSVP)

Los servicios del tipo SMTP o FTP en Internet son con calidad *best effort*, es decir, que no prevén una calidad de servicio. Esto tiene como consecuencia una latencia variable o *jitter* sobre la información del tipo tiempo real (audio o vídeo).

RSVP permite la reservación de ancho de banda para asegurar una QoS. El protocolo RSVP trabaja en conjunto con el protocolo de transporte **RTP** para servicios de voz y vídeo en tiempo real. El RSVP está definido en la RFC-2205.

Existen dos formas de reservación del ancho de banda: estática y dinámica.

La reservación estática permite asignar un porcentaje fijo del canal de comunicación a cada tipo de protocolo (por ejemplo, 10% a HTTP, 15% a FTP, 3% a Telnet, etc). El protocolo RSVP permite reservar el ancho de

banda en forma dinámica para asegurar una calidad de servicio **QoS** en las redes IP. La QoS permite garantizar el servicio en forma CAR.

El protocolo RSVP se define para los servicios integrados en Internet. Es utilizado por el *host* para solicitar una QoS al *router* para una aplicación particular y es usado por el *router* para establecer un ancho de banda con todos los nodos intermedios del trayecto.
Opera tanto sobre IPv4 como sobre IPv6, no es un protocolo de enrutamiento y solo se le utiliza para reservar ancho de banda y buffer. En el modelo de capas el protocolo RSVP ocupa la función de la capa 3 sobre IP, en la misma forma que los protocolos de *routing* (OSPF y BGP), de *multicast* (IGMP), de gestión (ICMP) y de transporte (TCP y UDP).

Una sesión manejada por del protocolo RSVP está definida mediante 3 direcciones: la dirección IP de destino (receptor), el identificador de protocolo y el puerto de UDP. Está definido para operar en forma de *unicast* o *multicast*. En el caso de operar con protocolo *multicast* primero se establece el enlace mediante IGMP (para establecer el grupo) y luego mediante RSVP (para establecer la reservación). Por otro lado RSVP es un protocolo de carácter *símplex*, es decir unidireccional. Está orientado al receptor, en el sentido que es el receptor el que solicita la reservación y el que la interrumpe.

#### 2.9.4.1.1 Control de Tráfico

La QoS es implementada por un mecanismo de flujo de datos denominado control de tráfico. Este mecanismo incluye 3 etapas:

- La clasificación del paquete para determinar la QoS y la ruta de cada paquete.
- El control de admisión para asegura la disponibilidad de la reservación.
- El proceso de determinación temporal de emisión (*Packet Scheduler*).

El requerimiento de reservación es iniciado por *host* receptor y pasa por los distintos *router* de la red. Si algún mecanismo intermedio falla se genera un reporte de error. Se dispone de dos mensajes de error: *ResvErr* y *PathErr*.
Este protocolo mantiene mediante software el estado de los *routers* y *hosts*, entregando un soporte dinámico para cambios de miembros y adaptación automática de cambios de *routing*. No es un protocolo de enrutamiento pero depende de los mismos. Los mensajes de *Path* y *Reservation* se utilizan para estos propósitos.

# Capitulo 3

# VoIP

### 3.1 Introducción

La red telefónica pública conmutada (RTPC) se encuentra distribuida en la mayor parte del mundo y brinda servicios de comunicaciones de voz de gran calidad y prácticamente instantáneos con una cobertura global, lo que la hace el sistema de comunicaciones de voz más empleado en todo el mundo. Los sistemas telefónicos han evolucionado, tratando de satisfacer las crecientes necesidades de los usuarios, mediante sistemas digitales que han permitido mejorar la capacidad de los sistemas de transporte y la incorporación de servicios suplementarios que buscan hacer frente a las necesidades de comunicación de los usuarios. Sin embargo, dada la gran complejidad y el costo de mantenimiento de la red telefónica mundial, se han buscado nuevas alternativas en un sistema que pueda brindar los mismos servicios, con una calidad comparable, y que permita la incorporación de otros nuevos servicios.

Puesto que el tráfico de datos está creciendo mucho más rápidamente que el de voz, desde hace varios años ha habido un interés considerable en transportar la voz sobre redes de datos (en contraposición con la forma tradicional de transportar los datos sobre redes de voz). El soporte para las comunicaciones de voz mediante el *Internet Protocol* (IP), conocido como Voz Sobre IP **VoIP** (*Voice over IP*), actualmente tiene un especial atractivo dado su bajo costo y grandes ventajas.

La viabilidad de transportar la voz sobre Internet ha llevado al desarrollo de normas y protocolos que permiten garantizar él tráfico de voz sobre redes IP y que han llevado a la disponibilidad de productos comerciales de alta calidad que permiten la implementación de sistemas telefónicos basados en IP con una calidad similar a la proporcionada por la red telefónica publica conmutada (RTPC). La gran calidad telefónica que actualmente se puede lograr sobre redes IP ha sido uno de los avances principales que conducen a la convergencia de las redes de voz, vídeo, y de datos.

El crecimiento y la fuerte implantación de las redes IP, tanto en el ambito local como en el global, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, asi como la implementación comercial de estandares que permiten la calidad de servicio **QoS** en redes IP, han creado un entorno donde es posible transportar la voz sobre IP.

Aunque VoIP existe desde hace algunos años, la demanda de servicios ha forzado una rápida evolución de la tecnología. El uso de servicios de banda ancha y la integración de voz y datos a todos los niveles han favorecido el desarrollo de aplicaciones y protocolos de VoIP, que se han sido pensados para ofrecer un mayor conjunto de características, escalabilidad y estandarización mejorados para brindar servicio de telefonía.

La mayoría de las redes existentes de proveedores de servicios soportan principalmente servicios de datos (Internet) basados en IP. Estos proveedores de servicios poseen y siguen desplegando infraestructuras IP que les permitirían incorporarse al mercado de los servicios de voz sobre IP. Los mayores proveedores de telecomunicaciones están buscando la forma de recortar el costo de funcionamiento y el mejoramiento de las redes de voz existentes, buscando reemplazar y aumentar sus redes con soluciones de VoIP. Lo mismo esta ocurriendo en las redes corporativas (principalmente redes LAN) que están tratando de aprovechar mejor sus recursos. Por lo anterior se estima que el futuro de los servicios telefónicos a nivel mundial esta en la telefonía IP.

Además de las ventajas del costo, los servicios de VoIP tienen ventajas técnicas importantes sobre la telefonía de conmutación de circuitos. Las redes de VoIP se basan en una arquitectura abierta que significa que los servicios de VoIP son más intercambiables y más modulares que los de un sistema de conmutación de circuitos. Se pueden seleccionar productos sin estar atado a un vendedor específico. Los estándares abiertos

también se traducen en la realización de nuevos servicios que pueden desarrollarse y desplegarse rápidamente en lugar de esperar a que un productor particular desarrolle una solución propietaria. Por otra parte, VoIP es conveniente para la CTI (Integración de la telefonía a la computadora) y otros usos de próxima generación.

### 3.1.1 Escenarios de Implementación

Existen tres escenarios para la implementación de VoIP en redes IP:

- Internet: Debido al funcionamiento y el estado actual de Internet, esta red no permite el tráfico de voz de una manera garantizada.
- Red IP Pública: Los proveedores de servicios ofrecen a las empresas la conectividad necesaria para interconectar sus redes de área local, en lo que al tráfico IP se refiere, mediante el arrendamiento de canales o lineas de trasmisión de banda ancha. Este escenario se puede considerar como algo similar a Internet, pero con una mayor calidad de servicio y con importantes mejoras en seguridad, ya que hay proovedores de servicios que incluso ofrecen garantías de bajo retardo y/o ancho de banda, lo que las hace muy interesante para el tráfico de voz.
- Intranet: La red IP implementada por la propia empresa. Suele constar de varias redes LAN (Ethernet, ATM, etc.) que se interconectan mediante redes WAN como ATM, líneas punto a punto, RDSI para el acceso remoto, etc. En este caso la empresa tiene bajo su control prácticamente todos los parámetros de la red, por lo que resulta ideal para su uso en el transporte de la voz.

La meta para los diseñadores de productos de VoIP es agregar las capacidades de las Redes Telefónicas Conmutadas RTC (transferencia de voz, señalización y servicios suplementarios) a las redes IP e interconectar éstos a la red de teléfono público y a las redes de voz privadas de tal manera que se mantengan los estándares de calidad actuales de la voz y se preserven las características que cada uno espera del teléfono. Se requiere asegurar que la calidad de la voz sea comparable a la que está disponible actualmente con la RTPC, incluso para las redes que tienen niveles variables de calidad de servicio.
La red IP debe resolver los criterios del funcionamiento incluyendo la minimización del rechazo de llamada, de la latencia de la red, de la pérdida de paquetes, y de la desconexión. Esto es requerido incluso durante condiciones de congestión o cuando múltiples usuarios deben compartir recursos de la red. El control de la llamada (señalización) debe hacer la llamada telefónica transparente de modo que los usuarios no necesiten saber qué tecnología es la que implementa el servicio.

### 3.1.2 Ventajas de VoIP

Utilizar VoIP significa obtener grandes ahorros económicos al integrar dos infraestructuras de comunicación, de voz y datos, en una sola con una mejor escalabilidad y de más fácil mantenimiento, pero sobre todo significa la incorporación de nuevos servicios que integran voz y datos y que permiten a los usuarios tener mejores herramientas de comunicación.

Las ventajas de esta tecnología se pueden dividir principalmente en las siguientes categorías:

**Reducción de Costos**. La compartición de equipo y de los costos de operación entre las redes de datos y de voz puede mejorar la eficacia de la red puesto que el exceso del ancho de banda en una red se puede utilizar por la otra, creando economías de escala para la voz (dado especialmente por el crecimiento rápido del tráfico de datos). Además en algunos casos se evitan cargos por acceso a la RTPC y honorarios e impuestos por el establecimiento de llamadas internacionales. Además se tienen menores costos que con tecnologías alternativas (voz sobre TDM, ATM o Frame Relay) para la implementación de servicio de telefonía.

**Simplificación**. Una infraestructura integrada que apoya todas las formas de comunicación permite una mayor estandarización y reduce el complemento total del equipo. Esta infraestructura combinada puede apoyar la optimización dinámica del ancho de banda y un mejor control de fallos. Las diferencias entre los patrones de tráfico de la voz y de datos ofrecen otras oportunidades para lograr mejoras significativas en la eficacia de la redes de comunicaciones.
**Consolidación.** El uso extendido de los protocolos de IP, para una gran diversidad de servicios, permite una complejidad reducida y una mayor flexibilidad para la implementación de nuevos servicios de

comunicaciones. Las redes IP son la redes estándares más utilizadas para las Internets, Intranets y Extranets y VoIP permite la integración sobre las redes existentes de datos de la voz como un servicio más. Además se cuenta con estándares efectivos que permiten la interoperabilidad de diversos proveedores.

**Usos Avanzados.** Aunque la telefonía básica y el fax son los usos iniciales para VoIP, las ventajas mayores de esta tecnología serán derivadas de aplicaciones multimedia y de aplicaciones multiservicios. Combinar las características de la voz y de los datos en nuevos usos proporcionará las ventajas más grandes a largo plazo de VoIP.

### 3.1.3 Aplicaciones de VoIP

Entre las aplicaciones que pueden ser soportadas por VoIP se encuentran las siguientes que producen de forma inmediata grandes ventajas y un ahorro de costos muy significativo.

**Centros de Llamadas *(Call Centers):*** Los centros de llamadas pueden usar la tecnología VoIP, mejorando la calidad de la información intercambiada en cada sesión. Por ejemplo un usuario podría consultar 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 consiguen 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**).

**Redes Privadas Virtuales de Voz:** Esta aplicación consiste en la interconexión de las PBXs a través de la red *IP* corporativa, de manera que se puede realizar una llamada desde una extensión de la oficina A a otra extensión de la oficina B a través de la red de datos de la empresa, produciéndose esta llamada de forma gratuita ya que se aprovecha la infraestructura de datos existente.

**Centros de Llamadas Vía *Web*:** Si una compañía tiene su información disponible en Internet, los usuarios que visitan este *website* podrían no sólo visualizar la información que esta compañía les ofrece, sino que podría establecer una comunicación, por ejemplo, con una persona del departamento de ventas sin necesidad de cortar la conexión. De esta manera el operador de ventas cuando atienda la llamada tendrá en su pantalla la misma información que esta viendo el usuario. Esta aplicación tiene las siguientes ventajas:

- Al ser la llamada a través de Internet, para el usuario no tiene costo adicional, aprovecha la llamada telefónica que tenía establecida para la comunicación de datos para mantener también la comunicación de voz.
- El usuario puede mantenerse *on-line* mientras habla con un operador.
- El operador puede cerrar la venta de manera más fácil ya que tendrá más argumentos comerciales para convencer al usuario.

**Aplicaciones de Fax:** Al igual que se hace con la voz, cabe la posibilidad de realizar transmisiones de fax sobre redes de VoIP, consiguiendo de esta manera reducir de forma significativa los costos en transmisión de fax. Los faxes se pueden recibir a través de máquinas de fax convencional. Una aplicación especial es el envío masivo de fax, el usuario sólo envía una copia del fax que desea enviar, así como la lista de números telefónicos de destino y el sistema se encarga de realizar todos los envíos. La calidad de transmisión se ve afectada por el retraso de la red, la compatibilidad de la máquina de fax, y la calidad de la señal analógica, por lo que para operar sobre redes de paquetes, la interfaz del fax debe convertir los datos a la forma del paquete, manejando conversión de señales y protocolos de control (estándares T.30 y T.4), y asegurar la entrega completa de los datos de la exploración en el orden correcto. Para este uso, la pérdida de paquetes y retrasos de entrega son más críticos que en aplicaciones de voz.

**Multiconferencia:** La telefonía *IP* permite la conexión de tres o más usuarios simultáneamente compartiendo las conversaciones de voz o incluso documentos sobre el que todos los miembros de la multiconferencia pueden participar. Esto resulta de gran utilidad para la realización de reuniones virtuales, con los consiguientes ahorros de gastos que supone el desplazamiento de personas.

**Teléfonos con Conexión a Internet:** Los teléfonos ordinarios (alámbricos o inalámbricos) pueden ser habilitados para servir como dispositivo de acceso a Internet así como para el abastecimiento de servicios de telefonía normal. Los servicios del directorio, por ejemplo, se podrían acceder en Internet mostrando un nombre y recibiendo una contestación de voz (o texto).

**Acceso Remoto:** Los usuarios pueden acceder a los servicios corporativos de voz, datos y fax usando la Intranet de su compañía (emulando una extensión remota para un PBX, por ejemplo) a través de los teléfonos IP.

**Movilidad:** Las llamadas se pueden realizar y recibir usando una PC multimedia conectada a Internet de igual manera que se harían en la oficina o lugar de trabajo del usuario, independientemente del lugar del mundo donde se localice el usuario.

**Buzón de Voz:** La mayoría de los usos de VoIP definidos se consideran actividades en tiempo real, sin embargo los servicios *store and forward* de la voz también pueden ser puestos en ejecución usando VoIP. Por ejemplo, los mensajes de voz se pueden entregar a un buzón de voz, para posteriormente ser escuchados por el destinatario.

### 3.2 Arquitectura y Funcionamiento

VoIP es una tecnología que permite establecer comunicaciones de voz utilizando como medio de transporte una red IP. Con esta tecnología, en lugar de utilizar la infraestructura telefónica tradicional (centrales telefónicas y cableados) de conmutación de circuitos, la voz es transmitida en forma de paquetes por medio de una red IP.

El concepto de VoIP es relativamente simple, se trata de transformar la voz en paquetes de información manejables por una red IP. Básicamente una llamada de VoIP debe pasar por las siguientes etapas:

- Digitalización de la señal de audio o voz.
- Las muestras de voz, una vez cuantificadas, se ordenan en bloques de datos de igual longitud, llamados tramas.
- Se estiman los niveles de energía de cada trama para que un detector de silencio, decida si el bloque debe ser tratado como silencio o como parte de una conversación.
- Cuando la trama es parte de una conversación, es comprimida de acuerdo a un algoritmo específico. La trama es entonces encapsulada de acuerdo al protocolo IP y es transferida a través de una red IP hasta el destino de la llamada.
- En el destino se decodifica la señal de audio utilizando el mismo algoritmo empleado para la codificación.
- El dispositivo de salida realiza una conversión digital a analógica, y entrega la señal de audio a través de un auricular o bocina.
- Este proceso se realiza en los dos sentidos para lograr una comunicación bidireccional.

La voz sobre redes IP inicialmente se implementó para reducir el ancho de banda mediante compresión vocal (aprovechando los procesos de compresión diseñados para sistemas celulares) y en consecuencia para disminuir los precios en el transporte internacional. Sin embargo, migró rápidamente a una red de servicios integrados sobre la misma LAN. Con posterioridad se migró de la LAN a la WAN con la denominación de Telefonía sobre IP (**ToIP** *Telephony over IP* o IP *Telephony*). Los operadores de este tipo de servicio se denominan **ITSP** (*IP Telephony Service Provider*) por similitud a los ISP de Internet.

Una diferencia inicial entre VoIP e IP Telephony es la interoperatividad con las redes telefónicas actuales y los servicios de valor agregado que generalmente se brindan en las redes RTPC soportadas en señalización SS7 y redes inteligentes **IN** (*Inteligent Network*). Otra diferencia está dada en que mientras VoIP se piensa en el ámbito de la LAN con interconexión mediante Internet, en IP Telephony se piensa en un *backbone* de alta velocidad para garantizar la calidad de servicio mediante herramientas de **QoS** y que cuente con conexión a la RTPC.

Normalmente se distinguen dos aplicaciones para VoIP. Una en redes LAN o mediante PBXs para comunicaciones internas en las empresas. Otra es en redes WAN para telefonía pública. En este último caso se puede observar las diferencias entre un operador local y otro de larga distancia. Cuando se habla de *IP Telephony* se refiere a la aplicación pública, donde el principal problema es la interoperatividad (conexión entre distintos operadores con distinta tecnología). En IP *Telephony* se aplica el concepto de *carrier-grade*. Este concepto puede incluir varios aspectos como son: Redundancia de equipamiento para lograr disponibilidad elevada (por ejemplo, 99.999%), calidad vocal (errores, retardo, *jitter*, eco, etc.), disponibilidad de servicios (valor agregado en la red RTPC mediante SS7 en la IN), conectividad con todos los otros operadores.

### 3.2.1 Funcionamiento Básico de VoIP

Las componentes de VoIP deben ser capaces de implementar las mismas funciones básicas de una RTC. Es decir:

- Señalización.
- Servicios de bases de datos.
- Conexión y desconexión de llamadas.
- Uso de *codecs*.

**Señalización:** La señalización en una red de VoIP es tan crítica como en el sistema de telefonía convencional. La señalización en una red VoIP, activa y coordina varios componentes para terminar una llamada. Aunque la naturaleza de la señalización es igual, hay algunas diferencias técnicas y arquitectónicas en una red VoIP. La señalización en una red VoIP se logra mediante el intercambio de los datagramas IP entre los componentes. El formato de estos mensajes es cubierto por un conjunto de protocolos estándares. Sin importar qué protocolos se utilicen, estos flujos de mensajes son críticos para el funcionamiento de una red de voz y pueden necesitar un tratamiento especial para garantizar su entrega.

**Servicios de Bases de Datos:** Los servicios de bases de datos son usados como una manera de localizar un punto final y de traducir la dirección que usan dos redes (generalmente heterogéneas). Por ejemplo, la RTPC utiliza números de teléfono para identificar puntos finales, mientras que una red de VoIP utiliza una dirección IP y los números de puerto para identificar un punto final. Una base de datos de control de llamada contiene estos mapeos y traducciones, además de que puede emplear lógica adicional para proporcionar seguridad de la red. Esta funcionalidad, junto al control del estado de la llamada, coordina las actividades de los elementos en una red VoIP.

**Conexión y Desconexión de Llamadas:** La conexión de una llamada es hecha por dos puntos finales que abren sesiones de comunicaciones entre cada uno. En la RTPC, el conmutador público o el PBX conectan los canales lógicos a través de la red para terminar las llamadas. En una implementación de VoIP, esta conexión es un *stream* multimedia (audio, vídeo, o ambos) transportado en tiempo real. Esta conexión es el canal del portador y representa el contenido de voz o vídeo que es entregado. Cuando la comunicación se termina, se terminan las sesiones de IP y opcionalmente se liberan los recursos de la red.

Uso de Codecs: La naturaleza de las comunicaciones de voz es analógica, mientras que la naturaleza de una red de datos es digital. Es por este que se requiere un proceso para convertir señales analógicas a señales digitales y viceversa, esta es la función de un codificador-decodificador o codec (que en este caso también se conoce como codificador-decodificador de voz o vocoder). Hay muchas maneras de transformar una señal de voz analógica, todas ellas gobernadas por varios estándares. El proceso de la conversión es complejo y requiere cierto tiempo que afecta el desempeño del sistema. La mayoría de las conversiones se basan en la modulación codificada mediante pulsos (PCM) o mediante variaciones de esta técnica. Además de la conversión de analógico a digital de la voz, el codec comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir un ahorro del ancho de banda. Los ahorros del ancho de banda para los servicios de voz pueden venir en varias formas y trabajar en diversos niveles. Por ejemplo, la compresión analógica puede ser parte del esquema de codificación (algoritmo) y no necesita la compresión digital adicional de las capas de trabajo más altas, otra manera de

ahorrar ancho de banda es el uso de la supresión del silencio, que es el proceso de no enviar los paquetes de la voz entre silencios en conversaciones.

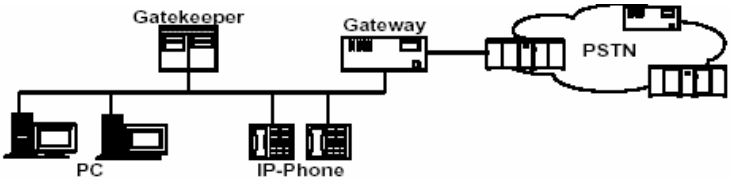
Usar la compresión y/o la supresión de silencios puede dar lugar a un ahorro importante del ancho de banda. Sin embargo, hay algunos usos que se podrían ver afectados por la compresión. Un ejemplo es el impacto en usuarios que utilizan *modems*. Los esquemas de compresión pueden interferir con el funcionamiento de *modems* confundiendo la codificación usada, el resultado podría ser que los *modems* nunca se sincronizen o que exhiban un rendimiento de procesamiento muy pobre. Algunos *gateways* implementan una cierta inteligencia en ejecución que puede detectar el uso de *modems* e inhabilitar la compresión. Otro argumento potencial se ocupa de esquemas de compresión de discurso de bajo número de bits, tales como G.729 y G.723.1. Estos esquemas de codificación intentan reproducir el sonido subjetivo de la señal más que la forma de onda, una mayor cantidad de pérdida de paquetes o de retardo es más sensible que la de una forma de onda no comprimida. Sin embargo, algunos estándares pueden emplear las técnicas de interpolación y otras que pueden reducir al mínimo los efectos de la pérdida de paquetes.
La salida del *codec* es una secuencia de datos que se pone en los paquetes IP y se transporta a través de la red a un destino. Estos destinos deben utilizar los mismos estándares, así como un sistema común de parámetros de *codec*. El resultado de usar diversos estándares o parámetros en ambos extremos es una comunicación ininteligible. Los estándares de codificación más importantes están cubiertos por la Unión Internacional de Telecomunicaciones (ITU). Cabe destacar que se paga un precio por la utilización reducida del ancho de banda por el creciente retraso de conversión.

### 3.2.2 Componentes de una Red de VoIP

Los componentes principales de una red de VoIP son muy similares en funcionalidad a los de una red con conmutadores de circuitos. Las redes de VoIP deben realizar las mismas tareas que hace una RTC, además de realizar una función de interconexión (*gateway)* a la red telefónica existente. Además se requieren dispositivos que se encarguen del control de las llamadas y de garantizar la QoS. Aunque se usan diversas tecnologías y acercamientos, algunos de los mismos conceptos que constituyen la RTPC también crean las redes de VoIP.

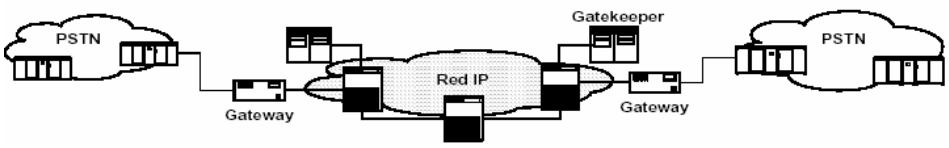
Los componentes la interconexión dependen del tipo de aplicación usada:

En el interior de una LAN (que usan PBXs) las terminales son las PC (con el software correspondiente) o los *teléfonos IP* (teléfonos especialmente diseñados para trabajar sobre redes LAN). El que establece las conexiones es el *Gatekeeper* (se trata del servidor de llamadas) y el que realiza las funciones de conectividad hacia el exterior (la red telefónica convencional) es el *Gateway.*



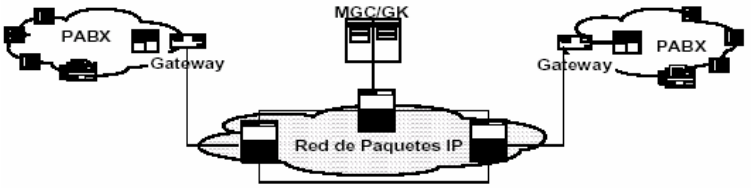
*VoIP en una LAN*

Cuando VoIP se aplica en una red WAN se establecen g*ateways* en ambos extremos de la red para conectar a la RTPC (PSTN). El transporte se realiza mediante IP (canales en la red IP con calidad contratada). En este caso existen *gatekeepers* en los distintos puntos de presencia **POP** (*Point of Presence*) del operador ITSP.



*VoIP en una WAN*

Una tercera posibilidad es la formación de un ITSP de telefonía local. En este caso la LAN y la PABX (con la interfaz de un g*ateway*) son conectadas a la red IP de transporte. El control nuevamente lo realiza el *gatekeeper*.




*Proveedor de VoIP*

El controlador de llamada es el *Gatekeeper*. Sin embargo, se ha popularizado también la denominación **MGC** (*Media Gateway Controler*) para una mayor extensión de funciones. Las funciones del MGC pueden ser realizadas mediante dos técnicas distintas. La primera toma de la telefonía pública convencional las partes que pueden ser utilizadas (procesador central, memoria, cómputo de tráfico, etc.) y elimina aquellas que no corresponden (red de conmutación de circuitos). La segunda se trata de un software (***Softswitch***) que corre sobre una plataforma de computo convencional (servidor).

**Estándares de VoIP**

**3.3 H.323**

La norma H.323 de la ITU-T ha sido generada para la implementación de sistemas de comunicación de multimedia basados en paquetes, en redes que pueden no garantizar correctamente la calidad de servicio **QoS**. Esta tecnología permite la transmisión en tiempo real de vídeo y audio por una red de paquetes. Es de suma importancia ya que gran parte de los servicios de voz sobre protocolo Internet (**VoIP**) actualmente utilizan esta norma.

H.323 es una familia de estándares basados en software que define varias opciones para la compresión y control de llamadas. Algunas de las características del estándar H.323 son que permite una conexión rápida, mediante el estándar H.235 permite funciones de seguridad (autentificación, integridad, privacidad), mediante el H.450 introduce los servicios suplementarios, soporta direcciones del tipo RFC-822 (e-mail) y del formato URL, mediante la unidad MCU permite el control de llamadas multipunto (conferencias), permite la redundancia de *gatekeepers*, soporta la codificación de vídeo, admite mensajes RIP (*Request in Progress*) para informar que la llamada no puede ser procesada por el momento y provee la facilidad que el *gateway* informe al *gatekeeper* sobre las disponibilidad de enlaces para mejorar el enrutamiento de llamadas, etc.

En la recomendación H.323 se produjo una gran colaboración entre los fabricantes de computadoras y de equipo de telecomunicaciones. De esta forma, la adopción del estándar H.323 asegura un alto grado de funcionalidad e interoperabilidad de estos equipos. Por otra parte, el hecho de que la recomendación H.323 permita que sus productos aseguren sus servicios sobre redes de calidad de servicio no garantizada, ha sido otro de los factores clave para asegurar su éxito, ya que si no se tiene una QoS garantizada en la red IP el sistema de VoIP funciona, pero no con la misma calidad de una RTC.

El estándar H.323 de la ITU-T, que cubría la mayor parte de las necesidades para la integración de la voz a las redes de datos, se eligió para que inicialmente fuera la base de VoIP. H.323 tiene como principal objetivo asegurar la interoperabilidad entre equipos de diferentes fabricantes, fijando aspectos tales como la supresión de silencios, la codificación de la voz y el direccionamiento, estableciendo nuevos elementos para permitir la conectividad con la infraestructura telefónica tradicional. Estos elementos se refieren básicamente a los servicios de directorio y a la transmisión de señalización por tonos multifrecuencia (DTMF).

**3.3.1 Componentes de H.323**

El estándar H.323 define los siguientes componentes más relevantes:

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

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

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

***Gatekeeper*:** El *gatekeeper* (**GK**) es una entidad que proporciona la traducción de direcciones y el control de acceso a la red de las terminales H.323, los *gateways* y las MCUs. El GK puede también ofrecer otros servicios a las terminales, *gateways* y MCUs, tales como gestión del ancho de banda y localización de los *gateways*. El *gatekeeper* realiza dos funciones de control de llamadas que preservan la integridad de la red corporativa de datos. La primera es la traslación de direcciones de las terminales de la red a las correspondientes IP, tal y como se describe en la especificación RAS. La segunda es la gestión del ancho de banda, fijando el número de conferencias que pueden estar dándose simultáneamente en la red y rechazando las nuevas peticiones por encima del nivel establecido, de manera tal que se garantice ancho de banda suficiente para las aplicaciones de datos sobre la red. El *gatekeeper* proporciona todas las funciones anteriores para las terminales, *gateways* y MCUs, que están registrados dentro de la denominada zona de control H.323.

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

**MCU** Unidad de Control Multipunto (*Multipoint Control Unit*): La MCU 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 transmisión de audio y vídeo y controlar la multidifusión.

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

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

El *gateway* es un elemento esencial en la mayoría de las redes pues su misión es la de enlazar la red VoIP con la red telefónica analógica o a la RDSI (Red Digital de Servicio Integrados).

Los distintos elementos pueden residir en plataformas físicas separada, o se pueden encontrar con varios elementos conviviendo en la misma plataforma. De este modo es bastante habitual encontrar juntos *gatekeeper* y *gateway*, además hay disponibles *routers* que tienen implementados las funciones de *gateway*.

### 3.3.2 Protocolos de H.323

El estándar H.323 comprende a su vez una serie de estándares y se apoya en una serie de protocolos que cubren los distintos aspectos de la comunicación, como son el direccionamiento, la señalización, la compresión, la transmisión y el control de la transmisión.

**Direccionamiento:**

- **RAS** (*Registration, Admision and Status*): Protocolo de comunicaciones que permite a una estación H.323 localizar otra estación H.323 a través del *gatekeeper*. Utiliza mensajes H.225 para la comunicación entre la terminal y el *gatekeeper* GK. Sirve para realizar las funciones de registro, control de admisión, control de ancho de banda, estado y desconexión.
- **DNS** (*Domain Name Service*): Servicio de resolución de nombres en direcciones IP con el mismo fin que el protocolo RAS pero a través de un servidor DNS.

**Señalización:**

- **Q.931:** Este protocolo se encarga de la señalización inicial de llamada, es definido originalmente para señalización en accesos ISDN básicos **BRI** (*Basic Rate Interface*). Se utiliza para realizar la señalización de llamada en la red IP (desde el GW hacia la terminal). Es equivalente al ISUP utilizado desde el GW hacia la RTPC.
- **H.225:** Este protocolo se encarga de funciones de control de llamada como son la señalización, el registro, la admisión, la paquetización y la sincronización del *stream* (flujo) de voz. Los mensajes de control de señalización de llamada permiten establecer la conexión y la desconexión. Este protocolo describe como funciona el protocolo RAS y Q.931. H.225 define como identificar cada tipo de codificador y discute algunos conflictos y redundancias entre la RTC y H.245.
- **H.245:** Protocolo de control para especificar mensajes de apertura y cierre de canales para *streams* de voz. Este protocolo de señalización transporta la información no telefónica durante la conexión. Es utilizado para la transmisión de comandos generales, de indicaciones, para el control de flujo, para la gestión de canales lógicos, etc. Se usa en las interfaces terminal a terminal y terminal a GK. H.245 es una librería de mensajes con sintaxis del tipo ASN.1. En particular codifica los dígitos DTMF (*Dual Tone Multi Frequency*) en el mensaje UserInputIndication.

**Compresión de Voz:**

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

**Transmisión de Voz:**

- **UDP (*User Datagram Protocol*):** La transmisión se realiza sobre paquetes UDP, pues aunque UDP no ofrece integridad en los datos, el aprovechamiento del ancho de banda es mayor que con TCP.
- **RTP** (***Real-Time Transport Protocol***): El Protocolo de Transporte en Tiempo Real maneja los aspectos relativos a la temporización y el marcando de los paquetes UDP con la información necesaria para la correcta entrega de los mismos en recepción. Trabaja junto con **RTCP** (*Real Time Control Protocol*) para entregar un informe sobre la calidad de la transmisión de datos. El encabezado de RTP puede ser comprimido para reducir el tamaño de archivos en la red.

**Control de la Transmisión:**

- **RTCP** (*Real Time Control Protocol*): Se utiliza principalmente para detectar situaciones de congestión de la red y tomar, en su caso, acciones correctoras**.** Se usa para reservar un ancho de banda especificado dentro de la red IP.

**Direcciones**

- **Dirección IP** (*IP Address*): Se trata normalmente de direcciones privadas que identifican a cada componente. La asignación de direcciones puede ser fija o asignada en forma dinámica (mediante el protocolo DHCP).
- **Dirección TSAP**: Corresponde al puerto *TCP/UDP*. Permite la multiplexación de canales con la misma dirección de red. Algunos componentes, como el GK y el protocolo RAS, tienen una dirección de puerto fija (*well-known*), mientras que en otros, como las terminales, se asignan en forma dinámica.

- **Dirección de *Alias***: Se trata de alguna identificación como el número telefónico, dirección de e-mail, nombre de usuario, etc. La resolución de direcciones alias se realiza en el *gatekeeper*.

### 3.3.3 Características de las Terminales H.323

Los elementos principales que componen una terminal H.323 son:

**Unidad de Control del Sistema**: Proporciona la señalización para que la terminal H.323 funcione de forma adecuada. Realiza el control de llamadas, el intercambio de funciones entre los equipos implicados en la comunicación, la señalización de los canales lógicos de comandos e indicaciones, y emplea mensajes para abrir y describir completamente el contenido de los canales lógicos.

**Capa H.225:** Da formato a los datos, audio, vídeo y flujos de control para enviarlos a la interfaz de red, y restaura los datos, audio, vídeo y flujos de control recibidos de la interfaz de red. Además realiza el entramado lógico, la numeración de secuencias, y la detección y corrección de errores de forma apropiada a cada tipo de medio. Los canales de vídeo, audio, datos o informaciones de control se establecen de acuerdo con la recomendación H.245 (protocolo de control para comunicaciones multimedia), y son unidireccionales e independientes en cada dirección de transmisión.
Algunos canales lógicos, por ejemplo para datos, pueden ser bidireccionales. Se puede transmitir cualquier número de canales de cada tipo de medio, pero para cada llamada existe un único canal de control H.245. Además de los canales lógicos, los puntos finales H.323 usan dos canales de señalización para el control de llamadas y las funciones relacionadas con el *gatekeeper*. El formato de los datos enviados por los canales debe cumplir la recomendación H.225, los canales lógicos reciben un número de canal lógico en el rango de 0 a 65535 que es seleccionado de forma arbitraria por el transmisor, excepto el canal 0 que se asigna de forma permanente al canal de control H.245. El límite superior de la tasa de bits del canal lógico se establece a partir de las limitaciones de los terminales implicados en la comunicación, de forma que será el menor de ellos.

**Interfaz de Red Basada en Paquetes:** Debe proporcionar los servicios descritos en la recomendación H.225, lo cual incluye lo siguiente:

- Servicio de transporte seguro (por ejemplo mediante TCP o protocolo de control del transporte, SPX o intercambio de protocolo secuencial) entre extremos de la comunicación para el control de canal H.245, los canales de datos y el canal de señalización de llamadas.
- Servicio de transporte inseguro (por ejemplo UDP o protocolo de datagrama de usuario, IPX o intercambio de protocolo inter-red) entre extremos de la comunicación para los canales de audio, de vídeo y de RAS (Registro, Admisión y Estatus).

**Unidad de Codificación de Audio:** Se encarga de codificar la señal de audio presente en la entrada (por ejemplo la proveniente de un micrófono) de forma que sea posible una transmisión más eficiente, y decodifica la señal de audio que recibe de la otra terminal con la que ha establecido la comunicación. Todas las terminales H.323 deben ser capaces de codificar y decodificar la voz de acuerdo con la recomendación G.711 según la ley A (estándar europeo) y la ley $\mu$ (estándar americano). El algoritmo de codificación se establece mediante el intercambio de funciones entre equipos emisor y receptor mediante la recomendación H.245. Al igual que en la transmisión de vídeo, la comunicación puede ser asimétrica (por ejemplo enviar audio codificado con G.711 y recibir en G.729, siempre y cuando ambos equipos lo soporten). El formato de la señal de audio viene estipulado por la recomendación H.225 y es posible enviar y/o recibir más de un canal de audio simultáneamente, lo cual es interesante, por ejemplo, para realizar transmisiones simultáneamente en dos idiomas distintos.
Cuando se trabaja a bajas velocidades de transferencia (<56 kbps) no es posible usar la codificación de audio G.711. En dicho caso, debe usarse la recomendación G.723 o la G.729.

**Unidad de Codificación de Vídeo:** Es un elemento opcional, que en caso de incorporarlo permite realizar la codificación del equipo de vídeo de entrada (por ejemplo la cámara de un sistema de videoconferencia) y decodifica la señal de vídeo presente a la entrada, proporcionando una salida hacia el visualizador de vídeo (por ejemplo un monitor). La transferencia de vídeo, el formato de imagen y las opciones del algoritmo de codificación que puede aceptar el receptor se definen durante el intercambio de funciones mediante H.245, de

forma que el codificador tiene libertad para transmitir en cualquier condición que sea interpretable por el receptor.
Además, el receptor puede enviar peticiones (mediante H.245) para un determinado modo. Sin embargo, el receptor puede ignorar estas peticiones. Además, dos terminales H.323 pueden establecer comunicaciones con transferencias asimétricas, diferentes resoluciones y número de imágenes por segundo. El modo de trabajo seleccionado se señaliza al receptor en el mensaje OpenLogicalChannel de H.245, mientras que el formato del flujo de bits de vídeo queda definido por la recomendación H.225.

**Retardo del Camino de Recepción:** Este bloque se encarga de mantener la sincronización y tener en cuenta el retardo que experimentan los paquetes en su transmisión por la red. Otro aspecto importante es mantener la sincronización entre las imágenes y el sonido, de forma que si en la imagen aparece una persona hablando, el movimiento de los labios corresponda con los sonidos reproducidos por el altavoz.

**Aplicaciones de Datos de Usuario:** Es un elemento opcional que soporta aplicaciones como la transferencia de imágenes estáticas, intercambio de archivos, acceso a bases de datos, etc. Pueden existir uno o más canales de datos, los cuales pueden ser unidireccionales o bidireccionales, dependiendo del tipo de aplicación. Por defecto se usa la recomendación T.120, pero son posibles otras. Por ejemplo, es posible controlar la cámara de un sistema remoto (zoom, panorámico, encuadre, etc.) a partir de los protocolos H.281 y H.224.

**Función de Control H.245:** La función de control H.245 (protocolo de control para comunicaciones multimedia) utiliza el canal de control H.245 para llevar mensajes de control sobre el modo de trabajo del equipo H.323. Entre ellos cabe destacar el intercambio de capacidades entre equipos, la apertura y cierre de canales lógicos, las peticiones de preferencia de modos, los mensajes de control de flujo e indicaciones y los comandos generales.

**Función de Señalización RAS (*Registration, Admission, Signaling*):** Utiliza mensajes de H.225 para realizar registros, admisiones, cambios de anchos de banda, estados, desenganches entre puntos finales y *gatekeepers*. El canal de señalización RAS es independiente del canal de señalización de llamadas y del canal de control H.245. En entornos de red sin *gatekeeper*, no se usa el canal de señalización de RAS, mientras que si existe *gatekeeper*, el canal está abierto entre el *gatekeeper* y el punto final. El canal de señalización de RAS es el primero que se abre entre puntos finales H.323.

**Función de Señalización de Llamadas:** El canal de señalización de llamadas es independiente del canal de señalización de RAS. En sistemas sin *gatekeeper*, el canal de señalización de llamadas está abierto entre los dos puntos finales implicados en la llamada. Si existe *gatekeeper*, el canal de señalización de llamada está abierto entre el punto final y el *gatekeeper* o entre puntos finales según la elección de este último.

### 3.3.4 Características de los *Gateways*

El término *gateway* de VoIP en ocasiones también se suele utilizar para hacer referencia a otros elementos funcionales, en tal caso se le suelen llamar *gateways* de VoIP especiales, que se localizan entre redes IP para desarrollar determinadas funciones. Entidades específicas como *proxies* VoIP, transcodificadores VoIP, traductores de direcciones de red VoIP, etc., caen en esta categoría de *gateways* de VoIP.

Los gateways de interconexión son básicamente dispositivos lógicos, aunque también pueden ser dispositivos físicos, que tienen una serie de atributos que caracterizan el volumen y los tipos de servicios que pueden proveer, por ejemplo:

- Capacidad: Expresa el volumen de servicio que puede brindar, estando relacionado directamente con el número de puertos que tiene (igual al número máximo de llamadas simultáneas) y la velocidad del enlace de acceso.
- Protocolos de señalización soportados.
- *Codecs* de voz utilizados.
- Algoritmos de encriptado que soporta.
- Rango de números telefónicos que puede manejar.

En general, los *gateways* tienen que proporcionar los siguientes mecanismos o funciones:

- Adaptación de señalización: Básicamente tiene que ver con las funciones de establecimiento y terminación de las llamadas.
- Control de los medios: Se relaciona con la identificación, procesamiento e interpretación de eventos relacionados con el servicio, generados por usuarios o terminales.
- Adaptación de medios, según requerimientos de las redes.

El *gateway* de interconexión también desarrolla la función de control de medios, que se ocupa de manejar toda la información de control generada por la terminal. Para el caso de comunicaciones de voz, la información de control del nivel de usuario que destaca más son los tonos multifrecuencia DTMF que produce un teclado telefónico convencional (por ejemplo, para interactuar con un servidor de voz). Dadas las características de estas señales, en el sentido que están en el rango audible pero no son señales de voz, sino tonos, es necesario prestar particular atención en su paso por la conexión híbrida que representa el *gateway* de interconexión. Las técnicas de compresión de voz de baja velocidad introducen considerable distorsión en los tonos DTMF, provocando la recepción y correspondiente decodificación incorrecta en los receptores. Entonces, esto requiere que las señales de audio y los tonos DTMF sean separados en el *gateway* (si no lo ha sido ya en el emisor) y conducidos de forma independiente al receptor.

Hay dos posibles soluciones para el transporte de los tonos DTMF, el transporte dentro de banda que consiste en transportar estos tonos, digitalizados y paquetizados, con los protocolos RTP/UDP, mediante un formato de carga útil dedicado y el transporte fuera de banda que implica utilizar un canal de control de medios seguro (no UDP, sino TCP) para el transporte de las señales DTMF. El transporte de los tonos DTMF dentro de banda se ve afectado por la falta de garantía en la entrega de paquetes que el protocolo UDP ofrece, con nefastas consecuencias para el funcionamiento del servicio en caso de pérdida de un paquete asociado a un tono DTMF. Tiene la ventaja de que los tonos permanecen sincronizados en el tiempo con respecto a la voz. En cambio, el transporte fuera de banda si bien gana en seguridad respecto a la entrega segura de los paquetes, aunque las señales pierden su referencia exacta en el tiempo en relación con el *stream* de voz. Esta es precisamente la solución adoptada en la Recomendación H.323, mediante el canal H.245.

### 3.3.5 Transporte de VoIP

H.323 utiliza comunicaciones seguras e inseguras. En el caso de señales de control y datos su transporte debe ser seguro, no se pueden perder partes de la información y se debe recuperar en el orden en que fue enviada. Para ello se usa TCP que garantiza que la información se recibe libre de errores y en la secuencia correcta. Sin embargo, puede existir un retardo considerable en la recepción. Este protocolo es válido para el control H.245, el canal de datos T.120 y el canal de señalización de llamadas. Sin embargo, carece de sentido para la transmisión de audio y vídeo en tiempo real, puesto que si un paquete de información llega tarde ya no es útil para el receptor. Por ello, para audio y vídeo se usa un protocolo de transmisión inseguro que a cambio ofrece una transmisión más eficiente, que en el protocolo Internet es el UDP (Ver capitulo 2). UDP usa un número mínimo de bits extras de protocolo ya que se establece un circuito virtual en la red desde el emisor al receptor. De esta forma todos los paquetes de información seguirán la misma ruta y por tanto será la propia red la que se encargará de que se entreguen en el mismo orden en que fueron introducidos. H.323 utiliza UDP para transportar la información de audio, de vídeo y el canal RAS. UDP asegura el mejor esfuerzo para entregar los paquetes de información al receptor, pero es posible que existan pérdidas de paquetes, recepción de paquetes duplicados, etc.

En conferencias con múltiples fuentes de audio y vídeo se usa un proceso denominado ***multicast***, que consiste en transmitir de una única fuente a varios destinos. El mecanismo usado para esto puede variar según el tipo de tecnología de red, pero se usa el protocolo de tiempo real (RTP) para gestionar el audio y el vídeo. De esta forma se añade una cabecera a cada paquete que contiene el código de tiempo y un número de secuencia. El receptor incorpora un *buffer* y a partir de la información de cabecera reordena los paquetes, sincroniza el sonido con el vídeo, elimina los paquetes duplicados y realiza una reproducción continua.

Dado que resulta crítico disponer en la red IP del ancho de banda necesario para una aplicación multimedia, se usa un protocolo de reserva de recurso desarrollado por IETF (*Internet Engineering Task Force*) llamado

RSVP (*Reservation Protocol*), que permite a un receptor pedir una cantidad de ancho de banda determinada y recibir una respuesta indicando si es posible asegurar la petición.

### 3.3.6 Características de los Teléfonos IP de Software

La voz y las llamadas telefónicas pueden ser vistas como una de las muchas aplicaciones para una red IP, mediante un software (*software IP phone*) usado como soporte de la aplicación y de la interfaz de la red. Las funcionalidades del software requeridas para la conversión de voz a paquetes en una terminal VoIP o *gateway* se llevan a cabo mediante los siguientes módulos:

**Módulo de Procesamiento de Voz**: Que prepara las muestras de voz para la transmisión por la red de paquetes. Este software se ejecuta sobre un DSP (*Digital Signal Processor*).

**Módulo de Procesamiento de Llamada (*Signaling*):** Que actúa como un *gateway* de señalización permitiendo que las llamadas sean establecidas a través de la red telefónica convencional.

**Módulo de Procesamiento de Paquetes**: El cual procesa los paquetes de voz y señales, añadiendo la apropiada prioridad de transporte para presentar los paquetes a la red IP (u otras redes de paquetes). La información de señales es convertida desde los protocolos de telefonía al protocolo de señalización de paquetes.

**Módulo de Administración de la Red:** El cual proporciona funcionalidad de agente de control, permitiendo informes remotos y control de configuración para ser llevado a cabo desde sistemas de control. El módulo de administración de la red puede incluir servicios tales como el soporte para la seguridad, para el acceso a directorios de marcado y para el soporte a accesos remotos.

#### 3.3.6.1 Módulo de Procesamiento de Voz

El módulo de Procesamiento de Voz debe incluir los siguientes elementos y funciones:

**Interfaz PCM**: Que recibe las muestras desde la interfaz de telefonía (PCM) y los dirige al módulo de software VoIP apropiado para procesarlos (y viceversa). La interfaz PCM lleva a cabo una continua fase de remuestreo de salida a la interfaz analógica.

**Unidad de Anulación de Eco**: Que realiza la anulación de eco en señales de puertos de voz full-dúplex de acuerdo con el estándar ITU G.165 o G.168. A partir de que el retraso de ida y vuelta en VoIP es mayor de 50 milisegundos (punto en el cual el eco resulta intolerable), la anulación de eco es necesaria. Los parámetros operacionales pueden ser programables.

**Detector de Actividad de Voz**: Que suprime la transmisión de paquetes cuando no hay presentes señales de voz (guardando ancho de banda). Si no se detecta actividad durante un período de tiempo, la salida del codificador de voz no es transportada a través de la red. Los niveles de falta de ruido son también medidos y presentados al destino, por eso un ruido confortable (*comfort noise)* puede ser insertado en la llamada (así el oyente no recibe señales vacías en su teléfono).

**Detector de Tono**: El cual detecta la recepción de tonos DTMF y distingue entre señales de voz y señales de fax. Puede ser usado para invocar a las funciones de procesamiento de voz apropiadas (es decir, la decodificación y empaquetamiento de información de fax o la compresión de voz).

**Generador de Tono**: El cual genera tonos DTMF y tonos de progreso de llamada bajo el dominio del sistema operativo.

**Módulo de Procesamiento de Fax**: El cual proporciona una función de retraso de fax demodulando los datos PCM, extrayendo la información relevante y empaquetando los datos obtenidos.

**Módulo de Protocolo de Paquetes de Voz**: El cual encapsula los datos de voz y fax comprimidos para su transmisión sobre la red de datos. Cada paquete incluye un número de secuencia que permite que los paquetes recibidos sean entregados en el orden correcto. Esto también permite que los intervalos de silencio se reproduzcan correctamente y se detecten paquetes perdidos.

**Módulo de Reproducción de la Voz**: El cual almacena los paquetes que son recibidos y los envía a los *codecs* de voz para su reproducción. Este módulo proporciona un buffer adaptable y un mecanismo de medida que permite adaptar los tamaños del buffer al funcionamiento de la red.

#### 3.3.6.2 Módulo de Señalización

El subsistema de Procesamiento de Llamadas (*signaling*) detecta la presencia de una nueva llamada y recoge información de direccionamiento. Varios estándares de señales telefónicas deben ser soportados. Un número de funciones deben ser ejecutadas si una llamada de teléfono es soportada.

- La interfaz a la red telefónica debe ser monitorizada para recoger comandos de entrada y respuestas.
- Los protocolos de señalización deben ser terminados y la información debe ser extraída.
- La información de señalización debe ser organizada en un formato que pueda ser usado para establecer una sesión a través de la red de paquetes.
- Los números de teléfono deben ser convertidos a direcciones IP (con la necesidad potencial de una referencia externa a un servicio de directorio).

Dos aproximaciones para realizar el marcado son usadas, marcar el número de destino y usar funciones de selección automática de rutas o marcar el número del puerto VoIP y marcar el destino real.

El software usado en los dispositivos VoIP debe también ser soportado por un entorno operativo en tiempo real y provisto de la habilidad para comunicarse entre módulos y con el mundo exterior.

La habilidad para digitalizar y procesar *streams* de voz usando software independiente construyendo bloques es la clave del éxito de la implementación de VoIP.

### 3.3.7 Fases de Comunicación Mediante Protocolos de H.323

***Discovery*:** Se trata del proceso mediante el cual la terminal H.323 determina cual es el GK que atiende a la red en ese momento. El mensaje desde la terminal es del tipo *multicast* y se denomina **GRQ** (*Gatekeeper Request*), el GK responde con la aceptación **GCF** (*GK Confirmation*) o rechazo **GRJ** (*GK Reject*). El GK puede indicar un GK alternativo mediante mensajes **alternateGatekeeper**. Si no se está en condiciones de procesar el *request* se puede enviar un mensaje **RIP** (*Request in Progress*) para indicar que se está procesando la petición.

***Registration*:** La terminal informa de sus direcciones de transporte y alias mediante **RRQ** (*Registration Request*) y el GK responde con **RCF** (*Registration Confirmation*) o **RRJ** (*Registration Reject*). El RRQ se emite en forma periódica. El proceso de registro debe tener un tiempo de duración (expresado en segundos) para lo cual se utiliza el mensaje **timeToLive**. La terminal o el GK pueden cancelar la registración mediante el mensaje **URQ** (*Unregister Request*) al cual le corresponde la confirmación **URF** (*Unregister Confirmation*).

***Location*:** Una terminal o GK que tiene un alias para una terminal y quiere determinar su información de contacto puede emitir el mensaje de requerimiento de localización **LRQ** (*Location Request*). Al cual le corresponde la confirmación **LCF** (*Location Confirmation*) con la información requerida. La dirección puede ser del tipo IP si se trata de un GK fuera de la red.

***Admission*:** El pedido de admisión de la terminal al GK es el **ARQ** (*Admissions Request*) y contiene un requerimiento ***Call Bandwidth*** (en formato Q.931). El GK puede reducir las características de la solicitud en el mensaje de confirmación **ACF** (*Admissions Confirm*). En el mismo mensaje ARQ se dispone de la

funcionalidad **TransportQOS** para habilitar la funcionalidad de reservación de ancho de banda RSVP, para servicios unidireccionales (orientado al receptor).

***Bandwidth*:** Durante una conexión el terminal o el GK pueden requerir el cambio de ancho de banda del canal mediante el mensaje **BCR** (*Bandwidth Change Request*).

***Status*:** Se trata de un mensaje periódico (mayor a 10 seg) que emite el GK a la terminal para determinar el estado y requerir diagnóstico. Se trata de los mensajes **IRQ** (*Information Request*) y **IRR** (*Information Response*). La habilitación se realiza mediante **willRespondToIRR** enviado en el mensaje RCF o ACF.

#### 3.3.7.1 Proceso de Comunicación H.323

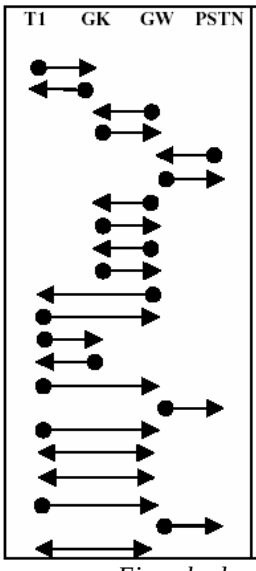
Se describen a continuación los distintos mensajes y etapas en el proceso de conexión de H.323. Más adelante se muestra un ejemplo del procedimiento de conexión, comunicación y desconexión de una llamada. De existir varios GK se disponen de mensajes para intercomunicación, por ejemplo, **LRQ** para *Locate Request* y **LCF** para *Locate Confirm*.

En H.323 se describen 3 tipos de mensajes de señalización diferentes:

**Mensaje H.245**: Se describen estos mensajes en forma de texto concatenado en letras tipo bold (ejemplo: **maximumDelayJitter**).

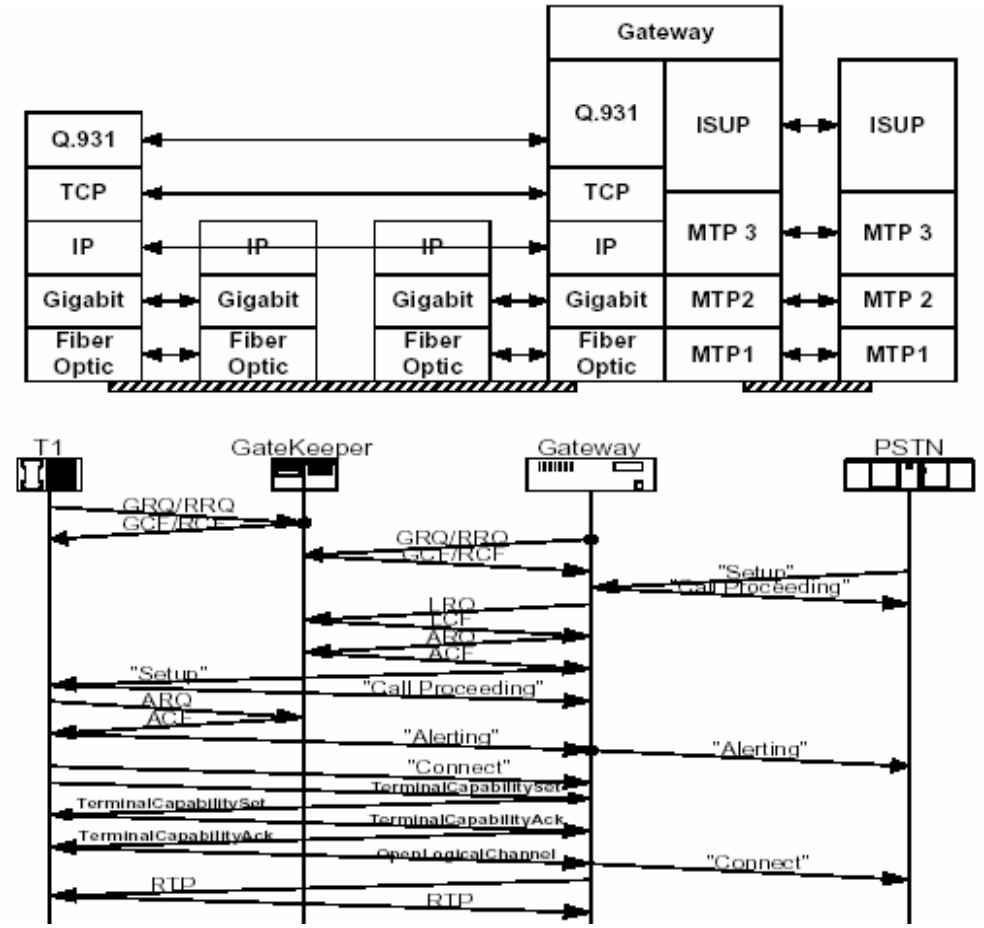
**Mensaje RAS**: Se representa mediante 3 letras (ejemplo: ARQ) y es usado para señalización entre terminal y *gatekeeper*.

**Mensaje H.225/Q.931**: Representado en una o dos palabras con la primera letra en mayúsculas (ejemplo: *Call Proceeding*). Es usado para encapsular los mensajes H.245 de señalización entre terminales y originalmente fue diseñado como protocolo DSS1 en capa 3/7 para los accesos ISDN.




| Protocolo | Mensaje |
|---|---|
| | **CALL SETUP** |
| RAS | GRQ/RRQ. Es el requerimiento de registración del terminal al gatekeeper. |
| RAS | GCF/RCF. Es la confirmación de registración desde el gatekeeper. |
| RAS | GRQ/RRQ. Es el requerimiento de registración del gateway al gatekeeper. |
| RAS | GCF/RCF. Es la confirmación de registración desde el gatekeeper. |
| ISUP | "Setup". Llamada entrante desde la PSTN con las direcciones E-164. |
| ISUP | "Call Proceeding". Se informa a la PSTN del procesamiento de llamada. |
| RAS | LRQ. Es el requerimiento de locación sobre el gatekeeper. |
| RAS | LCF. Es la confirmación de locación. |
| RAS | ARQ. Es el requerimiento de admisión de llamada. |
| RAS | ACF. Es la confirmación de admisión. |
| Q.931 | "Setup". Requerimiento de setup de llamada sobre el terminal. |
| Q.931 | "Call Proceeding". Información de llamada en proceso. |
| RAS | ARQ. Requerimiento de admisión del terminal sobre el gatekeeper. |
| RAS | ACF. Conformación de admisión. |
| Q.931 | "Alerting". Señalización de ring de llamada en proceso. |
| ISUP | "Alerting". Señalización de ring de llamada en proceso. |
| Q.931 | "Connect". Señalización de respuesta del terminal. |
| H.245 | **TerminalCapabilitySet.** Mensaje de H.245 para determinar capacidades. |
| H.245 | **TerminalCapabilityAck.** Confirmación. |
| H.245 | **OpenLogicalChannel.** Mensaje para abrir un canal lógico. |
| ISUP | "Connect". Mensaje de ISUP de conexión establecida. |
| RTP | Paquetes RTP con información vocal. |

*Ejemplo de señalización de llamada en H.323 desde la PSTN (RTPC).*




*Modelo de capas y mensajes en la conexión H.323*

**3.3.7.1.1 Formato de los Paquetes H.225/245.**

El formato del paquete H.225 sigue la estructura del **ITU-T Q.931**. Contiene la siguiente secuencia de bytes (equivalente a ISUP de SS7):

**PD** (Discriminador de Protocolo): (1 Byte) Identifica el mensaje de control de llamada en la interfaz usuario a red.
**RF** (*Call Reference Information Element*)**:** (2 Bytes) Referencia de llamada en la conexión usuario red. Contiene:

- **Length:** (1 Byte) Indica la longitud de CRV mediante 4 bits y 4 bits de relleno 0000
- **CRV** (*Call Reference Value*): (1 Byte) Análogo al identificador de canal lógico en la red X.25. Utiliza 7 bits y permite la multiplexación en el canal D. En el acceso primario ocupa 2 Bytes.

**MT** (*Message Type*): (1 Byte) Es el identificador del tipo de mensaje. Se disponen de las siguientes posibilidades:

- **Establecimiento de llamada:** Alerta o aviso, llamada en curso, inicio de conexión (*setup*), acuse de conexión, reconocimiento de inicio y de conexión.
- **Fase activa de la llamada:** Reanudación de llamada, acuse de reanudación, rechazo de reanudación, suspensión de llamada, acuse de suspensión, rechazo de suspensión, información de usuario.
- **Desconexión de la llamada:** Inicio de desconexión de llamada, liberación, liberación completada, reinicio y acuse recibo de reinicio.
- **Misceláneos**: Control de congestión, información, facilidades, notificación, estado, consulta de estado.

**ID:** (1 Byte) Identificador de mensaje para informar si lo que sigue es un mensaje de usuario a usuario, un estado de desconexión o el número de llamada.
**LON:** (1 Byte) Indica la longitud del contenido del mensaje.
**CON:** (N Bytes) Contenido del mensaje propiamente dicho. Para un mensaje de *Setup* (similar a IAM) se dispone de los siguientes campos:

- **Type:** (3 bits) Identifica el tipo de llamada
- **NSI:** (4 bits) Identifica el esquema de numeración utilizado.
- **NUM:** (Nx7 bits) Se trata de la transferencia de cifras en codificación de 7 bits cada cifra.

Sobre el paquete H.225 se dispone del MT para identificar la función del mensaje. Entre los distintos tipos de mensaje se encuentran:

- Mensajes para establecimiento de llamada: *Alerting, Call Proceeding, Connect, Setup, Progress*, etc.
- Mensajes para la fase de información de llamada: *Resume, Suspend, User Information*, etc.
- Mensajes para el cierre de la llamada: *Disconnect, Release, Restart*, etc.
- Mensajes misceláneos: *Segment, Congestion Control, Information, Notify, Status, Status Enquiry*, etc.

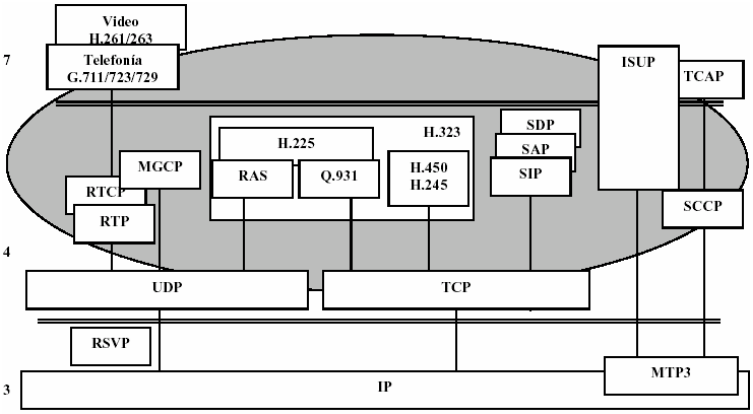
Los mensajes manejados en el ámbito de H.245 (durante la fase de comunicación telefónica) son:

**MultimediaSystemControl:** Para efectuar el control del sistema, las variantes del mensaje son *request, response, command and indication.*

Otros mensajes de interés que se utilizan en H.245: *masterSlaveDetermination, terminalCapability, MaintenanceLoop, communicationMode, communicationMode, conferenceRequest and Response, terminalID.*

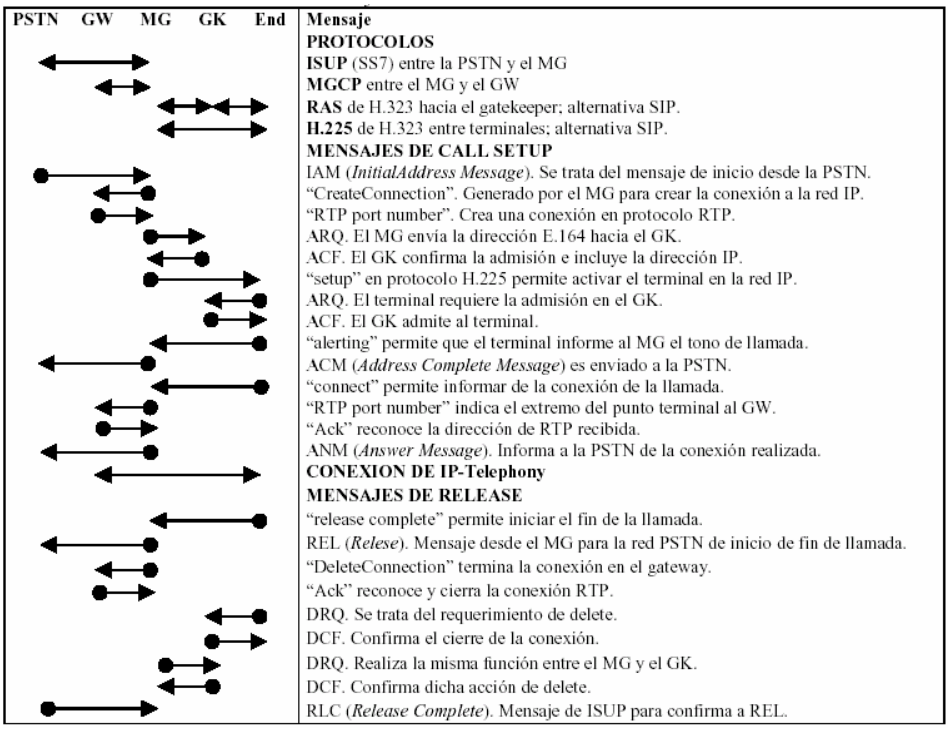
### 3.3.8 Modelo de Capas y Protocolos Utilizados en VoIP

A continuación se muestra el modelo de capas y protocolos que son utilizados por VoIP, en el se puede apreciar de manera grafica todos los protocolos que se requieren la realizar una llamada de VoIP y las capas de red en que actúan dichos protocolos.

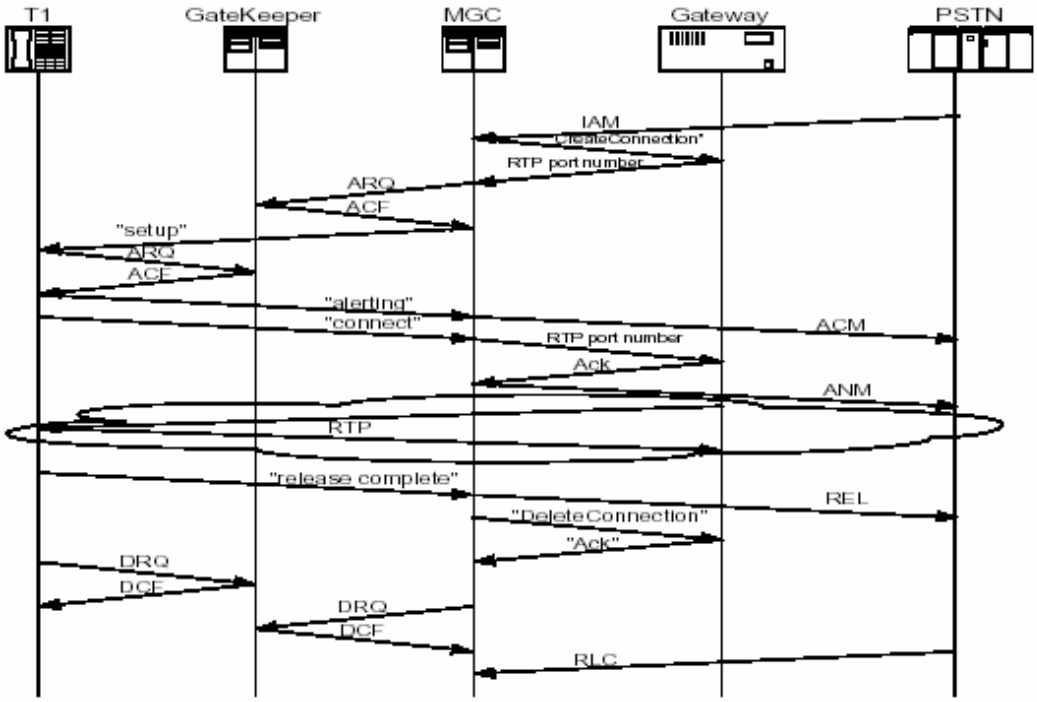



*Modelo de Capas*

A continuación se muestra un ejemplo de intercambio de mensajes en una red de VoIP H.323, que involucra a casi la totalidad de los protocolos de señalización involucrados en este estándar.




*Conexión y desconexión en una llamada desde la RTC a VoIP.*




*Intercambio de mensajes*

### 3.4 Protocolos de Red Usados por VoIP

A continuación se describen algunos de los protocolos de red más importantes que son empleados para brindar servicios de VoIP:

### 3.4.1 Protocolo ISUP

**ISUP** (*ISDN Unit Part*) es el protocolo del ITU-T usado para mensajes de señalización en la red telefónica pública. Una red de VoIP utiliza a ISUP en el borde para comunicarse con la RTPC. Dentro de la nube IP el protocolo ISUP es transportado por TCP/IP. El ISUP corresponde a funciones de capa 4/7 en el conjunto de protocolos de señalización por canal común SS7 del ITU-T.

### 3.4.2 Protocolo RTP (*Real-Time Transport Protocol*)

El protocolo RTP tiene como objetivo asegurar una **QoS** para servicios del tipo tiempo real, es decir aplicaciones que no son tolerantes al retraso, como es el caso de la voz. Incluye la identificación del *payload*, la numeración secuencial, la medición de tiempo 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. El protocolo **RTP** es de transporte (capa 4) y trabaja sobre **UDP**, de forma que posee un *checksum* para detección de errores y cuenta con la posibilidad de la multiplexación de puertos (*ports* 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 puerto en UDP. Sobre RTP se disponen de protocolos de aplicación del tipo H.320/323 para vídeo y voz. RTP funciona en conjunto con **RSVP** (protocolo de capa 3) para la reservación de ancho de banda y asegurar de esta forma la calidad del servicio **QoS** del tipo Garantizada. 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 los *routers*.
Un algoritmo particular de gestión de prioridad de tráfico es el **WFQ** (*Weighted Fair Queuing*) que utiliza un modelo de multiplexación TDM para distribuir el ancho de banda entre clientes, donde cada cliente ocupa un intervalo de tiempo en un modelo *Round-Robin*.
El tipo de servicio **ToS** (*Type of Service*) en IP puede ser usado para determinar un ancho de banda específico para el cliente, por ejemplo un servicio sensible al retardo requiere un ancho de banda superior. En IP además del ToS se puede utilizar la dirección de origen y destino IP, el tipo de protocolo y el número de *socket* para asignar una ponderación. En redes que disponen de *switches* de capa 2 se requiere extender la gestión de la calidad de servicio a dicha capa. Para ello la IEEE ha determinado el ToS sobre IEEE-802.3. RTP además provee transporte para direcciones *unicast* y *multicast*. Por esta razón, también se encuentra involucrado el protocolo IGMP para administrar el servicio *multicast*. El paquete de RTP incluye un encabezado fijo y el *payload* de datos, RTCP utiliza el encabezado de RTP y ocupa el campo de carga útil.

#### 3.4.2.1 Campos del Protocolo RTP

**OH:** 2 Bytes de encabezado fijo para aplicaciones de identificación.
- **VRS:** (2 bits) Es la versión del protocolo.
- **PAD:** (1 bit) El bit de *padding* activo informa que luego del encabezado existen bytes adicionales (por ejemplo para algoritmos de criptografía).
- **X:** (1 bit) Con el bit de extensión activado existe solo una extensión del encabezado.
- **CC** (*CSRC Count*): (4 bits) Identifica el número de identificadores CSRC al final del encabezado fijo.
- **M: (**1 bit de *Marker*) La interpretación está definida por el perfil. H.225 indica que es usado para identificar períodos de silencio (fijado en 1 para el primer paquete luego del período de silencio).
- **PT** (*Payload Type*): (7 bits) Identifica el formato de *payload* y determina la interpretación de la aplicación. Por ejemplo, el IANA (la autoridad que reserva números en Internet) ha reservado el PT=18 para el codificador G.729, PT=8 para el PCM ley-A, PT=31 para vídeo H.261.

**SN** (*Sequence Number*): (2 Bytes) Numera en forma secuencial los paquetes de RTP y permite la identificación de paquetes perdidos.
**TS** (*TimeStamp*): (4 Bytes) Refleja el instante de muestreo del primer Byte en el paquete RTP (en telefonía la frecuencia de reloj es de 8000 Hz). Dependiendo de la aplicación es el uso de esta información. En aplicaciones de vídeo puede permitir determinar modificaciones en el orden de los paquetes o la pérdida de los mismos. En aplicaciones de audio puede permitir el cálculo del tiempo de propagación y *jitter* en la red y de esta forma gestionar el buffer de recepción. La ausencia del paquete a tiempo puede obligar a la interpolación de muestras.

**SSRC** (*Synchronization Source*): (4 Bytes) Identifica la fuente de sincronismo de forma que dos sesiones del mismo RTP tengan distinta SSRC. Todos los paquetes con idéntico SSRC tienen un tiempo y referencia de secuenciamiento común.
**CSRC** (*Contribution Source*): (Nx4 Bytes) Identifica la fuente que contribuye al *payload* contenido en el paquete. El valor de N lo da el campo CC.

#### 3.4.2.2 RTP-HC (*Real-Time Protocol-Header Compression*)

La compresión del encabezado permite mejorar la eficiencia del enlace en paquetes de corta carga útil. Se trata de reducir los 40 bytes de RTP/UDP/IP a una fracción de 2 a 5 bytes, eliminando aquellos que se repiten en todos los datagramas. Como los servicios de tiempo real generalmente trabajan con paquetes pequeños y generados en forma periódica se procede a formar un encabezado de longitud reducida que mejore la eficiencia de la red.

### 3.4.3 Protocolo de Control RTCP (*Real-Time Control Protocol*)

Este protocolo permite completar a RTP facilitando la comunicación entre extremos para intercambiar datos y monitorear de esta forma la calidad de servicio y obtener información acerca de los participantes en la sesión. RTCP se fundamenta en la transmisión periódica de paquetes de control a todos los participantes en la sesión usando el mismo mecanismo RTP de distribución de paquetes de datos. El protocolo UDP dispone de distintas puertas (*UDP Ports*) como mecanismo de identificación de protocolos. La función primordial de RTCP es la de proveer una realimentación de la calidad de servicio, se relaciona con el control de congestión y flujo de datos. RTCP involucra varios tipos de mensajes (uno de los más interesantes es el *send report*):

***Send Report**:* Para emisión y recepción estadísticas (en tiempos aleatorios) desde emisores activos.
***Receiver Report**:* Para recepción de estadísticas desde emisores no activos.
***Source Description**:* Para un identificador de nivel de transporte denominado CNAME (*Canonical Name*).
***Bye**:* Para indicar el final de la participación.
***Application**:* Para aplicaciones específicas.

#### 3.4.3.1 Formato del Mensaje *Send Report*

**Encabezado Común**

**OH:** 1 Byte de encabezado con las siguientes funciones:
- **VRS:** (2 bits) Identifica la actual versión del protocolo.
- **PAD:** (1 bit) Indica si luego de este paquete existe un *padding* adicional (por ejemplo, para completar el número de Bytes para criptografía en múltiplos de 8).
- **RC** (*Reception Report Count*): (5 bits) Contiene el número de bloques de reportes (unidades de 6x4 Bytes) que contiene el paquete. Un paquete puede contener más de un reporte de retorno.

**PT** (*Packet Type*): (1 Byte) Identifica el tipo de paquete (decimal=200 para el paquete *Sender Report*).
**Length:** (2 Bytes) Indica la longitud del paquete en unidades de 4 Bytes.
**SSRC:** (4 Bytes) Identifica la fuente de temporización para el generador del reporte.

**Información Para Evaluación de Parámetros**

**NTP-TS** (*Network Time Protocol-TimeStamp*): (8 Bytes) Es el tiempo relativo al UTC. Para otras aplicaciones se utiliza una versión reducida de 4 Bytes con la información de tiempo más significativa.
**RTP-TS:** (4 Bytes) Se refiere al *TimeStamp* que es emitido en RTP.
**SPC** (*Sender´s Packet Count*): (4 Bytes) Es el total de paquetes emitidos por el transmisor desde el inicio de la sesión.
**SOC** (*Sender´s Octet Count*): (4 Bytes) Es el total de Bytes transmitidos desde el inicio de la sesión como carga útil. Es usado para estimar la tasa de datos promedio de *payload* en conjunto con SPC.

**Reportes de Parámetros Evaluados**

**SSRC-n** (*Source Identifier*): (4 Bytes) Identifica la fuente SSRC de información en el reporte de recepción.
**FL** (*Fraction Lost*): (1 Byte) Indica la relación fraccional (paquete perdido/total de paquetes) de paquetes perdidos desde el último reporte.
**CNPL** (*Cumulative Number Packet Lost*): (3 Bytes) Indica el total de paquetes perdidos desde el inicio de la recepción.
**EHSNR** (*Extended Highest Sequence Number Received*): (4 Bytes) Indica la numeración secuencial de recepción. Si el inicio de la recepción es distinto implica que los distintos posibles receptores (*multicast*) tienen un campo EHSNR diverso.
**IJ** (*Interarrival Jitter*): (4 Bytes) El *jitter* se mide como la desviación de recepción respecto de la transmisión. Equivale a la diferencia de tiempo de tránsito relativo.
**LSR-TS** (*Last SR TimeStamp*): (4 Bytes) Es el último *timestamp* (información más significativa) de los paquetes recibidos.
**DLSR** (*Delay Since Last SR*): (4 Bytes) Es el retardo (entre la emisión y recepción) en unidades de 1/65536 seg. del último paquete recibido.

Los mensajes *Send Report* disponen de 3 secciones bien diferenciadas:

- Los primeros 8 Bytes (desde la versión hasta el identificador de la fuente de temporización SSRC) se refieren a un encabezado común.
- La segunda parte de 20 Bytes (desde el tiempo universal de emisión NTP-TS hasta el conteo de octetos emitidos SOC) permite la evaluación de diferentes parámetros (retardo, *jitter*, eficiencia de datos, etc).
- La tercera parte de 24 Bytes lleva reportes que han sido obtenidos desde el último reporte informado.

Obsérvese la presencia de reportes referidos a la cantidad total de paquetes RTP perdidos y a la proporción de los mismos, la cantidad de paquetes recibidos y el *jitter* entre paquetes, el horario del último paquete recibido y el retardo de transmisión del mismo. Se puede comparar este formato de RTCP con el utilizado en AAL5/ATM para reportes y mediciones de calidad de servicio (tasa de error, tasa de celdas perdidas, etc). La medición de tiempo y *jitter* se realiza en la misma unidad que el RTP *Timestamp*.

### 3.5 Protocolos de la IETF para VoIP

El protocolo H.323 es complejo y orientado principalmente a las aplicaciones en multimedia LAN, por esta razón existen generaciones de protocolos posteriores definidos por la EITF, los cuales interactúan entre si y con H.323, entre los cuales están incluidos MGCP y SIP que representan una alternativa para la implementación de VoIP.

#### 3.5.1 Protocolos para Multimedia

**MGCP** (*Media Gateway Control Protocol*): Es un protocolo que soporta un control de señalización de llamada escalable. El control de QoS se integra en el *gateway* o en el controlador de llamadas. Este protocolo tiene su origen en el SGCP (de Cisco y Bellcore) e IPDC.

**SIP** (*Session Initiation Protocol*) RFC-2543: SIP se aplica para sesiones punto a punto o *unicast*, puede ser usado para enviar una invitación a participar en una conferencia *multicast.* Utiliza el modelo cliente-servidor y se adapta para las aplicaciones de VoIP. El servidor puede actuar en modo *proxy* o *redirect* (se direcciona el requerimiento de llamada a un servidor apropiado).

**SAP** (*Session Announcement Protocol*): SAP es usado para gestionar sesiones del tipo *multicast* entre un gran grupo de recipientes, lo que le permite anunciar sesiones de *multicast* (en forma similar al e-mail, *newsgroups*, páginas web). Utiliza mensajes UDP para *multicast*.

**RTSP** (*Real Time Streaming Protocol*) RFC-2326: RTSP es usado como interfaz a un servidor que entrega datos en tiempo real (por ejemplo un servidor del tipo *halfduplex*). RTSP establece y controla los flujos de tiempo real (audio y video). Actúa como control remoto de red para servidores multimedia. La sintaxis y operación son intencionalmente similares a HTTP, por lo que puede ser fácilmente asimilable.

**SDP** (*Session Description Protocol*) RFC-2327: SDP se utiliza para describir la sesión y trabaja sobre todos los anteriores protocolos. La descripción de la sesión incluye el nombre, período de tiempo, tipo de medio (vídeo, audio, etc), protocolo de transporte y número de puerto, información de ancho de banda, etc.
Se utiliza en aplicaciones de *multicast*. Se encarga de las sesiones en conferencia para comunicar direcciones e informaciones específicas para participar de la misma. Permite simplificar el proceso a conocer la dirección *multicast* IP y el puerto UDP. Es un protocolo de sesión que puede trabajar con cualquier protocolo de transporte, como son SAP, SIP, RTSP o protocolos como HTTP. SDP es el protocolo que se utiliza para describir una sesión multimedia dentro de un mensaje de petición SIP. El propósito de éste es transportar información acerca de los medios de comunicación en sesiones multimedia, permitiendo a los diferentes usuarios recibir una descripción de la sesión para participar en ésta.

### 3.5.2 Protocolo MGCP

MGCP (RFC-2705) es un protocolo que permite comunicar al controlador de *gateway* **MGC** (también conocido como *Call Agent*) con los *gateways* de telefonía **GW** (hacia la PBX o RTC). Se trata de un protocolo de tipo *master/slave* 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 *routers* 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. MGCP entrega al GW la dirección IP, el puerto de UDP y los perfiles de RPT, siguiendo los lineamientos del protocolo **SDP.**

#### 3.5.2.1 Comandos de MGCP

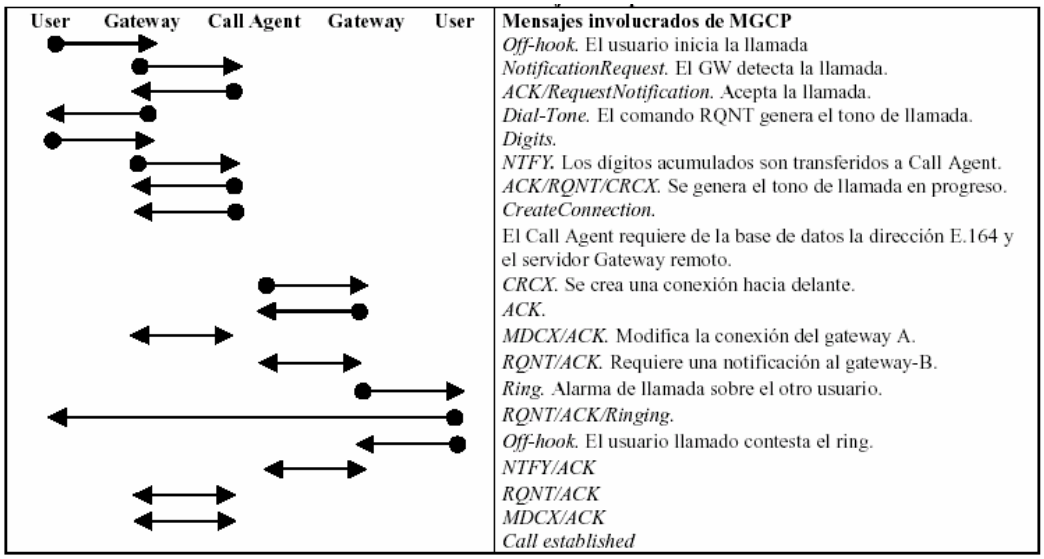
Los comandos disponibles en MGCP son los siguientes:

*NotificationsRequest*: Indica al GW de eventos, como son la señalización DTMF en el extremo.
*Notification Command*: Confirma las acciones del comando NotificationsRequest.
*CreateConnection*: Usado para crear una conexión que se inicia en el GW.
*ModifyConnection*: Usado para cambiar los parámetros de la conexión existente.
*DeleteConnection*: 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.

Los comandos *AuditEndpoint* y *AuditConnection* permiten obtener información que posteriormente forman parte de la MIB y pueden consultadas mediante el protocolo SNMP o por el sistema de administración.

Como respuesta al comando *DeleteConnection* el GW envía una serie de informaciones obtenidas desde el protocolo RTP, el número de paquetes y de Bytes emitidos, el número de paquetes y Bytes recibidos, el número de paquetes perdidos, el *jitter* promedio en ms. y el retardo de la transmisión (las definiciones se encuentran en RFC-1889).

Por ejemplo, el comando de *AuditEndPoint* permite obtener las siguientes informaciones: *RequestedEvents, DigitMap, SignalRequests, RequestIdentifier, NotifiedEntity, ConnectionIdentifiers, DetectEvents, ObservedEvents, EventStates, RestartReason, RestartDelay, ReasonCode, and Capabilities.*




*Intercambio de mensajes en el protocolo MGCP*

### 3.5.3 Protocolo SIP

El protocolo H.323 es básicamente usado para conexiones en el interior de una red corporativa o en una red IP. El IETF ha generado un conjunto de protocolos que simplifican esta función. SIP es un protocolo más simple que H.323 y está basado en HTTP.

En H.323 se utiliza el *gatekeeper*, mientras que en SIP se usa el SIP *Server*, el cual tiene mejores aspectos de escalabilidad para redes grandes. En H.323 para grandes redes se recurre a definir zonas de influencia y colocar varios *gatekepper* y para la interoperación de protocolos se requiere un *gateway* de borde que realice la conversión.

SIP es un protocolo basado en texto (de acuerdo con RFC-2279 para la codificación del conjunto de caracteres) y utiliza mensajes basados en HTTP (RFC-2068 para la semántica y sintaxis). La dirección usada en SIP se basa en un localizador **URL** (*Uniform Resource Locater*) con formato *sip: marco@192.190.132.31* (o mediante un dominio Domain: unam.com.mx), de forma que SIP integra su servicio a la Internet. En este modelo se integra un servidor de resolución de dominio **DNS** (*Domain Name Server*).

SIP es un protocolo de señalización de la capa de aplicación que puede establecer, modificar y terminar sesiones interactivas multimedia sobre IP entre terminales inteligentes. Estas sesiones incluyen conferencias multimedia y llamadas de teléfono sobre Internet, y distribución multimedia. Los miembros en una sesión pueden comunicarse vía *multicast.*

SIP soporta descripciones de la sesión que permiten a los participantes ponerse de acuerdo en el tipo de medio de comunicación a utilizar. También soporta movilidad del usuario gracias al paso o redirección de peticiones, a través de un *proxy* o servidor, para la localización actual del usuario. SIP no está atado a ningún protocolo de control de conferencia en particular.

SIP está fuertemente basado en los protocolos del IETF: SMTP (*Simple Mail Transfer Protocol*) y el HTTP (*HyperText Transfer Protocol*). Del mismo modo que ambos, SIP es un protocolo cliente-servidor textual. SIP reutiliza mucha de la sintaxis y semántica de HTTP, incluyendo su arquitectura de código de respuesta, muchas cabeceras de mensaje y su completa operación. Cada petición SIP es una tentativa de invocar algún método en el servidor.

SIP suministra bloques funcionales a las nuevas aplicaciones de comunicaciones:

- Potentes esquemas de direccionamiento (URLs) para servicios dirigidos a los usuarios.
- Facilidades y negociación de medios para aplicaciones de medios combinados de fácil actualización y terminales *plug&play* mejorados.
- Integración sin problemas con las redes y aplicaciones IP existentes, integración con los servidores de nombres de dominio (DNS) de la red y con el directorio corporativo que utiliza el protocolo ligero de acceso al directorio (LDAP), etc.
- Facilidad incorporada de extensión para otras tecnologías de información como correo electrónico, documentos transportados como adjuntos *Multipurpose Internet Mail Extension* (MIME), etc.
- Nuevas facilidades como el mecanismo de abono/notificación que es adecuado para transportar la información de presencia de usuario y de estado del terminal. También soporta la mensajería multimedia instantánea.

La tecnología SIP proporciona una arquitectura *peer to peer* en la cual la inteligencia se suministra en el borde de la red (terminales, servidores de aplicación). La red proporciona funciones a medida (transporte, control de acceso, enrutamiento, control del ancho de banda, etc.), mejorando de esta forma la escalabilidad y la solidez. Los servicios en tiempo real centralizados (supervisión de llamadas, encolado de llamadas) se implementan en el borde de la red en servidores de aplicación. También se pueden suministrar mediante entidades que son monitorizadas por aplicaciones, o que interpretan la inteligencia (*scripts*, códigos, etc.) empujadas por dichas entidades.
SIP ofrece direccionamiento de direcciones y direccionamiento de contenidos. El direccionamiento de direcciones es el proceso de enrutamiento que permite a las entidades SIP recibir mensajes SIP a beneficio de un usuario para suministrarle servicios. Como las direcciones de correo electrónico, los URLs de SIP describen un dominio de usuario. Los mensajes en primer lugar se encaminan al dominio, después se envían por las entidades de red del dominio a los terminales, a otros servidores de red o a las aplicaciones. En una base de datos de la posición se mantienen vinculaciones entre los URLs SIP públicos y los URLs de destino, que se pueden actualizar dinámicamente mediante mensajes SIP. Estos mecanismos reducen las limitaciones en la instalación de los servicios, simplificando el desarrollo de nuevos servicios y permitiendo que se puedan mezclar servicios alojados por el operador y servicios alojados por las corporaciones. El direccionamiento de contenidos significa que el SIP no transporta contenidos de datos, sino que transporta los URLs que las entidades del borde pueden utilizar para recuperar los contenidos. Esto da lugar a un único acceso convergente a los contenidos de las aplicaciones. Los terminales SIP dan acceso a las aplicaciones de la empresa.

SIP suministra protección de integridad y de confidencialidad de extremo a extremo. La seguridad salto a salto en la red se trata en el nivel de transporte de la red.

La arquitectura funcional distribuida consta de un servidor de aplicación SIP, que maneja no sólo el protocolo SIP, sino también los diferentes protocolos estándar para construir aplicaciones de medios combinados dirigidas al usuario. Los medios involucrados en cada sesión de comunicación (voz, vídeo, web, correo electrónico, etc.) se asignan dinámicamente de acuerdo a los recursos y las preferencias de los usuarios. Usando esta arquitectura, la lógica de la aplicación se centraliza, y cuando se necesita llama de forma dinámica a los otros componentes de los servicios distribuidos a lo largo de la red (servidor de conferencias, servidor de web, etc.). Se usan protocolos abiertos, tales como el HTTP para el transporte, el protocolo SOAP (*Simple Object Access Protocol*) para la invocación de servicios, el protocolo de transferencia de correo simple (SMTP) y SIP. Este modelo permite a los diseñadores de aplicaciones enfocarse en la aplicación del cliente cuando los componentes de los servicios están ya disponibles. Por este motivo sería posible construir nuevas y mejores aplicaciones más fácil y rápidamente y a un costo más bajo.

Los servicios típicos de SIP son el reenvío de la llamada a una página *web* o a un correo electrónico si la parte llamada está ocupada, la respuesta de voz interactiva vía *web* (presentación de una página *web* para mejorar la respuesta de voz), el enrutamiento personal de llamadas basado en la presencia, el seguimiento de usuario posibilitado por la posición del usuario (para movilidad de la parte llamada), y la asignación dinámica de

medios (voz, vídeo, correo electrónico, mensajería instantánea) basada en la presencia, en terminales disponibles y en las preferencias del usuario.

SIP incorpora también funciones de seguridad y autentificación, así como descripción del medio mediante SDP. Para el proceso de facturación (*billing*), SIP puede recurrir a RADIUS y RSVP.

#### 3.5.3.1 Mensajes SIP

Existen dos clases de mensajes SIP, peticiones (***requests***) y respuestas (***responses***). Los clientes emiten peticiones y los servidores responden con respuestas. Las peticiones y las respuestas usan un formato genérico de mensaje el cual consiste en una línea de inicio, uno o más campos de cabecera (para describir los detalles de la comunicación), una línea en blanco indicando el final de los campos de cabecera y un opcional cuerpo del mensaje.

Se han definido 6 métodos para los mensajes de *request*/*response*.

***Invite**:* Para invitar al usuario a realizar una conexión. Localiza e identifica al usuario.
***Bye**:* Para la terminación de una llamada entre usuarios.
***Options**:* Información de capacidades que pueden ser configuradas entre agentes o mediante un servidor SIP.
***ACK**:* Usado para reconocer que el mensaje *Invite* puede ser aceptado.
***Cancel**:* Termina una búsqueda de un usuario.
***Register**:* Emitido en un mensaje *multicast* para localizar al servidor SIP.
Existen 37 cabeceras, y pueden ser divididas en cuatro grupos diferentes de cabeceras: Generales, Entidad, Petición y Respuesta y seis clases de respuesta diferentes:

- *Informational:* Petición recibida, continúa el procesamiento de la petición.
- *Success:* La acción fue recibida con éxito, entendida y aceptada.
- *Redirection:* Necesarias acciones adicionales para completar la petición.
- *Client Error:* Error de sintaxis en la petición.
- *Server Error:* Fallo del servidor al resolver una petición aparentemente válida.
- *Global Failure:* La petición no puede ser resuelta en ningún servidor.

SIP es un protocolo del nivel de aplicación que no requiere el soporte de un protocolo de transporte seguro. A diferencia de lo que ocurre en HTTP y SMTP, SIP puede funcionar tanto sobre TCP como sobre UDP, incluso también sobre IPX, *Frame Relay*, ATM o X.25.

SIP soporta el mapeo de nombres y servicios de redireccionamiento, permitiendo la implementación de servicios ISDN y de Red Inteligente, que proporcionan al usuario una movilidad personal.

Las fases de comunicación soportadas en una conexión *unicast* son las siguientes:

***User location*:** Para determinar el sistema terminal para la comunicación.
***User capabilities*:** Para determinar los parámetros del medio a ser usados.
***User availability*:** Para determinar la disponibilidad del llamado para la comunicación.
***Call setup*:** (*ringing*) Para el establecimiento de la llamada entre ambos extremos.
***Call handling*:** Incluye la transferencia y terminación de la llamada.

Un sistema SIP posee únicamente dos componentes: agentes usuario (***user agents***) y servidores de red (***networks servers***). Un agente usuario es un sistema final que actúa en conducta de alguien que quiere participar en llamadas. En general, un agente usuario contiene ambos, un protocolo cliente, llamado agente usuario cliente (**UAC**, *User Agent Client*), usado para iniciar la llamada, y un protocolo servidor, llamado agente usuario servidor (**UAS**, *User Agent Server*) usado para responder la llamada.

Además de los agentes usuarios, SIP proporciona dos tipos diferentes de servidores de red: ***proxy server*** y ***redirect server***. Un *proxy server* SIP actúa prácticamente del mismo modo que un *proxy* HTTP, recibe una petición, determina a que servidor la debe enviar, y entonces redirige la petición, posiblemente tras la

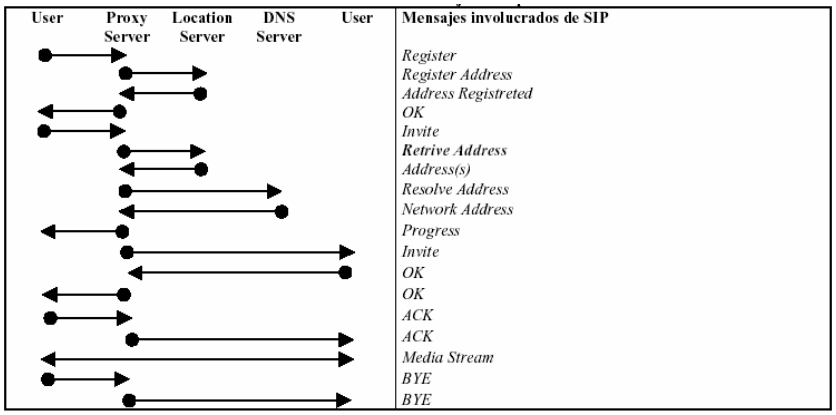
modificación de algunos de los campos de cabecera. Un *redirect server* recibe peticiones, pero en lugar de redirigirlas hacia el próximo servidor, éste dice al cliente que debe contactar al próximo servidor directamente.

### 3.5.3.2 Formatos de los Mensajes *Request* y *Response*

El encabezado de los mensajes *request* y *response* contienen los siguientes campos:

***Start Line**:* Usada para indicar el tipo de paquete, la dirección y la versión de SIP. Por ejemplo: <INVITE SP sip:mark@unam.mx SP SIP/2.0 CRLF>.
***General Header:*** Contiene las siguientes informaciones:
***-Call-ID**:* Se genera en cada llamada para identificar la misma. Contiene la dirección del dominio del *host*, por ejemplo: <CallID: 1876@imp.mx>.
***-Cseq:*** Por ejemplo: <Cseq: 1234 Invite>. Se inicia en un número aleatorio e identifica en forma secuencial a cada *request*.
***From**:* Por ejemplo <From: "MyName" <sip:myaccount@company.com>>. Se encuentra presente en todo mensaje *request* y *response*. Es la dirección del origen de la llamada.
***-To:*** Por ejemplo <To: "Helpdesk" <sip:helpdesk@company.com;tag=287447>>. Se encuentra presente en todo *request* y *response*. Es la dirección del destino de la llamada. El *tag* es usado cuando el mismo destino designa a varios puntos finales.
***-Via:*** Por ejemplo <Via:SIP/2.0/UDP PXY1.provider.com; received 10.0.03>. Sirve para recordar la ruta del *request*, por ello cada proxy en la ruta añade una línea de vía.
***-Encryption:*** Por ejemplo <Encryption: PGP versión=2.6.2, encoding=ascii>. Identifica un mensaje que ha sido encriptado para seguridad (proceso descrito en SDP).
***-Additionals:*** Además del encabezado general se pueden transportar campos adicionales. Por ejemplo: *Expire* indica el tiempo de valides del registro, *Priority* indica la prioridad del mensaje; etc.

A continuación se muestra un ejemplo de intercambio de mensajes de un sistema SIP:




*Intercambio de mensajes en el protocolo SIP.*

### 3.5.3.3 Ventajas de SIP

- **Simplicidad**: Es el más sencillo que H.323, posee únicamente 37 cabeceras mientras que H.323 define cientos de elementos y sus especificaciones son más extensas.
- **Extensibilidad**: Se ha construido un rico conjunto de funciones de extensibilidad y compatibilidad, además por defecto, las cabeceras y valores desconocidos son ignorados.
- **Neutralidad con Respecto al Protocolo de Transporte**: Puede apoyarse tanto en TCP como en UDP.
- **Integración con Otros Protocolos**: Buena integración con la *Web*, *e-mail*, aplicaciones y protocolos de flujo de datos, y otros servicios de red.
- **Servicios Avanzados**: Proporciona una gran facilidad para implementar servicios avanzados y de Red Inteligente.

### 3.6 La Calidad de VoIP

Proporcionar un nivel de la calidad que iguale por lo menos al de la RTPC se ve como un requisito básico para el éxito de VoIP, aunque algunos expertos argumentan que debería aplicarse una compensación entre costo, funcionalidad y calidad.

Aunque la calidad del servicio se refiere generalmente a la fidelidad de las transmisiones de voz y de los documentos, puede también ser aplicado a la disponibilidad de la red (es decir, capacidad de la llamada, o nivel de bloqueo de llamada), a la disponibilidad de las características del teléfono (conferencia, exhibición del número que llama, etc.), y a la escalabilidad (cualquiera a cualquiera, universal, extensibles).

La calidad de la reproducción de los sonidos sobre una red de teléfono es fundamentalmente subjetiva, aunque las medidas estandardizadas han sido desarrolladas por el ITU.

El mantenimiento de unos niveles aceptables en la calidad de la voz a pesar de las inevitables variaciones en el funcionamiento de la red (tales como congestión o fallos de conexión) se alcanza usando técnicas tales como la compresión, la supresión del silencio, y redes que permiten servicios de transporte con calidad (QoS).

#### 3.6.1 Factores que Afectan la Calidad de la Voz en VoIP

Las redes IP por naturaleza son redes del tipo *best effort* y por tanto no ofrecen garantía de QoS, pero las aplicaciones de VoIP necesitan algún tipo de garantía de **QoS** en términos de retardo, *jitter* y pérdida de paquetes. Por tanto, es necesario buscar QoS no solo en la red, sino también en las terminales, y en los procesos que en los mismos se desarrollan, la sensibilidad a la pérdida de paquetes, a las demoras y sus fluctuaciones, que experimentan los servicios de voz sobre IP, dependen en buena medida de los mecanismos implementados en las terminales.

Como se ha visto la preparación de los paquetes en las terminales para ser enviados y transferidos por la red IP involucra varios procesos: digitalización, compresión y empaquetado en el extremo emisor, y los procesos inversos en el extremo receptor. Todo esto se lleva a cabo mediante un complejo procesamiento que sigue determinado algoritmo, lo cual a su vez se desarrolla en cierto intervalo de tiempo, esto es, implica retardos de procesamiento y retardos de empaquetado. El resultado de esta codificación y paquetización incide directamente en la QoS, y también la forma en que se lleve a cabo. Así, cuando se reduce la velocidad de codificación los requerimientos de ancho de banda también se reducen, lo que hace posible poder manejar más conexiones simultáneas, pero se incrementa la demora y la distorsión de las señales de voz. Lo contrario ocurre al aumentar la velocidad de codificación.

Entre los factores que afectan a la calidad de la voz en un sistema de VoIP se encuentran los siguientes:

**Ancho de Banda:** La velocidad de transmisión de datos en la infraestructura de red es un factor que puede afectar la calidad de la voz en una red de VoIP, el principal problema ocurre cuando la capacidad de los enlaces es rebasada, provocando perdida de paquetes por el desbordamiento de datos y retardos producidos por el tiempo que tienen que esperar los paquetes para que puedan ser transmitidos, otro problema ocurre cuando la infraestructura tiene cuellos de botella, o enlaces de diferentes capacidades donde el flujo de datos que va desde un enlace atraviesa por otro de menor capacidad que esta expuesto a saturaciones por no contar con la capacidad para soportar todo el tráfico que pasa por el.

**Retardo o Latencia:** Se define como el tiempo que le toma a un paquete llegar de una terminal a otra, debido a los retardos acumulados. El primer retardo es producido por el proceso *store-and-forward* y el retardo de procesamiento (cambio de encabezado, etc). A esto se suman los retardos propios del proceso de compresión vocal. Los retardos en la red pueden ser reducidos mediante el protocolo de reservación RSVP, mientras que el retardo debido a la compresión vocal se puede eliminar usando un codec de voz de 64 kbps (sin compresión). Inicialmente VoIP se desarrolló para reducir costos mediante tasas de transmisión de datos más bajos que la tradicional de 64 Kbps y usando la infraestructura de Internet. Actualmente, con los modelos de

red IP de alta velocidad, la compresión vocal no es obligatoria. En este caso VoIP se desarrolla para brindar una red de servicios integrados soportada en protocolo IP.

Por ejemplo el tamaño de un paquete RTP que incluye 66 Bytes de encabezado (26 de MAC, 20 de IP, 8 de UDP y 12 de RTP) y 71 de carga útil, sin embargo su encabezado puede ser comprimido al usar el protocolo cRTP. También la información vocal puede ser reducida, por ejemplo mediante el codec G.723 que trabaja a 6.3 kbps (trama de 30 mseg), que sin supresión de silencios requiere 11 paquetes/seg y 71 Bytes/paquete. Si integramos la supresión de silencios esta velocidad se reduce sustancialmente. Un problema que resulta del retraso entre un extremo y otro de la red es la superposición de transmisiones. La superposición de transmisiones llega a ser significativo si la comunicación unidireccional se retrasa en más de 250 milisegundos.

**Jitter:** Se entiende como el efecto por el cual el retardo entre paquetes no es constante. Se trata de una latencia variable producida por la congestión de tráfico en el *backbone* de red, por distintos tiempos de tránsito de paquetes debido al funcionamiento *connectionless*. Para solucionar esto se puede utilizar un buffer para distribuir los paquetes y reducir el *jitter*, es decir, recoger los paquetes y guardarlos el tiempo suficiente para permitir que los paquetes más lentos lleguen en hora para ser tratados en la secuencia correcta, pero esto introduce un retardo adicional. Lo correcto seria incrementar el ancho de banda del enlace y hacer más eficiente el tráfico mediante políticas de calidad de servicio, solución posible en un *backbone* pero de menor posibilidad en los enlaces WAN.

**Eco:** La latencia y el *jitter* pueden producir eco sobre la señal telefónica, lo cual hace necesario el uso de canceladores de eco (**ITU-T G.168**). El cancelador de eco permite la transmisión simultánea *full dúplex*.
El eco se convierte en un problema cuando el trayecto ida vuelta se retrasa en más de 50 milisegundos, puesto que el eco se percibe como un problema significativo de la calidad, los sistemas de VoIP proporcionan mecanismos para cancelar el eco.

**Pérdida de Paquetes:** Las redes IP no pueden proporcionar una garantía que los paquetes serán entregados y mucho menos en el orden correcto. Los paquetes serán perdidos bajo cargas máximas y durante períodos de congestión (causada, por ejemplo, por faltas de acoplamiento o capacidad inadecuada). Debido a la sensibilidad del tiempo en las transmisiones de voz los esquemas normales de la retransmisión basados en TCP no son convenientes. Los enfoques usados para compensar la pérdida de paquetes incluyen la interpolación del habla retransmitiendo de nuevo el último paquete, y enviando información redundante. Las pérdidas de paquetes mayores al 10% son generalmente intolerables.

Otro aspecto a tener en cuenta es el compromiso entre el retardo de paquetización y la utilización del canal (relación entre bytes de información y bytes de cabecera en cada paquete de voz), es decir, la búsqueda de mayor utilización del canal conduce a mayor retardo de paquetización para cierto estándar de codificación. Según el estándar de codificación que se utilice será la demora resultante en relación con la utilización del canal, diferencias que se acentúan cuando la utilización del canal está por encima del 50 %, con un crecimiento de la demora en forma exponencial en el caso de los *codecs* de baja velocidad como el G.723. El retardo de paquetización también puede ser reducida mediante multiplexación de varias conexiones de voz en el mismo paquete IP.

### 3.6.2 Soluciones para Garantizar la Calidad de la Voz en Sistemas de VoIP

Hasta hace poco tiempo el ancho de banda necesario para la transmisión de voz y vídeo en tiempo real era considerablemente elevado, lo que hacia imposible este tipo de comunicaciones sobre redes de datos que no garantizaran una calidad de servicio, como por ejemplo Internet o redes basadas en protocolo *IP*. Actualmente la voz que recibe un *gateway* es digitalizada y comprimida según distintos algoritmos (GSM, G.723.1, G.711, G.729, etc) los cuales se caracterizan por conseguir mayores tasas de compresión en detrimento del tiempo de latencia (tiempo necesario para descomprimir la voz para que pueda ser entendida de nuevo). Algunos de estos algoritmos consiguen comprimir los paquetes de voz en 8 Kbps aproximadamente. El protocolo **IP** añade al paquete de voz digitalizado y comprimido una serie de cabeceras para su correcto transporte a través de la red, lo que hace que el ancho de banda necesario se incremente hasta unos 16 Kbps.

Hay que considerar así mismo el parámetro denominado supresión de silencio. 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 esto, se puede afirmar que el tamaño medio de un paquete de voz durante una conversación es de 8 Kbps. Esto viene a demostrar que las necesidades de ancho de banda para este tipo de aplicaciones están al alcance de prácticamente cualquier empresa.

A continuación se mencionan algunas herramientas que se pueden usar para disminuir los efectos de los factores que degradan la calidad de la voz y de aplicaciones de tiempo real transmitidas en redes IP:

**Supresión de Silencios y Detección de Voz *VAD*** (*Voice Activity Detection*): Establecer diferencia entre habla y silencio, no transmitir paquetes de silencio y generación de silencios al otro extremo.

**Compresión de Cabeceras:** Mediante *RTP/ RTCP*, se comprimen las cabeceras sin resolver reserva de recursos o calidad de servicio garantizada. RTCP proporciona realimentación sobre la calidad

**Reserva de Ancho de Banda:** RSVP incorpora reserva de ancho de banda y retardo además de establecer una lista de acceso dinámica de extremo a extremo.

**Priorizar:** existen diferentes tendencias tales como:

- ***CQ*** (*Custom Queuing*): Asignación de un porcentaje del ancho de banda disponible
- ***PQ*** (*Priority Queuing*): Establecimiento de prioridad en las colas
- ***WFQ*** (*Weight Fair Queuing*): Asignación de prioridad al tráfico de menos carga.
- ***DiffSer****v*: Que evita tablas en *routers* intermedios y establece decisiones de rutas por paquete.

**Control de Congestión:** Uso del protocolo ***RED*** (*Random Early Discard*) que es una técnica que permite descartes aleatorios y que disminuye la perdida de paquetes de VoIP.

***IPv6***: La utilización de esta versión del protocolo IP brinda un mayor espacio de direccionamiento y la posibilidad de utilizar *Ipv6 & Tunneling*, que permitiría facilitar el proceso de enrutamiento del tráfico y disminuir la latencia de la paquetes.

La calidad de la voz y de los servicios de VoIP, están determinadas principalmente por la infraestructura de la red IP, de tal modo que si no se tienen implementadas políticas de QoS consistentes a lo largo de toda la red IP, no se podrá aspirar a alcanzar los niveles de satisfacción para el usuario que brindan actualmente la redes telefónicas tradicionales.

# Capitulo 4

# Implementación de VoIP y Aplicaciones para la Industria Petrolera

## 4.1 Guía de Implementación

La implementación de VoIP es una excelente opción para satisfacer las crecientes demandas de productividad de la industria petrolera, ya que esta tecnología provee de poderosas herramientas de comunicación que permitirán a los usuarios estar comunicados de una manera más efectiva y oportuna, sin importar en que parte del mundo se localicen. Esta tecnología permitirá que los usuarios colaboren en la toma de decisiones o en la elaboración de proyectos de una manera remota, con aplicaciones de videoconferencias, con aplicaciones para compartir información y documentos, y otras aplicaciones que definitivamente impactaran en la productividad de los empleados al ahorrar tiempo, dinero y esfuerzo al evitar la necesidad de viajar para solucionar ciertos problemas.

En la mayoría de los casos la implementación de esta tecnología es posible mediante cambios menores en la estructura de la red de datos existente, que es el caso de una implementación pura de VoIP y que es la que más ventajas brinda, mientras que en otros casos será necesario integrar algunos elementos a las redes de datos y telefónica, lo que implica una implementación híbrida, que permite que los usuarios de la tecnología de conmutación de circuitos del sistema telefónico tradicional puedan intercomunicarse con los usuarios de telefonía IP de una manera transparente o sin que perciban que tipo de tecnología están usando.

La implementación de una red de VoIP ocurre en dos niveles, que se escalonan secuencialmente durante la planificación y la implementación, el primero se lleva a cabo en la infraestructura y el segundo en las aplicaciones. Preparar la infraestructura de red para el tráfico en tiempo real, como la voz, es el primer paso para la implementación exitosa de aplicaciones multimedia, esta etapa se refiere básicamente a asegurar el transporte de VoIP, tanto en la red de datos como en la RTC (Red Telefónica Conmutada), de tal manera que los usuarios tengan servicios de voz dentro y fuera de la red de VoIP. La segunda etapa mencionada se refiere a la integración de teléfonos IP, aplicaciones de voz para computadoras y aplicaciones basadas en red que integran voz y datos. Las dos etapas pueden llevarse a cabo simultáneamente, pero **la preparación de la infraestructura es la clave del proceso de planeación para asegurar la implementación exitosa** de las aplicaciones.

Esta guía de implementación esta basada en las recomendaciones de expertos de las compañías Cisco y Nortel Networks, que son los fabricantes más importantes de equipo de redes y de telefonía IP, esta revisa los aspectos que deben ser considerados para evolucionar una red exclusiva de datos hacia una infraestructura de red multiservicio que pueda incluir tráfico de datos, voz y video o la integración de las redes de datos y telefónica. Los pasos recomendados para la planeación de una infraestructura multiservicio son los siguientes:

1. Revisión de la infraestructura de red disponible
2. Establecimiento de los objetivos para la red
3. Revisión de la tecnología y servicios
4. Diseño técnico y planeación de capacidad
5. Análisis financiero
6. Implementación y pruebas

Este enfoque comienza con una evaluación de la red actual, entonces se fijan objetivos y metas, se evalúan las tecnologías disponibles, se hacen las consideraciones de diseño técnico para el soporte de comunicaciones en

tiempo real, se realiza un análisis financiero y por último se realiza la planificación para la implementación y pruebas del sistema.

### 4.1.1 Revisión de la Infraestructura de Red Disponible

El primer paso en el diseño de una red VoIP es realizar un inventario y evaluación del equipo existente en la red de datos y en la red telefónica. Se debe revisar el equipo existente y evaluar sus capacidades y costos de operación y averiguar cuales son los servicios y aplicaciones con que se cuenta actualmente. Se deben identificar las aplicaciones multimedia y nuevos servicios que serian necesarios para mantener o aumentar la productividad y satisfacción de los usuarios, y determinar el impacto que tendrían de estos nuevos servicios y aplicaciones en la red (retardo, consumo de ancho de banda, etc.) tanto como sea posible.

Se deben determinar la calidad de los servicios de voz y de datos que perciben los usuarios y las áreas que necesitan mejorarse, la implantación de esta tecnología supone varias ventajas para los usuarios y administradores de la red, de tal manera que las ventajas y beneficios de la nueva red integrada deberán ser mayores y considerablemente apreciables, por lo tanto hay que buscar brindarle a los usuarios mejores servicios y aplicaciones que las que les podrían brindar las redes de datos y voz por separado.

Un estudio de tráfico podría ser necesario para observar los patrones actuales de tráfico de voz y datos, determinar que aplicaciones y protocolos utilizan la red y sobre todo determinar los requerimientos de ancho de banda de la red. A raíz de este estudio posiblemente algunos enlaces en la red pueden ser aumentados o disminuidos para cubrir adecuadamente las necesidades de ancho de banda.

Se deben revisar las políticas acerca de que tipo de tráfico (aplicaciones) en la red deben tener prioridad, es decir, las aplicaciones que son criticas, como podrían ser los sistemas de producción, y que ancho de banda será asignado a cada una de estas aplicaciones, además también es importante definir que tipo de tráfico no es permitido.

El resultado de este análisis es la base para determinar las técnicas de calidad de servicio QoS que serán implementadas en la red para asegurar ciertos tipos de tráfico, como la voz y las aplicaciones prioritarias.

### 4.1.2 Establecimiento de los Objetivos para la Red

Una vez que se conoce el tráfico y el uso actual de la red, el siguiente paso es establecer los objetivos de la red integrada. Primero se deben determinar los tipos de tráfico dominantes que serán soportados por la red integrada, y el nivel de servicio que se espera proporcionar a los usuarios. También considerar que tanto se relacionarán las aplicaciones de voz con las de datos, estas estimaciones ayudaran en la selección de la tecnología apropiada. Los objetivos de calidad de voz determinarán los límites para la compresión y el retardo aceptable para la red.

Es necesario determinar cuales son las razones por las cuales se requiere migrar a VoIP y dar prioridades a dichas razones, esto permite asegurar que se cumplan los objetivos, en la medida de lo posible, cuando se selecciona el equipo y se toman decisiones de diseño, entre las razones para migrar a una red multiservicio integrada están las siguientes:

- Implementación de nuevas aplicaciones: Para aumentar la eficiencia y productividad por ejemplo.
- Ahorro de costos: En la administración de la red, en mantenimiento de equipo, eficiencia del ancho de banda, llamadas de larga distancia.
- Incremento de competitividad: Mediante herramientas que permitan la realización de negocios de una manera remota con proveedores, socios y clientes, ofreciendo nuevos servicios y productos que mejoren las relaciones con los clientes.

Lo que sigue es determinar los requerimientos técnicos de la red de VoIP, se debe determinar si es necesario que un equipo de VoIP se pueda comunicar con todos los demás equipos de la red, incluso los de la red telefónica conmutada, o si solo es necesaria la comunicación entre equipos de VoIP (para los jefes por ejemplo), es decir que hay que determinar que equipos se van a comunicar con cuales. También es importante

saber si se va a transportar información de fax, por ejemplo, o cualquier otro servicio que sea comúnmente brindado por las redes telefónicas, como son los servicios suplementarios, también hay que determinar si el plan de marcación se mantendrá igual o si será cambiado, todo esto para poder seleccionar el equipo adecuado y necesario.

### 4.1.3 Revisión de la Tecnología y Servicios

El tercer paso evalúa la tecnología disponible en el mercado así como los servicios que se pueden brindar con dicha tecnología con la finalidad de alcanzar los objetivos previamente fijados.

Existen otras alternativas a VoIP, como lo son VoFR (*Voice over Frame Relay*) y VoATM (*Voice over* ATM) que son tecnologías de capa 2 del modelo OSI, VoIP es una tecnología de capa 3 y por lo tanto puede ser transportada por tecnologías de capa 2 como FR y ATM. VoIP se prefiere sobre VoFR y VoATM por su capacidad de interconexión con otras aplicaciones de voz o multimedia. VoFR y VoATM son buenas tecnologías de transporte a nivel WAN, usualmente manejan un mayor ancho de banda que VoIP pero tienen la desventaja de que no pueden ser implementadas sobre redes LAN o hasta el usuario final, es por esto que VoIP es la forma de voz sobre paquetes que predomina actualmente y es la única opción cuando se requiere una implementación híbrida (interconexión con PBXs).

Como se vio en el capitulo 3 VoIP aprovecha la infraestructura de las Intranets y de Internet, sobre todo la capacidad de enrutamiento, por lo que el diseño para que un usuario de VoIP se pueda comunicar con otro usuario de VoIP es muy sencillo.

El estándar H.323 ha estado disponible por varios años y es el más ampliamente implementado actualmente, mientras que los estándares emergentes para VoIP como MGCP y SIP se están convirtiendo en opciones tecnológicas validas. Como se explica en el capitulo 3, H.323 y SIP siguen un modelo distribuido donde los *gateways* cuentan con suficiente inteligencia para manejar los proceso básicos de una llamada sin la asistencia de otro elemento de red. Si se requieren otras características o servicios de valor agregado como servicios suplementarios se añaden elementos de red (servidores de servicios) llamados *gatekeepers* para H.323 y SIP *proxies* para SIP. MGCP utiliza un modelo centralizado donde hay un servidor central que sirve de agente de llamadas que contiene todas las funciones de procesamiento de llamadas.

Cuando se considera una red multiservicio, se debe hacer una evaluación de las tecnologías WAN, IP es una tecnología no orientada a conexión (ver capitulo 2), por lo que tiene que usar protocolos de capas superiores como UDP y TCP para habilitar sesiones a través de la red, incluyendo llamadas de voz, el protocolo RTP se utiliza para aplicaciones de tiempo real como VoIP. IP tiene un sistema de señalización robusto, funcionalidades de enrutamiento, se integra bien con las aplicaciones actuales de datos y el es el protocolo de red más usado. IP funciona en todas las plataformas por su gran flexibilidad para soportar nuevas aplicaciones. IP tiene la gran ventaja de que puede ser transportado por una gran cantidad de tecnologías de transporte como Ethernet, SDH, ATM, etc. Es importante realizar un análisis de las ventajas y desventajas que implica el uso de alguna de estas tecnología, en el capitulo uno se hace una revisión de PDH, SDH y ATM que son algunas de las tecnologías que se usan en PEMEX, algunas características de ATM, por ejemplo, pueden ser usadas para lograr un mejor desempeño de VoIP. Por ejemplo, ATM fue diseñado para manejar tráfico que es sensitivo al tiempo, como la voz, y es una tecnología orientada a conexión. Usa celdas de tamaño fijo (en lugar de *frames* de tamaño variable), la función de conmutación de ATM esta optimizada para un desempeño de alta velocidad, permitiendo construir conexiones basadas en criterios de retardo y variación de retardo.

Otro aspecto tecnológico importante es como se van a interconectar las PBXs existentes, o como se va a interconectar la red telefónica convencional con la nueva red integrada, es importante asegurar que los *gateways* soporten una amplia variedad de protocolos de señalización que permitan una mayor flexibilidad en la elección de equipo, otro aspecto importante a considerar en la elección de un *gateway* es que sus interfaces sean las adecuadas para su conexión a la red telefónica conmutada.

### 4.1.4 Diseño Técnico y Planeación de la Capacidad

#### 4.1.4.1 Diseño Técnico

Como se vio en el capitulo 3, es necesario utilizar un proceso de codificación para digitalizar la voz de una llamada telefónica para poder transmitirla en un sistema digital de comunicación, VoIP en este caso, además de que es posible utilizar un método de compresión de voz para reducir la cantidad de información digital, debajo de la tradicional tasa de 64 kbps, para hacer un uso más efectivo del ancho de banda. Los avances en la tecnología han mejorado considerablemente la calidad de la voz comprimida y ha resultado en un conjunto de estándares de la ITU (serie G) para los algoritmos de compresión, los más importantes se muestran a continuación.

| Compression Method | ITU Standard | Payload Bandwidth | MOS Score | Delay |
|---|---|---|---|---|
| PCM | G.711 | 64-kbps | 4.1 | 0.75 ms |
| MP-MLQ/ACELP | G.723.1 | 6.3-kbps/5.3-kbps | 3.8/3.75 | 30 ms |
| ADPCM | G.726 | 32-kbps | 3.85 | 1 ms |
| LD-CELP | G.728 | 16-kbps | 3.61 | 3 to 5 ms |
| CS-ACELP | G.729 | 8-kbps | 3.9 | 10 ms |
| CS-ACELP | G.729a | 8-kbps | 3.85 | 10 ms |

*Algoritmos de Codificación más Importantes*

Cuando se usa alguna técnica de compresión, se obtiene un ahorro en el ancho de banda, pero a su vez se tiene una reducción en el nivel de la calidad de la voz. La elección del *codec* (*coder-decoder*) adecuado para la red VoIP depende en parte de la calidad de voz que se este dispuesto a sacrificar con la finalidad de mejorar la eficiencia del ancho de banda, de tal manera que se tenga una calidad de voz aceptable para los usuarios. Por ejemplo el estándar G.729 requiere un ancho de banda 8 veces menor que el estándar G.711, aunque también hay una reducción en la calidad percibida de la voz de 4.1 a 3.9 (ver tabla), una perdida aceptable considerando el ahorro de ancho de banda. G.729 es el *codec* predominante que se usa para transportar voz sobre redes WAN, mientras que G.711 o G.726/32 son frecuentemente usados en redes LAN donde la eficiencia del ancho de banda no es tan crítica.

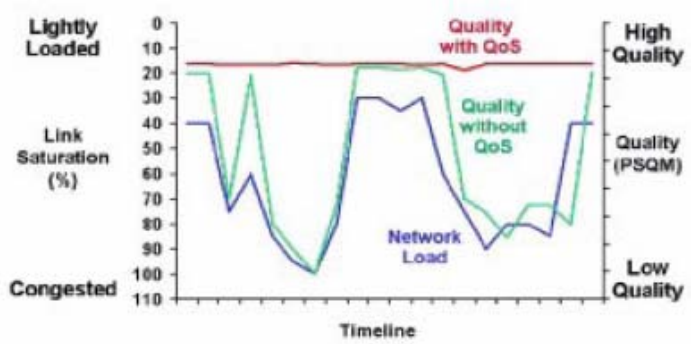
MOS (*Mean Opinion Score*) es una medida subjetiva de la calidad de la voz. Una señal de voz con una puntuación de 4 a 5 es considerada de muy buena calidad, una con una puntuación de 3 a 4 se dice que es adecuada para la comunicación, mientras que una señal de voz con una puntuación menor que 3 se considera que tiene una calidad sintética o que ha perdido algunas características básicas y que se escucha robotizada. La tabla anterior muestra la puntuación MOS de una muestra para los *codecs* más comúnmente usados. La puntuación MOS no es un estándar, se basa en el resultado de estudios individuales y la puntuación de un *codec* particular puede variar dependiendo de si el usuario es hombre o mujer y del idioma que se use en el estudio. Últimamente se ha empezado a utilizar un nuevo método para medir la calidad de la voz, el PSQM (*Perceptual Speech Quality Measurement*)

El otro aspecto a considerar en la elección del *codec*, es el retardo (*delay*) que se introduce al usarlo, en la tabla se muestran lo retardos que producen los *codecs* más comunes, a una mayor compresión introduce un mayor retardo. En el diseño de la red estos factores deben ser balanceados para asegurar la calidad de la voz.

La calidad de la voz en una red de paquetes es afectada por más factores que la elección del *codec*, como se indica en el capitulo 3, el retardo, la variación del retardo (*jitter*), el eco y la perdida de paquetes afectan considerablemente la calidad de la voz.

El estándar G.165 es usado para eliminar el eco, para minimizar los efectos del retardo se utilizan varias técnicas de QoS (ver capitulo 2), mientras que para compensar la perdida de paquetes se diseñan las redes para descartar paquetes de una manera selectiva cuando ocurre una situación de congestión.

La siguiente gráfica muestra como se deteriora la calidad de la voz cuando se incrementa la carga de la red que no tiene implementadas técnicas de QoS, y como se puede mantener la calidad de la voz independientemente de la carga de una red que tiene implementadas técnicas de QoS.




*Calidad de Servicio v.s. Mejor Esfuerzo*

La grafica muestra que si se implementan políticas de QoS en la red integrada, las llamadas de voz pueden tener una calidad comparable a las de la red telefónica tradicional con la tecnología actual.

Los mecanismos de QoS son más efectivos sobre enlaces *full-duplex*, en enlaces punto a punto y enlaces WAN donde solo un dispositivo en cada lado del enlace hace uso de dicho enlace, como *switches* ATM por ejemplo, los puntos críticos para la implementación efectiva de QoS son:

- Que haya un medio de transmisión separado en cada dirección del enlace serial.
- Que los dispositivos tengan un control total sobre los datos que envían
- Que no haya otros dispositivos que puedan interferir con la transmisión

Un ejemplo de dispositivos que soporta una operación *full-duplex* son los *switches* Ethernet mientras que los *hubs* no lo hacen y no pueden proporcionar QoS.

La QoS no puede ser garantizada en enlaces que comparten el medio físico con otros dispositivos, ya que dichos dispositivos pueden consumir ancho de banda de otro dispositivo que este tratando de implementar QoS. Sin embargo esto no significa que el medio de transmisión para VoIP tenga que ser *full-duplex* de punto a punto para funcionar adecuadamente, los puntos críticos son aquellos enlaces que transportan una mayor cantidad de tráfico, y que es donde se puede generar la mayor parte de los problemas.

Como se explica en el capitulo 3 los retardos pueden producir efectos indeseables en las llamadas de VoIP. Los retardos debajo de 150 ms son considerados aceptables para la mayoría de las aplicaciones de voz en tiempo real, retardos entre 150 y 400 ms son aceptables solo bajo ciertas condiciones, en llamadas de muy larga distancia por ejemplo.

Generalmente **las redes de voz deben ser diseñadas** para tener **retardos menores de 150 ms**, hay que considerar en el diseño que el retardo esta formado por el retardo de propagación, el retardo de serialización y el retardo de procesamiento. (Ver capitulo 3)

Algunos de estos componentes se pueden controlar durante el diseño de la red, el retardo de serialización puede ser ajustado modificando el tamaño de los paquetes o implementando técnicas de QoS de fragmentación de paquetes. La elección de los *codecs* repercute en el retardo de procesamiento, el retardo de paquetización es configurable en algunos *gateways* y puede ser ajustado en base en las características de la red.

Hay dos tipos de pérdida de paquetes con los que hay que lidiar en un entorno VoIP, el primero es el de los paquetes que se pierden en la red, *frames* con errores o corrompidos durante fallas o paquetes descartados por *routers* bajo condiciones de congestión, el segundo tipo se debe a problemas en la variación del retardo (*jitter*)

y son los paquetes que llegan a su destino, pero que llegan tarde para ser usados por lo que tienen que ser desechados, de acuerdo al comportamiento de la red se debe configurar el buffer del *jitter*, que almacena los paquetes que van llegando para entregarlos después a una tasa de retardo constante, la utilización de estos dispositivos más la utilización adecuada de técnicas de QoS pueden reducir considerablemente las pérdidas de paquetes para VoIP.

**Otro aspecto importante para la implementación de VoIP es asegurar que la red este libre de averías que puedan degradar la calidad de la voz, esto puede incluir la configuración incorrecta de equipo y problemas con enlaces dañados.**

Se recomienda la operación *full-duplex* en los enlaces de la red cuando sea posible, es altamente recomendable usar *switches*, en lugar de *hubs*, para conectar dispositivos que solo son capaces de funcionar en modo *half-duplex*, para reducir los dominios de colisión. Los principales problemas en la LAN ocurren cuando los equipos funcionan entre si en un modo diferente, uno en *full-duplex* y el otro en *half-duplex*, provocando una perdida aleatoria de paquetes. Los *switches* tienen la capacidad de detectar el modo de funcionamiento y velocidad de cada dispositivo que esta conectado a el y de manera automática ajustar los parámetros del puerto al que esta conectado dicho dispositivo, sin embargo en algunos casos esto no ocurre, por lo que es necesario hacer un ajuste manual en el *switch* en estos casos.

Para evitar este tipo de problemas en la red LAN se recomienda lo siguiente:

- La utilización de *switches* desde el nivel de acceso hasta el de *backbone*.
- El uso de *switches* con capacidad para brindar QoS
- El uso del modo *full-duplex* en todas partes
- Configurar los puertos de los *switches* para que negocien automáticamente la velocidad de funcionamiento y resolver los problemas que pudieran surgir caso por caso
- Utilización de cableado estructurado categoría 5E o superior.
- Asegurarse de que la longitud de los cables no exceda las especificaciones correspondientes.

En el caso de enlaces WAN, algunos bits erróneos provocan la perdida de paquetes, por la naturaleza de su funcionamiento que remueve los paquetes dañados tan pronto son detectados, es importante que estos enlaces funcionen tan claramente como se posible, ya que para la aplicaciones de tiempo real no hay tiempo para reponerse de *frames* dañados o perdidos. Problemas de sincronía producen la pérdida de paquetes en intervalos de tiempo regulares, esto típicamente sucede cuando uno o más dispositivos funcionan con sus propios relojes internos en lugar de hacerlo con una base de tiempo común.

Las recomendaciones generales para enlaces WAN son las siguientes:

- Asegurarse de que hay suficiente ancho de banda para transportar todo el tráfico.
- Monitoreo de la utilización de los enlaces para solucionar posibles problemas de congestión.
- Implementación de estrategias de QoS.
- Implementación de fragmentación de paquetes e intercalado de paquetes para enlaces con una capacidad inferior a 1024 kbps.
- Asegurarse de tener una baja tasa de error de bits en el enlace.
- Asegurarse de que no hay problemas de sincronización de relojes

Para que el *gateway* de voz pueda conmutar o enrutar una llamada en cualquier punto de la red es necesario que el *gateway* entienda los dígitos marcados y, para el caso de un teléfono IP, trasladar el número marcado a una dirección IP, para lograr esto es necesario implementar un plan de marcación en el *gateway* de voz, de una manera similar a como se hace en los PBXs.

Se deben considerar varios factores para asegurar que haya una transición suave entre el antiguo y el nuevo plan de marcación, que permita una red manejable. Se tiene que considerar si se requiere que el plan de marcación permanezca igual desde la perspectiva de los usuarios o si es necesario introducir alguna clave o código de acceso para pasar una llamada de voz por la red IP o por la red conmutada, también hay que

considerar en el plan si se tendrá acceso a la red telefónica publica conmutada (RTPC), para que el *gateway* pueda trasladar el número marcado a un número que pueda entender la RTPC. Los *gateways* usualmente ofrecen varias herramientas para manipular los números de tal manera que puedan ser adaptados al plan de marcación de un país o a redes telefónicas privadas.

#### 4.1.4.2 Planeación de la Capacidad

Para realizar la planeación de la capacidad de la red telefónica híbrida, es necesario determinar el número de canales de voz que se necesitaran para transportar las llamadas de voz desde el PBX hasta la red integrada multiservicio, después el número de canales telefónicos se trasladan al ancho de banda necesario para transportar esas llamadas en la red VoIP. El número correcto de canales de voz necesarios usualmente se calcula mediante el volumen de tráfico, el factor de bloqueo y otros valores estadísticos.

En otros casos en que se tienen implementaciones puras de VoIP, lo que se hace es calcular el ancho de banda necesario para el transporte de las llamadas, el cálculo del ancho de banda debe tomar en cuenta el tipo de compresión usada (*codec*), el *overhead* y la utilización. Estos varían dependiendo de la tecnología de transporte utilizada.

En este caso el cálculo del ancho de banda no es tan simple como el caso de la red telefónica, donde esencialmente se tiene un ancho de banda de 64 kbps por llamada, o menos si se usa algún *codec*, en una red VoIP este cálculo es más complejo principalmente por la forma en que opera la pila de protocolos en una red de datos, cada capa (protocolo) tiene una función especifica y se comunica con la capa correspondiente de otros elementos de red, para esto se agrega información de encabezado (*overhead*) a cada unidad de datos y conforme van pasando los paquetes de las capas superiores a las inferiores se tiene un mayor *overhead*, ya que cada protocolo agrega sus propios encabezados, entonces para realizar el cálculo del ancho de banda necesario para el transporte de llamadas de VoIP se tienen que considerar principalmente el *overhead* que introducen los protocolos que se usan para una aplicación, así como el *codec* usado, que es el que determina el tamaño de la carga útil (voz).

Para VoIP los protocolos más relevantes son RTP, UDP, IP y el protocolo de acceso al medio, Ethernet por ejemplo. Las llamadas de voz son aplicaciones *full-duplex*, así que el cálculo de ancho de banda se tiene que hacer en cada dirección, para ello necesitamos saber algunos datos:

N: Cuantas llamadas serán soportadas por la red
P: El número de paquetes (o *frames*) que serán generados por segundo (pkt/s):

$$P = \frac{1000(ms/s)}{pr(ms/muestra)} * 1(pkt/muestra)$$

Donde **pr** (*packetization rate*) es la tasa de paquetización o tiempo que se necesita para generar un paquete expresado en ms. Por ejemplo para el **pr** usual de 20 ms se generan 50 paquetes por segundo (P=50 pkt/s).

V: La carga de voz de cada paquete expresada en Bytes por paquete (B/pkt), esta en función del *codec* utilizado:

$$V = \frac{codec(b/s)/8(b/B)}{P(pkt/s)}$$

Por ejemplo para el codec G.729 (8000 b/s) se tiene una V=20 (B/pkt)

**I**: El *overhead* introducido por los protocolos IP, UDP y RTP que es una constante al menos que se use RTP con compresión de cabeceras.

**I**=(IP+UDP+RTP)(B/pkt)=(20+8+12)(B/pkt)=40(B/pkt)

**L**: El *overhead* producido por el protocolo de la capa de enlace, hay que considerar que, por ejemplo, para Ethernet 802.11 se tienen varias versiones y campos que son opcionales, por lo que se tienen diferentes *overheads* para cada versión y configuración.

La demanda de ancho de banda por llamada para un enlace específico esta definido por la siguiente formula:

**Bw** (b/s) =(V+I+L)(B/pkt)*8(b/B)*P(pkt/s)

La demanda total del ancho de banda para un enlace específico esta definido por:

**TBw** (b/s)=Bw(b/s/llamada)*N(llamadas)

Esto indica el ancho de banda que requiere VoIP, aunque en algunos casos se deben hacer algunas otras consideraciones, como en los siguientes casos.

El tráfico de señalización usualmente no es un problema ya que el ancho de banda que demanda es mucho menor que el que requiere el tráfico de voz, el protocolo de control RTPC típicamente se usa en paralelo con RTP, el tráfico RTCP se supone limitado al 5 % del ancho de banda del tráfico de voz.

Se pueden usar técnicas y protocolos para hacer más eficiente el ancho de banda, como el uso de RTP con compresión de encabezados (ver capitulo 2) y detectores de actividad de voz VAD (*Voice Activity Detection*) o supresores de silencios que impiden que los paquetes de una llamada de VoIP que no contienen voz (silencios) sean transmitidos (ver capitulo 3), esto usualmente representa entre un 30 y 40 % de ahorro en el ancho de banda utilizado. En una red VoIP, el ancho de banda solo es utilizado cuando se están realizando llamadas, cuando no se realizan llamadas el ancho de banda puede ser utilizado por las aplicaciones de datos.

Como una regla general **se recomienda que en el diseño de la capacidad de la red VoIP no se exceda el 80% de la capacidad en un enlace serial**, esto se debe a situaciones como las que a continuación se describen. Es por la existencia de *overheads* invisibles y problemas de sincronización que no se diseña considerando los valores teóricos máximos de la capacidad de los enlaces, se diseña considerando un 80 % de esa capacidad.

Para el estándar 802.3 es de suma importancia saber cuando empieza y cuando termina un *frame*, para ello es necesario un espacio muerto entre *frames* con una duración de 12 bytes, además se utiliza un preámbulo de 8 bytes para avisar a otros equipos que un equipo esta a punto de transmitir y para que sincronicen sus relojes, esto representa un *overhead* oculto, en sistemas que funcionan con 802.3 *half-duplex* el problema son las colisiones, ya que el tiempo que tienen que esperar los equipos para poder transmitir una vez que ocurre una colisión y las retransmisiones también consumen un ancho de banda del enlace.

En enlaces WAN basados en HDLC, como PPP y Frame Relay, usan caracteres especiales (01111110) para indicar el comienzo y el final de un *frame*. Si una o más secuencias de bits (01111110) ocurrieran dentro del *frame*, el receptor creería que se trata del final de *frame*, trataría de calcular el CRC, detectaría un error y desecharía el *frame*, por lo que este *frame* nunca podría ser transmitido. La técnica ZBS (*Zero Bit Stuffing*) resuelve este problema insertando un 0 en la secuencia de bits cuando 5 bits 1 son detectados, el receptor remueve los ceros agregados y reconstruye los datos cuando no ve una bandera, en el peor de los casos se agregaría un 0 cada cinco bits de datos enviados, lo que representaría aproximadamente un 17 % de *overhead* invisible, lo cual consumiría el mismo porcentaje de la capacidad de un enlace serial.

Es importante diseñar la red de tal manera que las llamadas que no puedan ser atendidas en un cierto momento por la red VoIP, por falta de ancho de banda, sean redireccionadas a la red telefónica conmutada, es decir que se tiene que implementar un control de admisión de llamadas.

Las recomendaciones de diseño técnico se pueden resumir como sigue:

- Implementación de técnicas de QoS para minimizar varios componentes del retardo.

- Balanceo entre la calidad de la voz, el retardo y el ancho de banda.
- Determinación del retardo aceptable
- Cálculo del retardo y ajuste de los parámetros para mantener el retardo y el *jitter* por debajo del umbral permitido.
- Hacer las consideraciones pertinentes para el plan de marcación
- Planificación de la capacidad y ancho de banda requerido para el tráfico esperado en la red e implementación de técnicas de control de admisión de llamadas.

### 4.1.5 Análisis Financiero

Una vez que se han determinado las características que debe cumplir el nuevo equipo, es necesario realizar un análisis financiero para determinar cual opción resulta más favorable para la empresa. En la elección del equipo se debe buscar proteger la inversión en los equipos y sistemas existentes. También es posible realizar un estudio para indicarle al cliente en cuanto tiempo se amortizara la inversión realizada en la implementación de la nueva tecnología, y para indicar los ahorros que se podrían tener con este nuevo sistema por conceptos de la simplificación de la administración de la nueva red integrada así como por la reducción de los gastos de administración.

### 4.1.6 Implementación y Pruebas

Al momento de la implementación de VoIP es importante que las aplicaciones de comunicación actuales no sean interrumpidas, o lo sean el menor tiempo posible, cuando se incorporan los nuevos equipos, tales como *gateways* y controladores de llamadas, por esto, si es posible, es recomendable realizar una implementación de prueba con un número pequeño de usuarios que puedan reportar la calidad de voz que reciben, para que se puedan hacer los ajustes necesarios. Una vez instalado todo el sistema es conveniente realizar otro análisis de tráfico para detectar posibles cuellos de botella o para hacer los ajustes necesarios en los anchos de banda de los enlaces o en el *codec* utilizado.

## 4.2 Aplicación Práctica de VoIP en la Industria Petrolera

A continuación se presenta un ejemplo de cómo se podría implementar VoIP en algunas instalaciones de PEMEX. El presente ejemplo es hipotético, aunque puede servir de referencia en una futura implementación de esta tecnología.

PEMEX opera por conducto de un corporativo y cuatro organismos subsidiarios: Pemex Exploración y Producción, Pemex Refinación, Pemex Gas y Petroquímica Básica y Pemex Petroquímica. **Petróleos Mexicanos** es el responsable de la conducción central y de la dirección estratégica de la industria petrolera estatal, **Pemex Exploración y Producción** tiene a su cargo la exploración y explotación del petróleo y el gas natural, **Pemex Refinación** produce, distribuye y comercializa combustibles y demás productos petrolíferos, **Pemex Gas y Petroquímica Básica** procesa el gas natural y los líquidos del gas natural; distribuye y comercializa gas natural y gas LP; y produce y comercializa productos petroquímicos básicos, **Pemex Petroquímica** a través de sus siete empresas filiales elabora, distribuye y comercializa una amplia gama de productos petroquímicos secundarios.

Cada organismo tiene necesidades particulares de servicios de telecomunicaciones, por lo que los sistemas de comunicaciones se diseñan e implementan de acuerdo a las necesidades de cada instalación, cada sistema está sujeto a una serie normas que dependen del tipo de instalación, de las condiciones ambientales y de las condiciones de riesgo (clasificación de áreas peligrosas), por lo cual se tienen sistemas diferentes.

PEMEX cuenta con un sistema de telecomunicaciones complejo y muy grande, que abarca prácticamente todo el país, que le permite desplegar diversas aplicaciones de telecomunicaciones de una manera independiente y confiable, la red de comunicaciones de PEMEX es la segunda más grande de todo el país y esta basada en varias tecnologías de transporte como son SDH, PDH y ATM a nivel WAN (ver capitulo 1) que utilizan diversos medios de transmisión como fibra óptica, enlaces de microondas y de radio, y enlaces satelitales. En lo que respecta a nivel LAN sus instalaciones se basan en el estándar IEEE 802.3 (Ethernet) que utilizan cableado estructurado, e infraestructura y equipo especial en zonas de alto peligro.

En lo que a equipo se refiere la red de PEMEX esta integrada por equipo y sistemas de comunicación de diferentes fabricantes, lo cual la hace una red difícil de mantener y administrar, adicionalmente de que se usan infraestructuras separadas para los servicios de datos y de telefonía.

Dada la heterogeneidad de los sistemas de comunicaciones de PEMEX, no es posible diseñar un modelo de VoIP que pueda ser aplicado en cualquier instalación de PEMEX, ya que cada instalación cuenta con equipo de diferentes fabricantes, utilizan diferentes tecnologías de transporte o diferentes protocolos de comunicación. Para cada instalación es necesario hacer un diseño particular, tomando en cuenta sus características particulares.

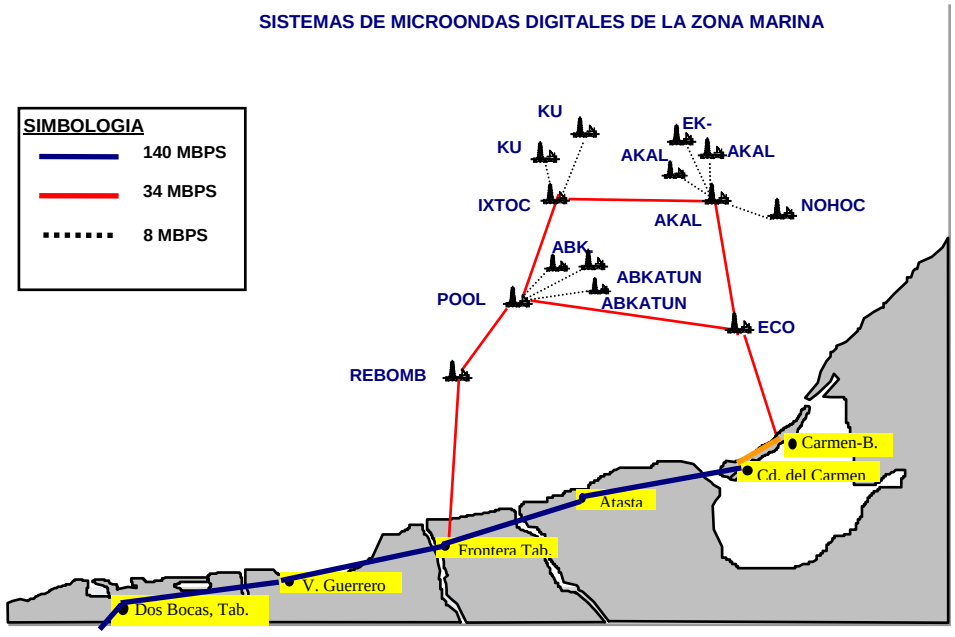
El siguiente ejemplo se basa en los sistemas utilizados en las instalaciones de la zona marina de PEMEX que abarca los centros de trabajo de Dos Bocas, Tab., el área de plataformas de Cd. del Carmen, Camp., Lerma, Camp., Mérida, Yuc. y Progreso, Yuc. Dentro de esta zona realizan sus operaciones básicamente los organismos subsidiarios Pemex Exploración y Producción, Pemex Refinación y Pemex Corporativo.

Entre las instalaciones de la zona marina se encuentran complejos de producción, plataformas periféricas de producción, pozos en producción, plataformas de perforación, plataformas exploratorias, plataformas de reparación y terminación de pozos, plataformas de mantenimiento, plataformas habitacionales, plataformas de medición, plataformas de rebombeo, almacenes, talleres, laboratorios, muelles y oficinas administrativas.

### 4.3 Revisión de la Infraestructura de Red Disponible

#### 4.3.1 *Backbone*

De acuerdo a la guía de diseño, el primer paso es el inventario y la evaluación del equipo de red existente. A nivel WAN las instalaciones de la zona marina de PEMEX se comunican mediante un sistema de enlaces de microondas digitales, con anchos de banda de 8, 34 y 140 Mbps, que utilizan ATM como tecnología de transporte, lo cual constituye una gran ventaja ya que se pueden aprovechar ciertas características de esta tecnología para implementar VoIP de una manera más efectiva que con otras tecnologías de transporte. A continuación se muestra el esquema del sistema.




*Backbone de la Zona Marina*

Este sistema de transporte sirve como *backbone* para la red de datos, la red telefónica y de otros sistemas de comunicaciones importantes.

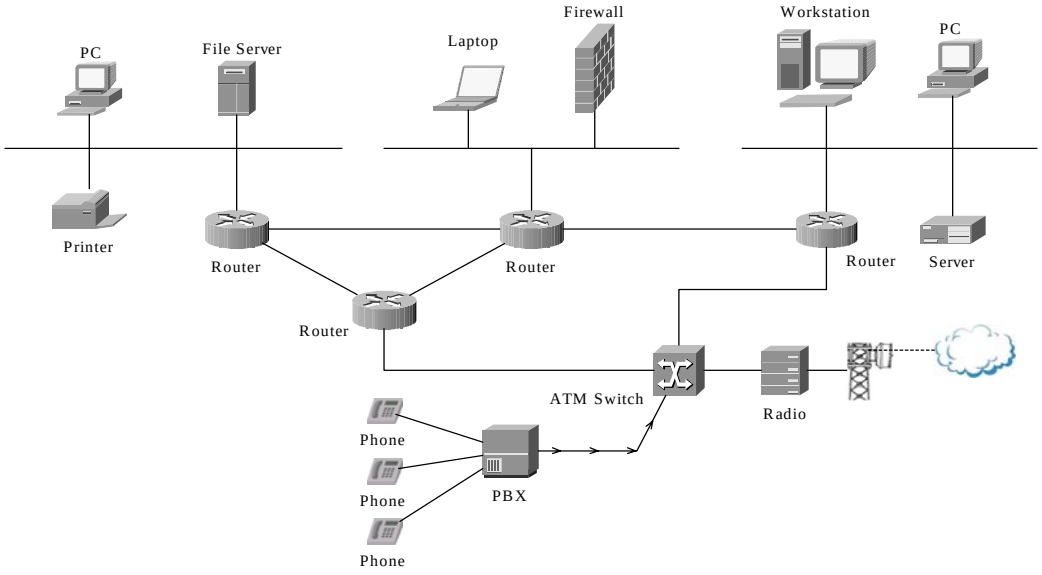
### 4.3.2 Red de Datos

La red de datos a nivel LAN esta integrada por cableado estructurado, se utiliza el estándar FastEthernet en la capa de enlace, que proporciona un ancho de banda de 100 Mbps, este sistema se usa para el trasporte de varios servicios, como lo son Internet, redes virtuales, sistemas de control y monitoreo, sistemas de producción, etc. que usan el protocolo IP, en estas instalaciones se utiliza equipo de conmutación y enrutamiento de datos de Cisco y Nortel Networks principalmente, aunque también se tiene equipo de otros fabricantes.

En algunas de las instalaciones, que están en áreas clasificadas como peligrosas, se utiliza una infraestructura para el cableado y equipo a prueba de explosiones de acuerdo a las normas correspondientes a ese tipo de instalaciones, esta infraestructura también tiene la finalidad de proteger los sistemas de la corrosión producida por la humedad y la salinidad del ambiente marino imperante en estas instalaciones.

#### 4.3.2.1 Topología de Red

A continuación se muestra un esquema generalizado de la topología de red que se tiene en las instalaciones de de la zona marina, esta compuesta principalmente por *switches* Ethernet 10/100 Mbps, para interconectar, mediante cableado estructurado, equipos como computadoras, servidores, *firewalls* e impresoras que se comunican entre si a través del protocolo IP mediante enrutadores, el acceso a la red WAN se realiza a través de *switches* ATM y el sistema de microondas digitales, que también es usado por la red telefónica como se puede observar en el diagrama.




*Topología General de Red de las Instalaciones de la Zona Marina*

Este modelo de red funciona mediante un esquema de direccionamiento IP privado, lo que significa que los elementos de la red, como computadoras y servidores, tienen una dirección IP que no puede ser accedida desde Internet, por lo que se usa un servidor DHCP/NAT (ver capitulo 2) para dar acceso a Internet a los sistemas de la red, adicionalmente se usan también servidores de acceso que brindan los servicios de seguridad y servidores de servicios, como lo son servidores de correo electrónico, entre otros.

Respecto al equipo de red, se tienen *modems*, *switches* Ethernet, *switches* ATM, enrutadores y multiplexores de diferentes fabricantes, localizados en cuartos de telecomunicaciones, algunos de estos dispositivos soportan mecanismos para proporcionar VoIP, como los enrutadores, los *switches* ATM y algunos *switches*

Ethernet, por lo que en algunos puntos de la red se podrán utilizar las características de estos dispositivos para asegurar la calidad de la voz transportada por la red de datos, mientras que en algunos otros puntos donde se detecten situaciones que degraden dicha calidad, como en cuellos de botella, se propondrá la sustitución de equipo por otro que permita asegurar la calidad de servicio (QoS) requerida.

La administración de las redes de datos y de voz es llevada a cabo de manera remota y por personal de PEMEX autorizado, por lo que para la implementación de este tipo de tecnología será necesaria una colaboración muy estrecha con dicho personal, esto con la finalidad de asegurar el correcto funcionamiento del sistema.

El uso de cableado estructurado, de sistemas de seguridad y equipo de comunicaciones adecuado permiten a PEMEX tener redes de datos confiables, seguras y de alto desempeño, que brindan un soporte adecuado a una gran cantidad de aplicaciones, así como también permiten la integración de nuevos sistemas y servicios de una manera efectiva y dando al usuario un servicio de gran calidad. En estas redes de datos se da prioridad a los sistemas críticos, como el de producción.

### 4.3.3 Red Telefónica

#### 4.3.3.1 Conmutador Meridian

La red telefónica conmutada de las instalaciones de la zona marina están basadas en los sistemas Meridian 1 de Nortel Networks, entre los servicios y características integradas de estos sistemas están los siguientes:

- Servicio de audioconferencia: Que permite la comunicación interactiva multipunto entre varios interlocutores de una manera remota y sin necesidad de proveedores externos. **Meridian Integrated Conference Bridge (MICB)**
- Sistema de mensajes y música digitales grabados: Que permite dar mensajes importantes a través del teléfono y reproducir música mientras un usuario espera que atiendan su llamada. **Meridian Integrated Recorded Announcement (MIRAN)**
- Sistema de redireccionamiento de llamadas: Que permite filtrar y enrutar las llamadas hacia otro teléfono de acuerdo a las preferencias del usuario con la finalidad de que sus llamadas le sigan a donde se encuentre. **Meridian Integrated Personal Call Director (MIPCD)**
- Sistema de despertador automático y un sistema que indica que el usuario no desea ser molestado. **Meridian Integrated Voice Services (MIVS)**
- Asistente integrado de llamadas: Que atiende automáticamente las llamadas y las enruta interactivamente con el usuario mediante un menú de voz. **Meridian Integrated Call Assistant (MICA)**
- Sistema de correo de voz: Que almacena mensajes de voz de los usuarios en buzones para que puedan ser escuchados por los dueños de dichos buzones desde cualquier teléfono.
- Servicios suplementarios tradicionales como llamada en espera, identificador de llamadas, multiconferencia, etc.

Adicionalmente los conmutadores Meridian 1 pueden brindar las siguientes funciones adicionando otros sistemas:

- **Symposium Call Center Server**: Que es un centro de llamadas que permite procesar las llamadas para que sean conmutadas automáticamente.
- **Optivity Telephony Manager**: Que es un sistema que permite administrar y configurar la red telefónica de una manera centralizada y remota.
- **Soluciones Remotas**: Que son sistemas que permiten la interconexión con el sistema Meridian de oficinas remotas de tal manera que los usuarios puedan usar todos los servicios del sistema Meridian como si estuvieran directamente conectados.
- **CallPilot**: Sistema de mensajería unificada que permite la integración de mensajes de texto, de voz y de datos.

Meridian 1

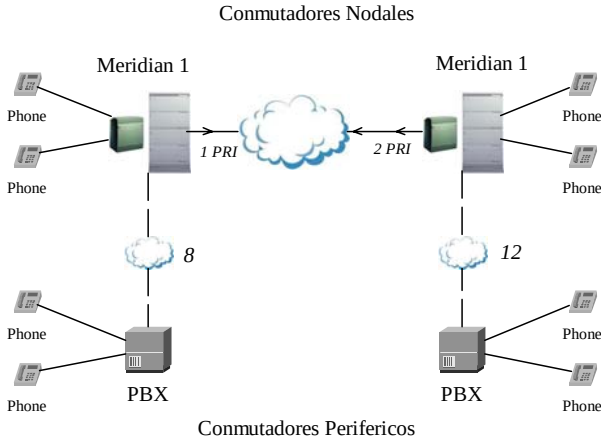
El conmutador telefónico Meridian 1 es un sistema flexible con el cual se pueden aprovechar las innovaciones tecnológicas más recientes, ya que tiene la posibilidad de interconectar la red telefónica a la red LAN y/o WAN mediante *gateways* de telefonía Internet (*Internet Telephony Gateways*) ITG, que permiten la integración de nuevos servicio y la implementación de VoIP.

La arquitectura de las PBXs Meridian incluye capas de procesamiento, conmutación, acceso y control que permiten invertir en tecnologías VoIP sin impactar en la inversión que se ha hecho en el resto del sistema Meridian. Lo anterior permite una migración suave y efectiva hacia VoIP y hacia una red integrada.

El nivel de servicio de la red telefónica es muy bueno, usualmente se tiene una disponibilidad del 99.999 % con este tipo de sistemas y los servicios brindados cumplen con las necesidades de comunicación esenciales además de otros que representan un valor agregado para los usuarios, sin embargo con VoIP se tendrían mejores herramientas para incrementar la productividad y se percibiría una mayor plusvalía del servicio por parte de los usuarios.

### 4.3.3.2 Topología de Red

En el siguiente esquema se observa la topología general de la red telefónica:




*Red Telefónica Conmutada*

En el esquema se puede observar que la red telefónica utiliza los PBXs Meridian 1, como conmutadores nodales, que sirven para interconectar a otros PBXs de menor capacidad llamados conmutadores periféricos y que en este caso son de diferentes fabricantes (ROLM, OMNI-S1, AT&T y Nortel Networks), el ancho de banda esta representado por el número de canales telefónicos digitales de 64 kbps (8 y 12) y por el número de troncales digitales primarios (RDSI) (1 PRI y 2 PRI) que equivalen a un enlace E1 con un ancho de banda de 2048 kbps.

Respecto a los teléfonos, se cuenta principalmente con teléfonos alambricos diseñados para el sistema Meridian que permiten hacer uso de los servicios avanzados del sistema (servicios suplementarios, correo de voz, etc) y otros que solo permiten hacer uso de los servicios básicos.

## 4.4 Establecimiento de los Objetivos para la Red

Considerando que el nivel de servicio de las redes telefónica y de datos de PEMEX es muy bueno, los objetivos para la red VoIP estarán orientados a mantener el nivel de servicio para los sistemas de datos y a mantener un nivel de disponibilidad cercano al 99.999% de la RTC en el nuevo sistema telefónico, brindando además mayores ventajas en cuanto a funciones y servicios que sirvan para incrementar la productividad de los usuarios, brindando adicionalmente ahorros económicos derivados de la integración de las redes de voz y datos, y además proporcionando ventajas en la administración del sistema.

Para lograr lo anterior, en este caso se propone una implementación híbrida de VoIP que permita la comunicación entre usuarios de la RTC y los usuarios de la red de VoIP de una manera transparente y que permita una migración paulatina hacia una implementación puramente IP, con la finalidad de proteger las inversiones en el sistema telefónico conmutado.

Se mantendrán los servicios y el plan de marcación de la red telefónica conmutada, permitiendo que los usuarios de la RTC y de la red VoIP se puedan comunicar entre si con un nivel de satisfacción similar, en lo que a calidad de la voz y disponibilidad se refiere, pero brindando una gran variedad de servicios a los usuarios de VoIP como los son un sistema de mensajería unificada que les permita combinar mensajes de voz, datos y fax en una misma aplicación, un directorio corporativo basado en Internet que permita la localización de personal de una manera sencilla y efectiva y que además brinde un sistema de marcación simplificado (con un “clic” o con un botón por ejemplo), un centro de llamadas basado en Internet que brinde información importante a un cliente, a un proveedor, a un trabajador, etc. y que permita que su llamada sea transferida a la persona indicada.

Los usuarios de VoIP también tendrán la ventaja de hacer uso de las nuevas aplicaciones multimedia para telefonía IP, que serán las que mayormente impacten en el incremento de la productividad del personal y en el nivel de satisfacción de los usuarios. Con estas herramientas serán capaces de saber si una persona esta disponible antes de llamarle, compartir información y aplicaciones de una manera segura y en tiempo real, mantener comunicaciones permanentes y la realización de videoconferencias entre otras cosas.

### 4.5 Revisión de la Tecnología y Servicios

El sistema que se propone para la implementación de VoIP en la zona marina es el “Succession” de Nortel Networks, que es el sistema que mejor se ajusta a los objetivos, que protege las inversiones hechas en el sistema Meridian, que es un sistema que mantiene el nivel acostumbrado de disponibilidad y servicio, que brinda una gran variedad de funciones, que soporta una gran cantidad de dispositivos como teléfonos y PBXs analógicos y digitales, que cuenta con las interfaces que actualmente se tienen en los sistemas de PEMEX, y que brinda además soporte para aplicaciones multimedia innovadoras.

Este sistema se basa en los estándares para VoIP H.323 y SIP. H.323 es el estándar más maduro y el que ha sido más ampliamente implementado, esto permite que se puedan integrar equipos o aplicaciones de otros fabricantes a la red VoIP de una manera efectiva, por otro lado el protocolo SIP permite aprovechar la nuevas aplicaciones multimedia para VoIP que han sido desarrolladas hasta el momento, así como las que están siendo desarrolladas o que serán desarrolladas en el futuro.

En este caso se tiene la gran ventaja de que el sistema Meridian se puede migrar o transformar en el sistema Succession de una manera económica y flexible que permite la implementación de VoIP tan rápido como se requiera. Para el caso de las instalaciones nuevas se puede instalar el sistema Succession que se puede interconectar transparentemente con los sistemas Meridian protegiendo así las inversiones en dicho sistema.

#### 4.5.1 Sistema Succession

A continuación se hace una revisión de los componentes y servicios del sistema Succession y posteriormente se describirá como realizar la migración del sistema Meridian al sistema Succession.

Los elementos clave del sistema Succession son los siguientes:

- *Call Server* (Servidor de llamada)
- Signaling *Server* (Servidor de señalización)
- *Succession Media* Gateway
- Soluciones para sucursales y oficinas remotas
- Comunicaciones Seguras
- Administración Unificada
- Infraestructura de Datos
- Aplicaciones: Mensajería unificada, centro de contacto a clientes, portal de solución por voz, consola de asistencia y soporte para teléfonos digitales

#### 4.5.1.1 *Call Server* (Servidor de Llamadas)

El *Call Server* o servidor de llamadas se encarga de los servicios de administración de conexiones y de llamadas para la red IP, para brindar servicios tales como el de oficina virtual que permite que los usuarios se identifiquen en cualquier teléfono IP de su red usando una contraseña para acceder a las características y al perfil de usuario de su propio teléfono de escritorio. Otras características soportadas por los *Call Servers* son:

- Directorio Corporativo
- Conferencias
- Regreso de llamadas
- Grabación de detalles de llamada

*Call Server*

#### 4.5.1.2 *Signaling Server* (Servidor de Señalización)

El servidor de señalización es un servidor estándar que proporciona las interfaces de señalización hacia la red IP usando aplicaciones de software que corren sobre el sistema de tiempo real VxWorks. Esto permite el uso de componentes a los largo de redes WAN. El servidor de señalización lleva a cabo importantes servicios de control de llamada como el registro de terminales y *gateways*, el control de admisión, la traducción de direcciones IP y el control del ancho de banda. Este servidor esta basado en el estándar H.323 que permite tener una interfaz de señalización entre sistemas Succession a través de una red WAN o con *gateways* H.323 y PBXs que actúan como *gateways*. Las aplicaciones son compartidas entre sistemas brindando continuidad de características y servicios.

*Signaling Server*

#### 4.5.1.3 *Succession Media Gateway*

La *Succession Media Gateway* actúa como traductor entre la red IP y la red telefónica basada en TDM, entre sus características más importantes están:

- Soporte de un amplio rango de interfaces, incluyendo troncales analógicas y digitales para la RTPC, RDSI y T1/E1, así como líneas analógicas y digitales.
- Soporte para teléfonos IP alámbricos e inalámbricos así como soporte para teléfonos y faxes analógicos
- Interfaz para soportar teléfonos digitales Meridian.
- Cumplimiento con el estándar Q.SIG para sistemas PBX

*Succession Media Gateway*


*Succession 1000*

**4.5.1.4 Oficinas Remotas y Sucursales**

El sistema Succession puede ser distribuido a través de una red WAN para dar soporte al personal de oficinas remotas de tal manera que dichos usuarios puedan hacer uso de las características del sistema tales como el de marcación abreviada y las aplicaciones avanzadas como la de mensajería unificada y los servicios del centro de contactos Symposium. Las soluciones para sucursales y oficinas remotas soportan la conexión a la RTC para el caso de que se pierda el contacto con el sitio principal, también que llamadas locales puedan ser pasadas directamente por el sistema telefónico local. Estos sistemas extienden transparentemente los servicios de señalización y de la *media gateway*, soportando hasta 400 usuarios.

El *Call Server* de la oficina principal proporciona el procesamiento de llamada tanto para la oficina principal como para las oficinas remotas, mientras que la *Media Gateway* H.323 localizada en la sucursal u oficina remota permite el acceso a la red telefónica local. Si una conexión IP hacia la oficina principal no se puede realizar, la *Media Gateway* pasa a un modo de supervivencia para continuar dando servicio a través de la RTC, una vez que la conexión WAN se restaura, la conexión con la oficina principal se reestablece automáticamente.

**4.5.1.5 Seguridad de Comunicaciones**

Nortel Networks proporciona herramientas que permiten un tráfico seguro para las llamadas y aplicaciones de VoIP de una manera escalable y eficiente. Los *gateways* ofrecen servicios de seguridad IP en una plataforma integrada que proporciona capacidades de enrutamiento IP, soporte de redes virtuales privadas o VPNs, funciones de *firewall*, encriptación, autentificación, aplicación de políticas y administración de ancho de banda.

**4.5.1.6 Sistema de Administración Centralizada**

El sistema Succession puede ser administrado por la aplicación de administración de telefonía *OTM* (*Optivity Telephony Manager*), esta aplicación proporciona características de configuración, administración y control simplificadas tanto para sistemas Succession como para sistemas Meridian, esta basada en una arquitectura cliente servidor y en una interfaz basada en *web* que ofrece un punto único de entrada para una administración centralizada de todo el sistema, con la capacidad para soportar un acceso multiusuario.
Este sistema además proporciona una visión clara del uso y estado de la red, entre las funciones avanzadas de administración están las alarmas de administración y notificación, la configuración y mantenimiento de estación y la generación de reportes. Entre las utilidades del sistema se encuentran un sistema para recuperarse de desastres, capacidad para importar y exportar bases de datos, capacidad de respaldo y restauración de bases de datos, sincronización con el protocolo LDAP (*Lightweight Directory Access Protocol*) y calendario de tareas.

**4.5.1.7 Soporte para Teléfonos IP**

El sistema Succession soporta todos los tipos de teléfonos, teléfonos de escritorio para VoIP, digitales, analógicos y teléfonos basados en aplicaciones de software que se integran a computadoras de escritorio y portátiles, además también se tiene soporte para teléfonos inalámbricos.

Los teléfonos IP de escritorio diseñados para el sistema Succession se conectan directamente a la red LAN mediante un conector RJ-45 y soportan conexiones Ethernet de 10 Mbps y 100 Mbps, estos soportan un amplio rango de aplicaciones como el de mensajería unificada y soportan direccionamiento estático o mediante DHCP, lo que permite que, una vez configurados, puedan ser movidos a cualquier nodo de la red IP. Estos teléfonos cuentan con un *switch* Ethernet 10/100 Base-T que les permite compartir un nodo de red con una computadora. En ambientes críticos se tiene la posibilidad de alimentar estos teléfonos a través de un cable UTP mediante una fuente de alimentación llamada BayStack 460-24T-PWR.

Las mayores ventajas de VoIP se pueden apreciar mediante los teléfonos multimedia basados en software. Mediante una interfaz gráfica las computadoras portátiles y de escritorio son convertidas en herramientas poderosas para comunicaciones unificadas de voz, datos y video. Esta solución brinda los mismos servicios y capacidades de los teléfonos IP de escritorio además de poderosas capacidades de directorio y aplicaciones multimedia.

El sistema Succession tiene otras características de valor agregado como los son el soporte de DHCP que permite que los teléfonos IP puedan ser movidos, agregados y cambiados de una manera muy sencilla, soporta el estándar 802.11 que se usa para dispositivos inalámbricos, entre los servicios soportados están el de mensajería unificada y centros de llamada basados en Internet.

### 4.5.2 Migración del Sistema Meridian 1 al Sistema Succession 1000

La conversión de los sistemas Meridian 1 al sistema Succession 1000 es posible mediante la actualización del software del sistema Meridian al software Succession 3.0 y agregando un servidor de señalización para el tráfico IP y la administración de terminales. Esta solución VoIP de Nortel Networks provee una ruta para la implementación de VoIP en sistemas basados en el Meridian de una manera transparente, segura, efectiva pero sobre todo económica al aprovechar la inversión en el sistema Meridian.

Este nuevo sistema es llamado Succession 1000M y brinda los beneficios de la arquitectura e interconexión del sistema Meridian más los beneficios de la familia de IP PBXs Succession 1000. Para esto se aprovechan bloques de arquitectura comunes en ambos sistemas y una plataforma de administración común para implantar la tecnología IP en el sistema Meridian de acuerdo a las necesidades del sistema para brindar VoIP donde sea necesario.

La arquitectura del software para la migración esta diseñada para soportar los modelos de comunicación IP actuales y los futuros, sus componentes principales son los siguientes:

- El Administrador de Procesos (*Feature Processing Manager*)
- El Administrador de Conexiones Virtuales (*Virtual Connection Manager*)
- El Administrador de Conmutación de Circuitos (*Circuit Switching Manager*)

**Administrador de Procesos (*Feature Processing Manager*)**
El administrador de procesos combina las características del software de los sistemas Meridian 1 y Succession 1000 para proporcionar servicios a equipos de ambos sistemas además de otras capacidades innovadoras.

**Administrador de Conexiones Virtuales (*Virtual Connection Manager*)**
El administrador de conexiones virtuales permite que los dispositivos basados en IP accedan a las mismas características del sistema Meridian que los dispositivos telefónicos existentes, de tal manera que el conjunto de características y funciones de los sistemas Meridian 1 y Succession 1000 estén disponibles y puedan ser usados por los dispositivos IP y clientes de software. Soporta los teléfonos IP i2002, i2004 y el teléfono de software i2050. Otros modelos de teléfonos IP que serán integrados para este sistema serán el i2001 especial para la atención de clientes, el i2005 que proporcionara funciones extendidas para agentes en centros de contacto IP, el i2008 que incluirá una pantalla grafica y un micro explorador *web*, y finalmente el cliente para telefonía móvil i2050 que servirá para brindar servicios de voz a computadoras de bolsillo inalambricamente.
Adicionalmente otros fabricantes están desarrollando productos para interactuar con el administrador de conexiones virtuales, un ejemplo es el *Gateway* de NET6 que permitirá la transformación de aplicaciones *web* para que puedan ser usadas por clientes de telefonía IP.

**Administrador de Conmutación de Circuitos (*Circuit Switching Manager*)**
Este componente se desarrollo a partir del software del Meridian 1 para permitir que los componentes de hardware del Meridian 1 puedan ser controlados por el administrador de procesos, de tal manera que las características del sistema Meridian puedan seguir siendo usadas mientras se añaden otras nuevas sin que se creen conflictos.

**Administración del Sistema**

El sistema de administración de telefonía Optivity OTM (*Optivity Telephony Manager*) es la plataforma que sirve para administrar los sistemas Meridian 1 y Succession 1000, esto brinda beneficios inherentes cuando se busca migrar hacia VoIP. Este sistema puede seguir siendo utilizado para administrar el sistema Succession 1000M, agregándolo al servidor en la misma manera como se agrega un nuevo sistema Meridian 1 o un sistema Succession 1000. Esto protege el capital intelectual en el que se ha invertido en capacitación y el soporte a la infraestructura es extendida al nuevo sistema de VoIP.

Las ventajas de utilizar sistema OTM son las siguientes:

- Acceso para la administración de telefonía desde una PC
- Soluciones de administración basadas en *web*
- Sistema simplificado de organización y configuración
- Administración de monitoreo y control
- Soluciones de administración remotas
- Soluciones escalables para sistemas de pequeños a grandes

### 4.5.3 Estrategias para la Migración

El sistema Meridian 1 usa el software X11 para brindar capacidades IP a PBXs tradicionales basados en TDM, mientras que el sistema Succession utiliza el software Succession 2.0. Con el software Succession 3.0 los dos sistemas de software se integran en un sistema que permite la convivencia de ambos sistemas.

La migración desde el sistema Meridian 1 Option 61C o 81C hacia el Succession 1000M ofrece una arquitectura completamente redundante y altamente escalable con servidores de llamadas integrados para el aseguramiento de las aplicaciones de voz criticas. La migración a partir de los sistemas Meridian 1 Option 11 se logra con el software Succession 3.0 y el servidor de señalización acompañados de actualizaciones en el núcleo del sistema de hardware.

Con el sistema Succession 1000M, los usuarios pueden ser soportados en un modo centralizado usando equipo periférico inteligente (*Intelligent Peripheral Equipment*) IPE, como se hace en el sistema Meridian, y también se pueden distribuir los usuarios sobre la red LAN y/o WAN mediante las *Succession Media Gateways*. Las soluciones para oficinas y sucursales remotas del sistema Succession también están disponibles con el sistema Succession 1000M.

El sistema Succession 1000M soporta hasta 10 000 usuarios IP por sistema, con la capacidad de interconectar hasta 1000 sistemas bajo una misma plataforma de administración.

Mientras que el sistema Succession funcionando con el software Succession 3.0 proporciona las siguientes características:

- **Escalabilidad:** Desde menos de 100 usuarios hasta 100 000 usuarios que pueden estar dispersos en una red WAN.
- **Alta Calidad de Voz sobre redes LAN y WAN:** La latencia de punto a punto se reduce al convertir a TDM solo cuando es necesario.
- **Confiabilidad:** La redundancia opcional completa de procesadores, mecanismos de recuperación de fallos y componentes MTBF (*Mean Time Between Failure*) innovadores permiten lograr un porcentaje de disponibilidad del 99.999.

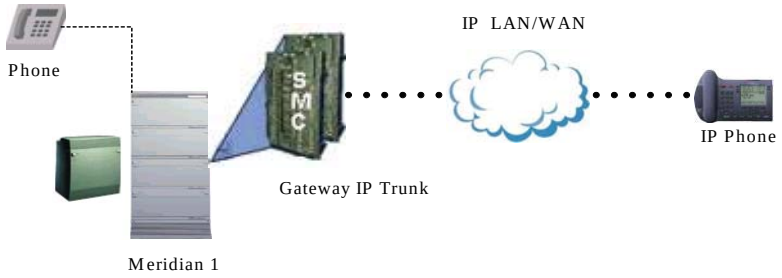
- **Uso de Estándares Abiertos:** Soporte para 802.1Q VLAN/QoS tagging, SNMP, soporte para teléfonos H.323 y *gateways* de otros fabricantes, soporte para clientes SIP y soporte para contenido *web* interactivo XML/HTML para teléfonos IP con pantalla.

Con el software Succession 3.0, el sistema Meridian 1 continúa brindando un sólido sistema de comunicaciones, permitiendo que los usuarios se muevan a su propio paso hacia modelos de comunicaciones IP más avanzados, la transparencia hacia el usuario de los servidores de llamadas también es mantenido, por lo que los usuarios pueden seguir usando aplicaciones que tenían con el sistema Meridian como el de mensajería unificada y el centro de llamadas Symposium. Esto provee protección en la inversión en equipo y en el entrenamiento para el usuario final cuando se migra a Succession 1000M.

Para proveer funcionalidades de VoIP a los sistemas Meridian 1 existen varias opciones desarrolladas para adaptarse a la velocidad con que se quieran integrar las redes de voz y de datos, una de estas opciones es la habilitación de la PBX para IP, otra opción es su interconexión con el sistema Succession y la opción más efectiva que es la de la actualización del sistema Meridian 1 al sistema Succession 1000M. A continuación se describen dichas opciones.

#### 4.5.3.1 Habilitación IP de una PBX

Una primera opción es la habilitación IP de una PBX (*Internet Enabling*) mediante *Gateways IP Trunk* y *Gateways Line Side* que sirven como puente para que se puedan comunicar los usuarios de VoIP y los usuarios del sistema telefónico tradicional.

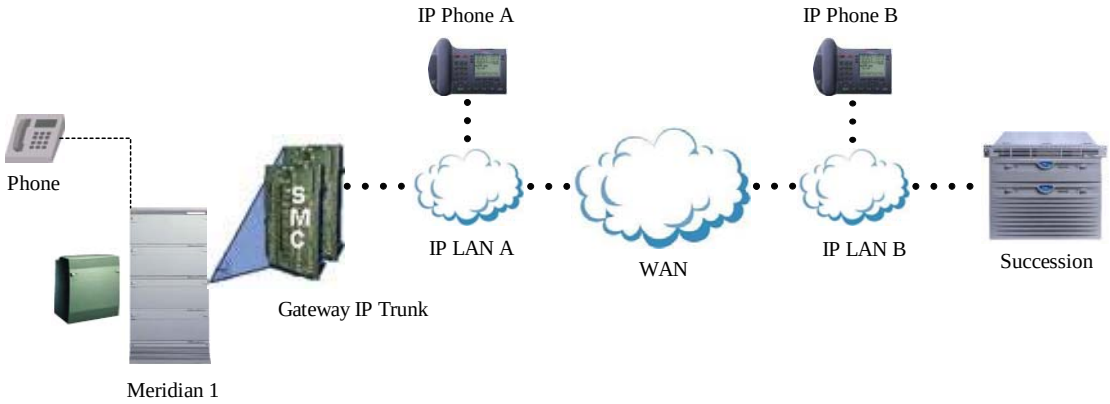



*Habilitación IP de la PBX Meridian 1*

Con esta opción los usuarios del sistema telefónico tradicional se pueden comunicar transparentemente con los usuarios de telefonía IP y viceversa.

#### 4.5.3.2 Interconexión del Sistema Meridian con el Sistema Succession

Otra opción es la interconexión del sistema Meridian con el sistema Succession 1000 mediante el sistema de interconexión de multi-sistemas de Nortel Networks, ya sea mediante una interfaz PRI ISDN o una interfaz IP, de tal manera que las funcionalidades para VoIP del sistema Succession puedan ser aprovechadas por otros puntos en la red. Si se usa el sistema IP Trunk 3.0 o superior se pueden establecer rutas directas entre teléfonos IP del sistema Succession 1000 y un gateway IP Trunk 3.0 en el sistema Meridian 1 mediante la red IP. El IP Trunk 3.0 puede ser conectado a cualquier terminal en el Meridian 1 usando protocolos de interconexión multi-sitios, lo que permite la transparencia entre las dos plataformas de la misma manera que entre dos sistemas Meridian. Las aplicaciones como CallPilot o Symposium pueden ser implementadas en cualquiera de las dos plataformas y brindar servicios a ambos sistemas. Algo similar ocurre con el sistema de administración, que es común en ambos sistemas, y que permite una migración más fácil.

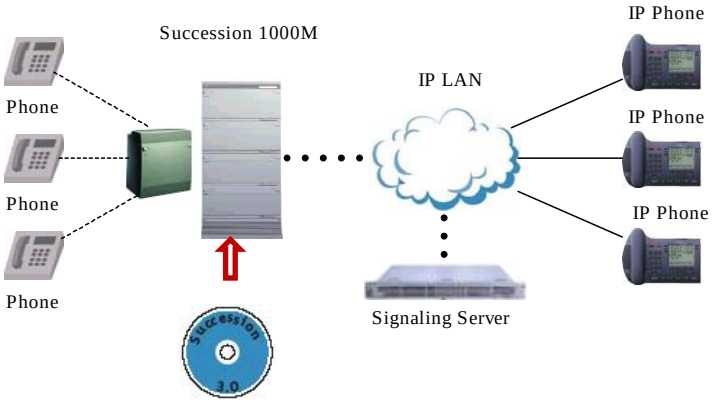



*Interconexión del Sistema Meridian con el Sistema Succession*

Con esta opción el teléfono IP A puede hacer uso de las características y funciones del sistema Succession localizado en la red LAN B a través de la red WAN, y los usuarios del sistema Meridian 1 se pueden comunicar con los usuarios del sistema Succession de la redes LAN A y B.

#### 4.5.3.3 Conversión del Sistema Meridian 1 al Sistema Succession 1000M

Una tercera opción, y la más recomendable, es la actualización al software Succession 3.0 en el sistema Meridian y el uso de un *Signaling Server*, esta solución permite la interconexión con sistemas Succession 1000, con un sistema Business Communications Manager Release 3.0, o con otro sistema Meridian 1 mediante una conexión IP usando el protocolo H.323. En este caso el sistema se transforma en el sistema Succession 1000M, donde el procesador de llamadas del Meridian 1 funciona como *Call Server* para toda la red IP. Los sistemas Meridian 1 pueden seguir usando entre ellos las interconexiones ISDN.




*Conversión del Sistema Meridian 1 al Sistema Succession 1000M*

Con esta opción los usuarios de la red telefónica tradicional pueden seguir haciendo uso de los servicios y características del sistema Meridian y se pueden comunicar transparentemente con los usuarios de VoIP, mientras que los usuarios de VoIP pueden disfrutar de todas las características y ventajas del sistema Succession 1000, esta opción permite una migración hacia VoIP de una manera parcial o total.

Como se puede observar estas opciones de implementación permiten una migración hacia una red integrada tan rápido o tan lento como lo demanden las necesidades del cliente.

La implementación de VoIP se puede llevar a cabo desde una pequeña hasta una gran escala mediante la agregación del software apropiado, mediante la agregación de *las Succession Media Cards*, que son tarjetas

IPE (*Intelligent Peripheral Equipment*) que proporcionan funciones de IP *trunking* y de *IP Line Side*, y mediante la elección adecuada de los clientes IP (i2002, i2004, i2050,Wireless VoIP).

La función *IP Peer Networking* esta disponible en los sistemas Succession y permite conexiones IP directas entre usuarios de VoIP en diferentes *Call Servers*. Esta función se realiza mediante software en el *Signaling Server* que es el que se encarga de proporcionar las funciones de *gatekeeper* H.323, las funciones de *gateway* H.323 para soportar la señalización entre *Call Servers* y los servicios *Proxy* para el registro de clientes IP. El *Signaling Server* permite que el sistema Succession 1000M se pueda interconectar con el sistema Succession 1000 a través de la red IP con las mismas ventajas que tendría otro sistema Succession 1000.

Si se tienen instaladas *Succession Media Cards* en el sistema Meridian cuando se migra al sistema Succession 1000M, estas tarjetas cambian de función ya que las conexiones IP se realizan directamente en el *Signaling Server*, entonces estas tarjetas se usan como *Voice Gateways Media Cards* que proporcionan funciones de DSP (*Digital Signal Processor*) para llamadas que se transmiten del dominio IP al dominio TDM en el sistema Succession 1000M, de tal modo que el equipo adquirido no se vuelve obsoleto.

La meta del software Succession 3.0 no es solo habilitar el sistema Meridian para VoIP, sino asegurar que el sistema Succession 1000M pueda tomar ventaja de todas las capacidades y características de la redes IP, ahora y en el futuro. Los sistemas que cuentan con una arquitectura de procesamiento de llamadas basadas en un sistema Pentium dual como el Meridian 1 Option 81C son capaces de utilizar el software *Succession Call Server* contenido dentro del Succession 3.0, con esta actualización de software y el *Signaling Server* los procesadores de llamadas duales Pentium (*Dual Pentium-based Call Processors*) actúan como el *Call Server* del Succession 1000M, mientras que el resto del sistema Option 81C funciona como un gran *Gateway* para incluir cualquier teléfono, incluso los teléfonos digitales Meridian.

Respecto a los sistemas Meridian Option 61C que no cuenten con *Dual Pentium-based Call Processors*, pueden ser actualizados para soportar todas las funciones del Succession 3.0 software, el sistema puede ser expandido vía *Succession Media Gateways*, que proveen la funcionalidad de *IP Trunk e IP Line*, o también se puede usar el *Signaling Server* opcional, para transformar el sistema Option 61C en un sistema Succession 1000M. El sistema Option 11C también puede ser actualizado con el Succession 3.0 software para proporcionar funciones de Succession 1000M.

### 4.5.4 Plan de Marcación y Administración

Uno de los factores de costo que a menudo no es reconocido en la migración de una red hacia un nuevo paradigma es la inversión hecha en la configuración del sistema y de los clientes IP, muchas soluciones VoIP requieren crear un ambiente de administración completamente nuevo o se tiene que trasladar el modelo de administración al nuevo sistema, usualmente las características entre el nuevo y el viejo son completamente diferentes por lo que se requiere invertir mucho tiempo para definir el plan de administración y de marcación.

En la migración del sistema Meridian 1 al sistema Succession 1000M no ocurre lo anterior, ya que el sistema de administración común permite que mucha de la información sea retenida y usada para la definición del nuevo sistema, por ejemplo la información personal de los usuarios (nombre, dirección, departamento, etc.) pero se puede ir más lejos al reutilizar la información de la configuración de características y servicios. El antiguo plan de marcación puede ser extendido hacia los nuevos nodos Succession. La herramienta de análisis y reportes OTM-ESN puede usar el plan de marcación de un nodo Meridian 1 como punto de partida para asignar los números a los nuevos clientes IP de acuerdo a dicho plan. Esto permite ahorrar hasta un 90% del esfuerzo requerido para definir las propiedades del sistema.

La administración de alarmas también se beneficia del ambiente de aplicación común, el ambiente de administración navegable en el OTM soporta los sistemas Meridian y Succession, además permite la visión de alarmas de los sistemas SNMP y de voz serial a través de toda la red, esto incluye alarmas desde el sistema Meridian 1 así como de aplicaciones como CallPilot, Meridian Mail y Symposium. Adicionalmente los *scripts* de notificación de alarmas definidos para los sistemas Meridian pueden ser reusados por el Succession. La notificación de alarmas proporciona la capacidad de reaccionar a condiciones de alarma específicas,

mandando un e-mail o fax, o filtrando y reenviando alarmas a sistemas administrativos de red de más alto nivel.

### 4.5.5 Aplicaciones Multimedia

#### 4.5.5.1 *CallPilot Unified Messaging*

Este es un sistema de mensajería unificada que integra los servicios de correo electrónico, mensaje de voz y fax para que puedan ser consultados mediante un teléfono o una computadora multimedia desde Internet. Este sistema almacena los mensajes de voz y de fax en el servidor **CallPilot Unified Messaging** mientras que para consultar los mensajes de correo electrónico interactúa en el servidor de correo sin impactarlo. El acceso al correo electrónico mediante el teléfono se logra mediante un convertidor de texto a voz TTS (*Text to Speech*), que también sirve para redactar correos. El acceso a los servicios mediante una computadora se realiza mediante la interfaz de exploración (*browser interface*) Callpilot, con el que se pueden reproducir y grabar mensajes de voz mediante las bocinas y el micrófono de la computadora, los faxes pueden ser vistos en la pantalla de la computadora o ser impresos por una impresora, mientras que los correos electrónicos pueden ser consultados de manera tradicional.

Entre las ventajas de esta sistema están que se puede integrar con el *callcenter* Symposium, para que los usuarios dejen mensajes de voz en caso de que su llamada no pueda ser atendida, por ejemplo, brinda varias características de seguridad, como opciones de encriptación, y que puede ser administrado remotamente mediante una computadora conectada a Internet.
Este sistema puede ser usado por los sistemas Meridian 1 y los sistemas Succession mediante la integración de una tarjeta IPE, con soporte para 2200 usuarios, o puede ser brindado por un servidor estándar con soporte para 7000 usuarios.

#### 4.5.5.2 *Nortel Networks Multimedia Exchange*

El Succession 3.0 software está diseñado para trabajar de manera fluida con *Nortel Networks Multimedia Exchange* (MX), una solución de entrega de aplicaciones multimedia y colaborativas basadas en SIP (*Session Initiation Protocol*) que forma parte del *Nortel Networks Multimedia Communications Portfolio*. El protocolo SIP proporciona servicios basados en *web* mediante sesiones multimedia en tiempo real que pueden integrar voz, datos y video, SIP tiene una arquitectura basada en texto que agiliza el acceso a nuevos servicios con una gran flexibilidad y escalabilidad. (Ver capitulo 3)

Los usuarios del sistema Succession pueden incorporar en sus computadoras un software de telefonía cliente y aprovechar las aplicaciones del servidor *web Multimedia Communication Server (MCS) 5100*, que incluye servicios de colaboración como conferencias, *whiteboard*, intercambio de archivos, *web push* y navegación conjunta, servicios de personalización como son control de llamadas, control de entrada de llamadas, administración de llamadas y enrutamiento, servicios multimedia como llamadas de video, ID de llamada mediante fotografías, servicios de presencia y mensajes instantáneos. Esta solución esta orientada a mejorar la productividad de los usuarios, reducir tiempos de producción y facilitar la toma de decisiones.

Las herramientas de colaboración agilizan el proceso de toma de decisiones al compartir recursos e información con compañeros, clientes, proveedores y socios de negocios. El *whiteboard* se usa para compartir información visual en tiempo real y para compartir archivos transparentemente mientras se habla por teléfono. La función de *push web pages* permite enviar páginas *web* a la pantalla de alguien más durante una llamada y también permite la navegación conjunta de páginas *web* entre varios usuarios.

Las características de personalización permiten adaptar los servicios de comunicación a la manera de trabajar del usuario, permite la administración de las llamadas entrantes basándose en la identificación de llamadas, la hora del día y otros criterios. Permite decidir entre contestar las llamadas o reenviarlas al buzón de voz, al e-mail o a una pagina *web*. Todas las llamadas son rastreadas automáticamente y se registra la forma en que fueron tratadas. La identificación de llamadas mediante fotos permite ver quien es el que esta llamando antes de contestar.

Las aplicaciones multimedia permiten enlazar al personal laboral distribuido mediante llamadas de video, permitiendo reuniones cara a cara sin la necesidad de la molesta, costosa y estresante necesidad de viajar. Mediante la mensajería instantánea se puede interactuar con uno o más compañeros de trabajo al mismo tiempo para mantenerse informado o intercambiar ideas.

La función de agente personal le permite al usuario establecer sus propias reglas para la presentación y manejo de las llamadas. Permite saber cuando otros usuarios están en línea, en una llamada, disponibles o no, antes de hacer una llamada.

### 4.6 Diseño Técnico y Planeación de la Capacidad

Para el diseño técnico se optimizara la infraestructura de la red de datos para asegurar que sea adecuada para la implementación de VoIP, además se determinara la estrategia de implementación de QoS para asegurar el tráfico de VoIP y proporcionar un buen nivel de servicio.

#### 4.6.1 Optimización de la Red para VoIP

##### 4.6.1.1 Modelo Jerárquico

Una característica esencial en el diseño de la red IP es la de asegurar que la topología de la red este basada en un modelo jerárquico que permita la modularidad, es decir, que permita crear modelos de diseño (módulos) que puedan ser repetidos o modificados conforme crece la red, de tal manera que el costo y complejidad de hacer una actualización en la red quede restringido a una pequeña porción de toda la red. El aislamiento de fallos es facilitado por este modelo al modular la red en elementos pequeños, fáciles de entender, que ayudan a identificar los puntos de fallo.

Este modelo incluye tres capas:

- El *backbone* (*core*) o médula de la red que proporciona un servicio de transporte óptimo entre sitios, que en este caso esta representado por la red ATM de microondas y por los enrutadores de mayor capacidad.
- La capa de distribución que proporciona una conectividad basada en políticas y que en este caso se lleva a cabo en los enrutadores de menor capacidad.
- La capa de acceso que es la que proporciona acceso a la red a los usuarios, esta función es desempeñada en este caso por los *switches* Ethernet.

El *backbone* debe estar diseñado para conmutar los paquetes tan rápido como sea posible, sin desempeñar manipulación alguna en los paquetes que pudieran retardar el proceso.

La capa de distribución tiene el propósito de establecer limites y es donde se lleva a cabo la manipulación de paquetes, entre sus principales funciones están la agregación de direcciones (definición de áreas), el control del acceso de grupos de trabajo o departamentos a la red, la definición de la dominios de *broadcast* y *multicast*, el enrutamiento de la red y de las redes virtuales, y la seguridad.

La capa de acceso es el punto a partir del cual los usuarios tienen acceso a la red, esta capa puede usar listas de acceso o filtros para optimizar los requerimientos de los grupos de usuarios, entre sus funciones se incluyen las siguientes: la administración del ancho de banda, funciones de conmutación (*switching*), filtrado a nivel de capa MAC y la microsegmentación.

###### 4.6.1.1.1 Servicios de *Backbone*

Entre los aspectos que se deben evaluar y asegurar en los servicios de *backbone* de la red están los siguientes:

- Optimización de rutas (*paths*)
- Priorización de tráfico
- Balanceo de carga

- Rutas alternativas
- Encapsulación (*tunneling*)

**Optimización de rutas (*paths*):** Es necesario evaluar si las rutas de tráfico son las óptimas, principalmente en entornos donde estas rutas son seleccionadas automáticamente por los enrutadores, se requiere determinar si el protocolo de enrutamiento empleado se ajusta a los requerimientos específicos de la red. Actualmente los enrutadores soportan una amplia variedad de protocolos de enrutamiento y algunos enrutadores permiten una convergencia rápida y controlable mediante el ajuste de tiempos y métricas. La convergencia se logra cuando todos los enrutadores de la red acuerdan que todas las rutas son óptimas. Los algoritmos de enrutamiento que convergen lentamente pueden provocar lazos (*loops*) o interrupciones en la red.

**Priorización de tráfico:** Es necesario evaluar o habilitar funciones de priorización de tráfico en los enrutadores para asegurar que los protocolos o aplicaciones que transportan datos críticos tengan precedencia sobre el tráfico menos importante (Ver QoS en capitulo 2). En este caso se pueden también aprovechar las características de ATM para realizar funciones de priorización de tráfico.

**Balanceo de carga:** Cuando sea posible es recomendable implementar el balanceo de tráfico, que permite que el tráfico para un mismo destino pueda seguir varias rutas, de igual costo, de un modo balanceado para evitar la saturación de enlaces, cuando se utiliza el protocolo IP los enrutadores brindan balanceo de carga por destino o por paquete. Cuando se utiliza el protocolo de enrutamiento IGRP es posible el balanceo de carga en enlaces de diferente costo.

**Rutas alternativas:** Es conveniente implementar rutas alternativas, principalmente en los enlaces que transportan información crítica, para respaldar el sistema cuando ocurran fallos.

**Encapsulación (*tunneling*):** La encapsulación toma paquetes o *frames* de un sistema de red y los coloca dentro de *frames* de otro sistema de red, lo que permite la creación de túneles o interfaces virtuales por los cuales fluyen dichos datos de una manera más eficiente ya que se crea una especie de circuito a través de los enrutadores.

#### 4.6.1.1.2 Servicios de Distribución

Los servicios de distribución que deben ser evaluados y asegurados son los siguientes:

- Administración del ancho de banda del *backbone*
- Filtrado de áreas y servicios
- Distribución basada en políticas
- Redistribución de información de enrutamiento entre diferentes protocolos

**Administración del Ancho de Banda del *Backbone*:** Para optimizar la operación del *backbone* de la red los enrutadores usualmente ofrecen varias características que permiten ajustar su desempeño, como ejemplo se tienen la priorización de colas, que permite que ciertos tipos de tráfico tengan prioridad sobre otros y sean procesados más rápidamente, las métricas de los protocolos de enrutamiento y la terminación de sesiones locales. Se puede ajustar el tamaño de la cola de salida, para evitar que una cola con prioridad se sature o exceda su capacidad y se tengan que descartar paquetes importantes o prioritarios, también se pueden ajustar las métricas de enrutamiento para incrementar el control sobre las rutas sobre las que atraviesa el tráfico más importante.
La terminación de sesiones locales permite que los enrutadores actúen como *proxies* (dispositivos que actúan en representación de otro dispositivo) para sistemas remotos, esto es útil, por ejemplo, cuando dos dispositivos que usan un control de sesión de enlace (de capa 2) se comunican a través de una red WAN, cada que un equipo envía una paquete necesita recibir cierta información de control de parte del otro dispositivo para saber que ya recibió ese paquete y para enviar el siguiente paquete, esa confirmación no tiene que atravesar la red WAN cuando los enrutadores usan la terminación de sesiones ya que el enrutador que inicialmente recibe el paquete le envía dicha confirmación en lugar del dispositivo al otro lado de la red WAN, lo que permite una ahorro en el ancho de banda en la red WAN.

**Filtrado de Áreas y Servicios:** Los filtros de tráfico basados en área o servicios son las herramientas básicas de los servicios de distribución que se usan para brindar un control de acceso basado en políticas hacia los servicios de *backbone*. El filtrado de áreas y servicios se implementan usando listas de acceso, que son secuencias de enunciados que permiten o deniegan de tráfico bajo ciertas condiciones o para ciertas direcciones IP, las listas de acceso también se pueden usar para permitir o impedir el paso por el *backbone* de paquetes provenientes de nodos particulares de la red que se envían usando un cierto protocolo o servicio. En este caso se debe asegurar que el tráfico de los protocolos que serán usados por VoIP, como RTP y RSVP, sean aceptados en las listas de acceso.

**Distribución Basada en Políticas:** Dentro de este contexto una política es una regla o conjunto de reglas que gobiernan la distribución del tráfico de extremo a extremo a través del *backbone* de la red. Una distribución basada en políticas aspira a cumplir con los diferentes requerimientos de los diferentes departamentos dentro de una misma organización, sin comprometer el desempeño de la red ni la integridad de la información. De esta manera se puede hacer que dentro de un departamento donde se usan varias aplicaciones y protocolos se de prioridad de acceso al *backbone* a una o más aplicaciones que transportan información critica, como pueden ser los sistemas de producción por ejemplo. Se requiere asegurar que el equipo de red, enrutadores por ejemplo, soporten un amplio rango de tecnologías y protocolos para implementar las políticas de distribución, en este caso en particular será necesario evaluar el equipo disponible así como averiguar cuales son las políticas implementadas actualmente de tal manera que no sean afectadas por la implementación de las nuevas políticas.

**Redistribución de Información de Enrutamiento Entre Diferentes Protocolos:** En caso de que se tenga una red que maneje diferentes protocolos de enrutamiento es necesario evaluar que la información de enrutamiento de un protocolo sea redistribuida correctamente por otro protocolo.

#### 4.6.1.1.3 Servicios de Acceso Local

Entre los servicios de acceso local que deben ser evaluados están los siguientes:

- Segmentación de la Red
- Capacidades de *Broadcast* y *Multicast*
- Naming, Proxy y Cache Local
- Seguridad de Acceso al Medio
- Descubrimiento de Rutas

**Segmentación de la Red:** La división de la red en piezas más manejables es una función esencial de los enrutadores de acceso local, que se encargan de implementar políticas locales y limitar el tráfico innecesario. Se requiere que dichos enrutadores estén configurados con las direcciones de interfaz y submascaras de red adecuadas de tal manera que el tráfico de un segmento dado este limitado al *broadcast* local y al tráfico para una estación en ese segmento. La distribución cuidadosa de *hosts* para dividir la red contribuye a disminuir la congestión de toda la red.

**Capacidades de Broadcast y Multicast:** Muchos protocolos usan capacidades de *broadcast* y *multicast*, *broadcasts* son mensajes que se envían a todos los destinos de la red mientras que *multicasts* son mensajes enviados a un conjunto específico de destinos. Los enrutadores por default reducen inherentemente la proliferación de *broadcasts*, sin embargo los enrutadores pueden ser configurados para tolerar este tipo de tráfico si es necesario, algunas herramientas VoIP podrían hacer uso de esta característica para enviar mensajes a todos los usuarios. Los enrutadores ofrecen varias funciones para limitar los mensajes de *broadcast* que reducen el tráfico de la red, es por ello necesario emplear alguna de ellas para evitar que el ancho de banda pueda ser reducido seriamente, un ejemplo puede ser la técnica que envía los mensajes sobre un árbol extendido (*spanning tree*) que asegura una cobertura completa sin tráfico excesivo porque solo un paquete es enviado a cada segmento de la red. Para aplicaciones como las conferencias de video y audio las transmisiones *multicast* proporcionan un soporte excelente ya que en lugar de mandar un paquete para cada destino, se envía un paquete a un grupo *multicast* identificado por una dirección IP de grupo. Para soportar mensajes *multicast* los equipos de red deben usar el protocolo de administración de grupos Internet **IGMP** (*Internet Group Management Protocol*).

***Naming, Proxy* y Cache Local:** Estas son tres características claves de los enrutadores que pueden ayudar a reducir el tráfico y a promover la eficiencia de la red. Las aplicaciones de red y los servicios de conexión requieren de una manera racional de resolver nombres y direcciones, para facilitar esta tarea es recomendable que los enrutadores soporten servicios de resolución de nombres como lo son NetBIOS y DNS (*Domain Name System*). Un enrutador puede funcionar como *proxy* para un servidor de *Naming* (servidor DNS, por ejemplo), almacenando los nombres DNS en la memoria cache local, lo que permite resolver los nombres en el enrutador y con lo cual se evita el tráfico de *broadcast* entre los clientes y el servidor de resolución de nombres (*Naming*).

**Seguridad de Acceso al Medio**: Para prevenir violaciones de seguridad y accesos inapropiados de información los enrutadores deben impedir que el tráfico local alcance el *backbone* si no es indispensable e impedir que el tráfico del *backbone* sea accesible para grupos de red o departamentos inapropiados. Para realizar estas funciones se requieren métodos de filtrado de paquetes que ayudan a reducir el tráfico de un red y mejorar la seguridad. Probablemente el más poderoso de estos mecanismos sea la lista de acceso, que lógicamente previene que ciertos paquetes atraviesen interfaces particulares del enrutador, adicionalmente se pueden usar otros sistemas de seguridad como son **TACACS** (*Terminal Access Controller Access Control System*) que sirve para controlar el acceso de usuarios remotos por *modem* a la red, otra forma de evitar el acceso a la red de usuarios no autorizados es mediante el protocolo **CHAP** (*Challenge Handshake Authentication Protocol*) que también es comúnmente utilizado para controlar las comunicaciones entre enrutadores, este protocolo solicita a los dispositivos remotos que proporcionen una respuesta apropiada, y en caso de que la respuesta adecuada no sea correcta le deniega el acceso a la red.

**Descubrimiento de Rutas**: Las terminales de red deben tener la capacidad de localizar enrutadores cuando necesitan acceder a dispositivos externos a la red local, pero cuando más de un enrutador esta conectado al mismo segmento de red, la terminal debe ser capaz de localizar el enrutador que represente la ruta optima hacia su destino, para esto los enrutadores deben soportar diversos protocolos de descubrimiento de enrutadores como son el **ES-IS** (*End System to Intermediate System*) que se encarga de intercambiar información entre los enrutadores (*intermediate systems*) y las terminales de red (*end systems*) de tal manera que dichos equipos se puedan localizar, otro protocolo es el **ARP** (*Address Resolution Protocol*) que usa mensajes de *broadcast* para determinar la dirección MAC que corresponde a una dirección de red en particular, el protocolo de enrutamiento RIP comúnmente es usado por las terminales IP y puede ser usado para encontrar las direcciones de los enrutadores en el segmento LAN, cuando hay varios enrutadores, y para escoger la mejor ruta para una dirección de red dada.

El proceso de optimizar el desempeño de una red para lograr la integración exitosa de servicios puede ser una tarea complicada por la gran variedad de tecnologías involucradas y por todos los aspectos a evaluar, si a esto le agregamos la problemática de la administración de dicha red y la implementación de las políticas de QoS necesarias para el funcionamiento optimo de VoIP, la tarea de preparar la red para soportar VoIP puede ser muy demandante, si no se tiene una infraestructura adecuada. A continuación se describen algunas de las tecnologías y consideraciones técnicas para la implementación de QoS y posteriormente se describen algunos equipos que pueden servir para ello y para facilitar considerablemente la preparación de la red para la integración de servicios multimedia y de VoIP.

### 4.6.2 Estrategia de Implementación de las Políticas de QoS

Para satisfacer las necesidades de calidad de la voz para VoIP, se requiere la implementación de servicios de QoS de extremo a extremo, para lo cual es necesario involucrar un amplio rango de tecnologías, arquitecturas y protocolos. A continuación se analizan algunas de las técnicas y sistemas con que se cuenta actualmente para proporcionar servicios de QoS.

#### 4.6.2.1 Categorías de QoS

Para implementar QoS es necesario categorizar las aplicaciones para asignarles el nivel de prioridad adecuado, una clasificación conveniente es la siguiente:

| CATEGORÍA DE APLICACIONES | APLICACIONES | PRIORIDAD |
|---|---|---|
| Control de Red | Enrutamiento, alarmas, aplicaciones críticas. | Máxima |
| Interactivas | VoIP, video conferencias. | Alta |
| Sensitivas | Comunicaciones cliente-servidor, *streaming* de audio y video. | Media |
| Oportunas | E-mail, aplicaciones no críticas. | Baja |

*Categorías de QoS*

El nivel máximo de prioridad debe ser para las aplicaciones de control de red. Estas son usadas para controlar y administrar la red, entre estas aplicaciones están los protocolos de enrutamiento que deben tener prioridad sobre cualquier aplicación de usuarios, ya que si el desempeño de estos se ve afectado el desempeño de la red y de otras aplicaciones también se ve afectado, después siguen las aplicaciones críticas como pueden ser las de los sistemas de producción SDMC (Sistemas Digitales de Monitoreo y Control).

Las aplicaciones interactivas son aquellas en que dos o más personas participan activamente, estas son las aplicaciones de tiempo real, como VoIP y videoconferencias, que requieren latencias y retardos mínimos, por ser sensitivas al tiempo, y que por lo tanto requieren prioridades de QoS altas. Este tipo de aplicaciones típicamente se basan en el protocolo UDP.

Las aplicaciones sensitivas son aquellas en las que las personas interactúan con dispositivos de red como servidores, es decir, aplicaciones cliente-servidor, estas aplicaciones requieren de bajo retardo y bajas perdidas pero no son tan susceptibles como las aplicaciones interactivas por lo que reciben una prioridad alta pero menor que estas. Esta categoría incluye aplicaciones como radio Internet y *broadcasts* de audio y video (noticias, capacitación, etc). Estas aplicaciones típicamente usan TCP o UDP.

Las aplicaciones oportunas son aquellas que requieren que la información sea entregada de una manera segura y oportuna, pero que no son sensitivas al tiempo, como ejemplo se tienen las aplicaciones de correo electrónico y de transferencia de archivos, estas aplicaciones normalmente usan el protocolo TCP.

Dentro de cada clasificación se pueden tener varios niveles de prioridad, para asignar mayores prioridades a las aplicaciones más importantes o críticas dentro de cada grupo.

Para hacer la clasificación se recomienda hacer un estudio del tráfico que pasa a través de la red para determinar a que aplicaciones se dará una mayor prioridad y para hacer los ajustes necesarios en los anchos de banda requeridos para cada aplicación, en este caso se respetaran las políticas establecidas por PEMEX y a la aplicación de usuario que se dará mayor prioridad es a la de los sistemas de producción SDMC, después seguirían las aplicaciones sensitivas al tiempo como VoIP, después vendrían las aplicaciones cliente-servidor, como las de *streaming* de audio y video, y por ultimo las aplicaciones que de red no sensibles al retardo como los servicios de correo electrónico por ejemplo.

En lo que respecta a los anchos de banda se partirá de los esquemas actuales para hacer las modificaciones pertinentes.

#### 4.6.2.2 Tecnologías de QoS

La QoS se puede proporcionar desde diferentes capas de red del modelo OSI, la QoS en la capa física permite la separación y la priorización de tráfico mediante longitudes de onda, circuitos virtuales, puertos físicos, frecuencias, etc. Esta es la forma más simple de QoS pero tiene la limitación de que no distingue entre aplicaciones, de tal modo que todo el tráfico que pase por un puerto, por ejemplo, seria tratado de igual manera.

En la capa de enlace también se tienen herramientas de QoS, Ethernet proporciona dos mecanismos para brindar funciones de QoS, uno es mediante el estándar 802.1p que diferencia 8 clases de servicio, el otro

mecanismo es mediante VLANs (*Virtual LANs*), por las cuales se puede separar, aislar y priorizar el tráfico usando el identificador de VLAN (VLAN ID). Las redes VLAN permiten agrupar lógicamente a un conjunto de usuarios o dispositivos con requerimientos similares de QoS, sin que tengan que estar conectados físicamente a la misma subred. Comúnmente las VLAN permiten la separación y priorización de tráfico basándose en el *switch* Ethernet al que esta conectado cada usuario, las VLAN pueden ser creadas en base a la dirección MAC, el tipo de protocolo u otra información definida por el usuario.

En lo que respecta a ATM se cuenta con diferentes categorías de servicio, cada uno con diferentes parámetros de administración de tráfico y niveles de desempeño. Las categorías de servicio más comunes son: CBR (*Constant Bit Rate*), rt-VBR (*real-time Variable Bit Rate*), nrt-VBR (*non real-time VBR*) y UBR (*Unspecified Bit Rate*) (Ver capitulo 1). En general el servicio CBR es usado para servicios de emulación de circuitos, para transportar redes telefónicas conmutadas por ejemplo, el servicio rt-VBR se usa para aplicaciones en tiempo real basadas en paquetes, como VoIP y videoconferencias, el servicio ntr-VBR se usa para servicios de datos prioritarios y el servicio UBR es usado para servicios de datos de mejor esfuerzo. (Ver capitulo 1)
Otras categorías de servicio de ATM son ABR (*Available Bit Rate*) y GFR (*Guaranteed Frame Rate*) que son extensiones del nivel de servicio UBR que proveen garantías de servicio adicionales a las de UBR. ATM también proporciona parámetros de administración de tráfico como son PCR (*Peak Cell Rate*), SCR (*Sustained Cell Rate*) y CLP (*Cell Loss Piority*), estos parámetros definen el nivel de desempeño del tráfico en cada categoría de servicio particular.

Otra forma de proporcionar QoS es mediante MPLS, MPLS proporciona dos diferentes formas de QoS determinadas por los bits del campo EXP (Experimental) de la cabecera MPLS. Cuando se usan E-LSP (*EXP-Label Switched Paths*), los bits del campo EXP proporcionan 8 clases de servicio que soportan tanto prioridades de emisión y de descarte, y servicios diferenciados (DiffServ). Cuando se usa L-LSP (Label-LSP) los bits EXP proporcionan 8 prioridades de descarte.

Otra manera de proporcionar QoS es mediante ingeniería de tráfico. En una red IP los paquetes pueden tomar diferentes caminos, por ser una red orientada a no conexión, por lo que al pasar por diferentes rutas, con diferentes niveles de QoS, la QoS es menos predecible bajo una congestión de red. Cuando se buscan ofrecer niveles de servicio garantizados, las rutas de red pueden ser definidas mediante ingeniería de tráfico para proporcionar un nivel de QoS garantizado, es decir, rutas con un mismo nivel de QoS. El tráfico que este dentro del mismo criterio de nivel de servicio puede ser dirigido hacia esas rutas para obtener un nivel de QoS predecible.

MPLS y ATM usan protocolos de señalización para solicitar un nivel de QoS deseado a otro nodo de red antes de establecer una conexión. Para esto ATM usa el protocolo PNNI (*Private Network-Network Interface*) mientras que MPLS usa el protocolo LDP (*Label Distribution Protocol*) para definir los LSPs (*Label-Switched Path*).

A nivel de capa de red el estándar DiffServ (*Differentiated Services*) define varias clases y mecanismos de QoS que se aplican a los paquetes de acuerdo a su clase de servicio, la clase de servicio o PHB (*Per-Hop Behaviors*) de cada paquete esta determinada por el campo DSCP (*DiffServ Code Point*) localizado en la cabecera IP. El DSCP ocupa el campo TOS (*Type of Service*) que ya no es compatible con DiffServ. Cada nivel de servicio estándar tiene asociado un único DSCP que es usado para determinar como será tratado cada paquete.

La clase de servicio ***Expedited Forwarding DiffServ (EF)*** proporciona una baja latencia y una alta prioridad que es **ideal para VoIP**. Esta clase de servicio se implementa con una alta prioridad de emisión y una baja prioridad de descarte. Cada nodo de red debe asegurar que el tráfico *EF* tendrá un retardo mínimo y perdidas muy bajas.

La clase ***Assured Forwarding DiffServ (AF)*** consiste de cuatro diferentes clases de servicio, cada una con tres diferentes niveles de prioridad y tres diferentes prioridades de descarte, resultando en 12 diferentes valores DSCP. Los enrutadores usan los valores de precedencia de descarte para determinar la prioridad de descarte de los paquetes bajo condiciones de congestión.

La clase ***Class Selector DiffServ (CS)*** puede ser representada por 8 clases de prioridad usando las mismas posiciones de bits del campo de precedencia IP en la definición de TOS, entonces se tienen 8 DSCP numerados del CS0 al CS7, el DSCP CS7 tiene la prioridad mayor de emisión (*forwarding*) mientras que el DSCP CS0 tiene la más baja prioridad de emisión, equivalente a un servicio de mejor esfuerzo (*best effort*), el servicio CS no soporta prioridades de descarte.

La clase ***DEfault DiffServ (DE***) es usada para transportar tráfico *best effort*, cualquier tráfico que no este clasificado dentro de alguna clase de servicio DiffServ será transportado usando un valor de DSCP de 0 teniendo la máxima prioridad de descarte y la mínima prioridad de emisión.

**4.6.2.3 Consistencia de la QoS**

Para mantener el nivel de servicio para una aplicación o servicio, los servicios de QoS deben ser implementados consistentemente a lo largo de toda la red. Las políticas de QoS a nivel de capa de red o IP deben ser mapeadas a las diferentes tecnologías de la capa de enlace, por ejemplo si se utiliza DiffServ para ofrecer QoS los diferentes servicios de calidad (PHBs) deben ser mapeados hacia las tecnologías de la capa de enlace como Ethernet y ATM para proveer un servicio de QoS lo más estable posible de extremo a extremo.

Por ejemplo para mapear los niveles de servicio de DiffServ hacia el estándar 802.1p se puede seguir el siguiente esquema:

| DIFFSERV CODE POINT (DSCP) | PRIORIDAD ETHERNET 802.1P |
|---|---|
| CS7, CS6 | 7 |
| EF, CS5 | 6 |
| AF4, CS4 | 5 |
| AF3, CS3 | 4 |
| AF2, CS2 | 3 |
| AF1, CS1 | 2 |
| DE, CS0 | 0 |

Para mapear DiffServ sobre ATM el siguiente:

| DiffServ Code Point (DSCP) | Categoría de Servicio ATM |
|---|---|
| CS7, CS6, CS5, EF | CBR o rt-VBR |
| AF4, CS4 | rt-VBR |
| AF3, CS3 | |
| AF2, CS2 | nrt-VBR |
| AF1, CS1 | |
| DE, CS0 | UBR |

La implementación de QoS puede ser muy complicada, principalmente por todas las tecnologías, estándares y arquitecturas de red que hay que considerar, además de que no hay una tecnología de QoS que pueda ser aplicada a lo largo de toda la red (en todas las capas del modelo TCP/IP). La dificultad en la preparación de la red para la implementación de VoIP dependerá principalmente del equipo con que se cuente, en algunos casos en que se tengan sistemas que cuenten con herramientas de QoS, con herramientas de administración de ancho de banda, con herramientas de seguridad o con equipos que trabajen en varias capas de red, el proceso será más sencillo. A continuación se describen algunos sistemas y equipos que pueden facilitar considerablemente la implementación exitosa de VoIP.

### 4.6.3 Herramientas de QoS de Nortel Networks

#### 4.6.3.1 *Optivity Policy Services*

Para simplificar la implementación de QoS actualmente existen algunas herramientas que pueden manejar los parámetros de QoS para qué aplicaciones como las de voz y video tengan el ancho de banda que necesitan y cuando lo necesiten, un ejemplo es el *Nortel Networks Optivity Policy Services* (***OPS***). Este sistema permite crear políticas de QoS para optimizar la red para el transporte efectivo de todas las aplicaciones de una manera inteligente, también permite establecer políticas de seguridad para asegurar que solo el tráfico autorizado tenga acceso a la red y limitar o bloquear ciertos tipos de tráfico, como el que se presenta durante un ataque *denial of service* (ataque que satura un servicio).

El sistema Optivity habilita la red para entregar soluciones de voz y datos de una manera confiable, diferenciada, escalable y segura. Esta basado en una aplicación de software diseñada para administrar la priorización del tráfico y la seguridad del acceso a la red, esta constituido por tres elementos, un directorio LDAP, un servidor de políticas y la consola de administración.

Un directorio LDAP (*Lightweight Directory Access Protocol*) se usa para almacenar las políticas, la información de los dispositivos de red administrados y la información requerida por el sistema Optivity.

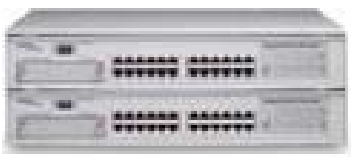
El servidor de políticas se encarga de recopilar toda la información relevante para la administración de la QoS y para la seguridad de la red, se encarga de tomar decisiones basadas en las políticas establecidas por el administrador y comunicarlas a los dispositivos de red encargados de llevar a cabo dichas políticas (*switches*, *routers*, etc). La comunicación entre los servidores de políticas y los dispositivos de red generalmente se lleva a cabo mediante un protocolo de transacción de políticas como el protocolo COPS (*Common Open Policy Service*) o el protocolo CLI (*Command Line Interface*). El objetivo del servidor de políticas es la de asegurar que la petición de una aplicación especifica, de un usuario o de un grupo es valida y de que la aplicación, usuario o grupo reciban el servicio apropiado (ancho de banda, QoS).

La consola de administración es una interfaz grafica de usuario que permite monitorear el sistema de administración de políticas, mediante ella el administrador crea políticas y las asigna a los dispositivos de red que las llevan a cabo.

Los sistemas y equipos que pueden ser administrados por este sistema para proporcionar políticas de QoS y de seguridad están los *switches* BayStack 460-PWR Power-over-Ethernet, los *switches* Baystack 470, los *switches* BayStack Business Policy 2000, y los sistemas Business Communication Manager, BayRS y Passport 8600.

#### 4.6.3.2 BayStack 460-PWR Power-over-Ethernet

Este *switch* cumple con la norma IEEE 802.3af, lo que permite suministrar energía a dispositivos como teléfonos IP, puntos de acceso inalambricos (*wireless access points*), cámaras de red, dispositivos de seguridad y alarmas, y dispositivos de control de acceso. Cuenta con 24 puertos Ethernet 10/100 Mbps, cada uno de los cuales puede proveer energía, y hasta 8 de estos *switches* pueden ser apilados. Adicionalmente cuentan con las mismas características avanzadas del Baystack 470 para brindar QoS, lo que los hace muy útiles para telefonía IP, sobre todo para aquellos teléfonos IP que se requiere que siempre estén disponibles.



*BayStack 460-PWR Power-over-Ethernet*

#### 4.6.3.3 Baystack 470

Los *switches* Baystack 470, permiten una conectividad de hasta 384 puertos Ethernet 10/100 Mbps apilándolos entre si (cada pila es manejada con una sola dirección IP), permiten una actualización de software sencilla, tienen funciones *plug&play*, soporte para VLANs, cuentan con un diseño de apilado que permite sobreponerse a fallos, entre otra muchas funciones, pero lo más importante es que proporcionan servicios de QoS de acuerdo al estándar DiffServ, y proporcionan servicios de seguridad y protección de datos. Estos *switches* clasifican el tráfico IP en la red LAN, lo prioritizan de acuerdo a las políticas definidas y lo marcan con el DSCP (*DiffServ Code Point*) correspondiente basándose en los siguientes parámetros:

- ToS/DSCP
- Dirección IP origen/destino o subredes
- Puertos TCP/UDP origen/destino
- Bits de prioridad 802.1p
- Puerto de ingreso
- Identificación de protocolo (TCP, UDP, IGMP, etc)
- Identificación de VLAN (VLAN ID)

Estos switches tienen la capacidad de leer los paquetes que han sido marcados por otros dispositivos como el *switch* Passport 8600, también soportan técnicas de QoS como *Priority Queuing* y *Weighted Round Robin* (ver capitulo 3). Las políticas pueden ser configuradas mediante una herramienta basada en red o mediante el sistema Optivity.

*Baystack 470*

**4.6.3.4 BayStack Business Policy**

El *switch* BayStack Business Policy (BPS) es un switch Ethernet 10/100 Mbps de 24 puertos que puede ser apilado hasta con otros 7 *switches*, que permite la clasificación y priorización del tráfico de las capas 2/3/4 del modelo OSI, para entregarlo al usuario final. El funcionamiento de este *switch* es prácticamente el mismo que el del Baystack 470, la principal diferencia esta en la característica de seguridad *BaySecure* que permite la autentificación de todos los accesos, no solo de los *switches* para la administración y configuración sino también los accesos de toda la red a través de este *switch*. El software BaySecure limita el acceso solo al personal autorizado mediante la identificación de la dirección MAC, también soporta la autentificación de usuarios mediante RADIUS (*Remote Authentication Dial-In User Service*), mediante el protocolo SNMP (*Single Network Management Protocol*) se proporciona la autentificación de usuarios y encriptación de datos, además este *switch* soporta el protocolo EAP (*Extensible Authentication Protocol*) basado en el estándar IEEE 802.1x que limita el acceso a la red basado en credenciales de usuario, los usuarios tienen que identificarse mediante un nombre de usuario y una contraseña, registradas en un servidor de autentificación.

*BayStack Business Policy*

**4.6.3.5 Passport 8600**

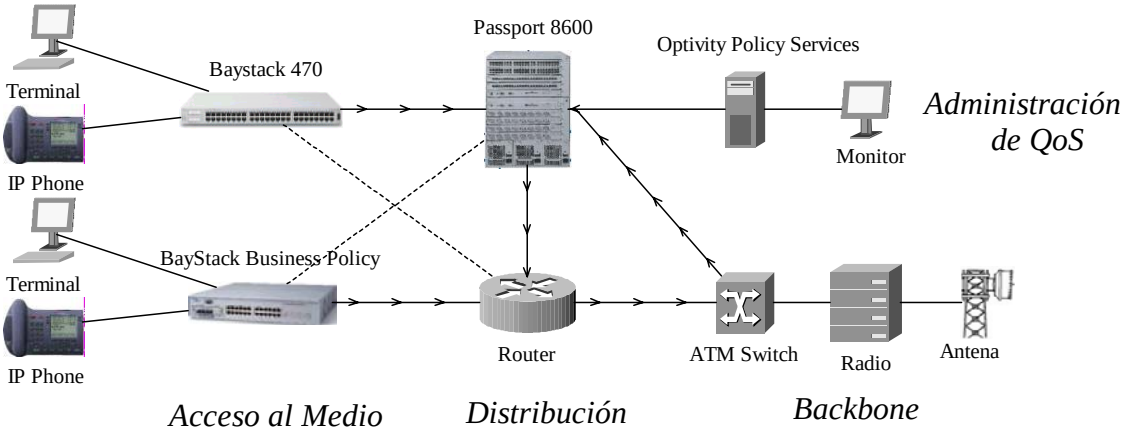
El *switch* Passport 8600 brinda servicios de conmutación de capa 2 y 3 (*switching and routing*) con un desempeño Gigabit Ethernet y brindando calidad de servicio de extremo a extremo (QoS) para las aplicaciones y servicios críticos. El Passport 8600 cuenta con una amplia gama de interfaces que incluyen 10-Gigabit Ethernet, Fast Ethernet, SONET y ATM, lo que permite la conectividad de redes LAN, MAN y WAN en una plataforma integrada, simplificando la complejidad de la topología. Este *switch* puede ser usado para llevar a cabo las funciones de los niveles de distribución y de *backbone* de una red, brindando además servicios para la seguridad e integridad de los datos. Entre los sistemas de seguridad se encuentran políticas de acceso, *passwords*, protocolos de seguridad, filtrado de direcciones y puertos, políticas de enrutamiento,

mecanismos de prevención de ataques DoS (*Denial of Service*). Además este *switch* integra funciones de *firewall*, soporte para VPNs, un sistema de detección de intrusiones, permite el balanceo de carga por rutas de igual costo y cuenta con mecanismos para evitar problemas de convergencia tipo *Spanning Tree*. Para brindar los servicios de QoS el Passport 8600 utiliza funciones de filtrado, basadas en hardware, de niveles 2,3 y 4, soportando clases de servicios (CoS) IEEE 802.1p y servicios IETF DiffServ

*Passport 8600*

**4.6.3.6 Topología de Red con QoS de Nortel Networks**

A continuación se muestra un esquema en donde se representa como se podría llevar a cabo la implementación de políticas de QoS en una red de PEMEX de extremo a extremo.




*Topología de Red con QoS de Nortel Networks*

En este modelo se pueden apreciar claramente las capas del modelo jerárquico para redes de datos, en la capa de acceso se usan los *switches* BayStack 460 y 470 para interconectar computadoras, teléfonos IP y otros dispositivos de red brindando servicios de clasificación, marcado y priorización de paquetes, en la capa de distribución se pueden utilizar enrutadores configurados adecuadamente con las políticas de QoS o se puede usar el *switch* multicapa Passport 8600 que brinda servicios de enrutamiento y funcionalidades avanzadas de seguridad y de QoS, mientras que en la capa de *backbone* el *switch* ATM sirve para brindar los servicios de QoS, de tal manera que el tráfico de VoIP y el de aplicaciones criticas este garantizado a lo largo de toda la red.

En este esquema las políticas de QoS son implementadas y administradas de una manera sencilla y de manera remota, desde cualquier computadora de la red, mediante el servidor Optivity Policy Services, que puede facilitar considerablemente la preparación de la red para el transporte de VoIP y de aplicaciones multimedia, lo que hace sencilla la administración, la configuración y funcionamiento del modelo mostrado.

Las características de estos *switches* permiten obtener un desempeño óptimo de la red y facilitan que las funciones de las capas de *backbone*, de distribución y de acceso al medio se lleven a cabo efectivamente, lo que asegura que los nuevos sistemas y servicios se integren efectivamente a la red y sin afectar su desempeño.

**4.6.4 Herramientas de QoS de Cisco**

#### 4.6.4.1 AutoQoS

Mediante el software Cisco IOS, Cisco ofrece un conjunto de herramientas para QoS para satisfacer los requerimientos de aplicaciones de voz, video y datos. Una de estas herramientas es Cisco AutoQoS que permite simplificar la implementación de QoS. Mediante una interfaz de líneas de comandos el administrador de la red puede implementar políticas de QoS en la red LAN y/o WAN de una manera prácticamente automática en los *switches* y *routers* Cisco, con esta herramienta se puede implementar QoS sin tener un conocimiento extensivo de las tecnologías de transporte (PPP, SDH, ATM, etc.), ni de los mecanismos de la capa de enlace necesarios para asegurar la calidad de la voz y reducir la latencia, el *jitter* y la perdida de paquetes.

A nivel WAN AutoQoS:

- Soporta Frame Relay, ATM, PPP, HDLC
- Automáticamente clasifica los paquetes RTP (*Real-Time Transport Protocol*) y los paquetes de control (H.323, SIP, MGCP)
- Crea políticas de QoS modulares en el software Cisco IOS.
- Proporciona encolamiento de baja latencia para tráfico de VoIP
- Proporciona garantías mínimas de ancho de banda (*Weighted Fair Queuing*) para el tráfico de control VoIP
- Habilita políticas de *shaping* de tráfico (ajuste de velocidades de transmisión).
- Habilita mecanismos de fragmentación e intercalado de paquetes y compresión de encabezados RTP (cRTP) donde sea necesario
- Proporciona alertas SNMP y SYSLOG para la pérdida de paquetes.

A nivel LAN AutoQoS permite:

- Reforzar los límites de seguridad de los teléfonos IP y de los puertos de acceso de los *switches* Cisco Catalyst.
- Habilitar colas de prioridad estrictas y colas *weighted round robin* (ver capitulo 3) en los switches Catalyst para voz y datos donde sea necesario.
- Modificar los criterios de admisión a las colas.
- Modificar el tamaño de las colas, como se requiera.
- Modificar los mapeos CoS-DSCP, IP precedence-DSCP.

AutoQoS permite implementar QoS para una red convergente de una manera mucho más rápida y más eficiente. Usando AutoQoS el tráfico de VoIP recibe políticas de QoS apropiadas de una manera automática. Para brindar servicios de QoS de extremo a extremo.

Cisco usa los *switches* Catalyst que soportan el software Cisco IOS, que proporcionan funciones avanzadas de QoS y realizan funciones de conmutación en varias capas de red, estas características pueden ser muy útiles para la implementación de VoIP. El *switch* Catalyst 6500 con la tarjeta PFC (*Policy Feature Card*) puede clasificar el tráfico de a cuerdo a la clase de servicio CoS (*Class of Service*), precedencia IP o por el DSCP, el *switch* Catalyst 4006 con Supervisor III y el Catalyst 3550 también proporcionan características avanzadas de QoS, la diferencia principal de estos *switches* son la capacidad de conmutación y la modularidad. Estos *switches* forman la base de la arquitectura AVVID (*Architecture for Voice, Video and Integrated Data*).

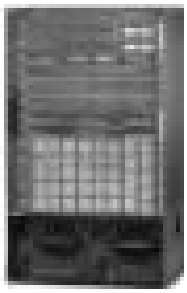
#### 4.6.4.2 Catalyst 6500

El *switch* Catalyst 6500 esta diseñado para permitir la convergencia de redes LAN, MAN y WAN al integrar una gran variedad de interfaces LAN y WAN que van desde Ethernet 10/100 Mbps Base TX hasta Ethernet 10 Gigabit e interfaces para OC12 para ATM y al realizar funciones de conmutación de capa 2 (*switching*) y de capa 3 (*routing*). Este *switch* soporta los estándares Ethernet y protocolos de enrutamiento soportados por los switches y enrutadores Cisco.

Este *switch* proporciona servicios avanzados de extremo a extremo para proporcionar QoS, servicios de manejo de ancho de banda y servicios de seguridad, que permiten la integración efectiva y segura de servicios de voz, datos y multimedia mediante una topología de red simplificada más fácil de administrar. Estas características lo hacen ideal para la implementación de VoIP, de servicios de multimedia y para asegurar aplicaciones criticas de datos.

Este *switch* puede ser escalado desde 48 hasta 576 puertos Ethernet 10/100 Mbps, que pueden ser habilitados para proporcionar energía a teléfonos IP por ejemplo. El *switch* multicapa Catalyst 6500 cuenta con un módulo que brinda servicios de *firewall*, un módulo de detección de intrusiones, un módulo para implementar redes privadas virtuales (VPNs), un módulo de conmutación de contenido y un módulo de análisis de red que le permiten implementar las políticas de red que pueden ser aplicadas de extremo a extremo basándose en información de capas 2,3 y 4, como pueden ser un usuarios especifico, direcciones IP o aplicaciones. Entre las técnicas y estándares de QoS que implementa este *switch* están las siguientes:

- Detección y clasificación de precedencia IP
- 802.1Q/802.1p
- DiffServ
- Políticas de ancho de banda
- Mecanismos de prevención de congestiones (*Congestion Avoidance*, WRED)
- Programación de tráfico (*Traffic Scheduling, Weigthed Round Robin* por puerto)
- COPS/RSVP



Catalyst 6500

**4.6.4.3 Catalyst 4006 con Supervisor III**

Este *switch* de hasta 240 puertos, proporciona capacidades de conmutación de capa 2,3 y 4 y es una muy buena opción para la implementación de servicios basados en red en una red LAN o MAN, y puede funcionar como *backbone* para una red LAN o también puede brindar servicios de distribución de capa 3 para redes más grandes, este modelo en particular ofrece servicios de manejo de ancho de banda y de calidad de servicios avanzados así como servicios de voz opcionales que pueden ser muy útiles para la implementación de VoIP. Entre las características más importantes de este *switch* están las siguientes:

- Soporte para VLANs
- Enrutamiento estático
- Soporte para los protocolos de enrutamiento más comunes (IGRP, EIGRP, OSPF, RIP, BGP)
- Configuración de QoS por puerto
- Soporte para colas estrictas de prioridad
- Clasificación y marcado de paquetes basados en IP ToS o DSCP
- Clasificación y marcado de paquetes basados en los encabezados de capa 3 y capa 4

**4.6.4.4 Catalyst 3550**

Este es un *switch* multicapa brinda una alta disponibilidad, seguridad y calidad de servicios (QoS) y puede funcionar en la capa de acceso para redes medianas o como *backbone* para redes pequeñas. Este *switch* permite brindar servicios inteligentes a lo largo de toda la red como son políticas de QoS, listas de control de acceso, administración de ancho de banda y enrutamiento IP de alto desempeño, manteniendo la simplicidad

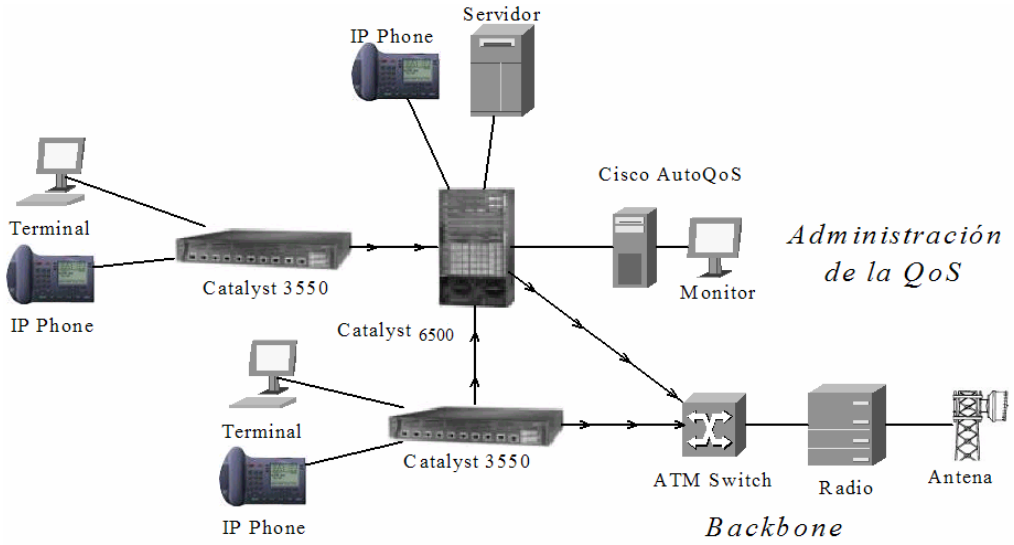
de una red LAN pero brindando servicios de red WAN. El modelo 3550-24 PWR adicionalmente puede brindar el suministro de energía a teléfonos IP y a *wireless access points*. Entre sus características principales están las siguientes:

- Soporte de enrutamiento estático y de los protocolos de enrutamiento RIP, OSPF, IGRP, EIGRP, BGP
- Soporte y enrutamiento de VLANs
- Mecanismos para sobreponerse a fallos rápidamente
- Administración de tráfico
- Herramientas de seguridad como autentificación de usuarios y dispositivos, y encriptación
- QoS basada en los estándares 802.1p CoS y DiffServ
- Mecanismos para evitar congestiones como WRED

Catalyst 3550

**4.6.4.5 Topología de Red con QoS de Cisco**

A continuación se muestra un esquema de una topología de red usando equipo cisco para implementar QoS de extremo a extremo.




*Topología de Red con QoS de Cisco*

En este esquema no se pueden apreciar claramente las capas del modelo jerárquico, sin embargo sus funciones se llevan a cabo mediante una topología simplificada por la utilización de *switches* multicapa que realizan las tareas de la capa de acceso al medio y de distribución, brindando además servicios de seguridad y de QoS de extremo a extremo. La administración de las políticas de QoS también se realiza de una manera simplificada y remota mediante la herramienta AutoQoS que permite asegurar la consistencia de la políticas de QoS a los largo de toda la red. En este esquema se pueden observar algunas ventajas de usar *switches* multicapa, por ejemplo el *switch* Catalyst 6500 por su mayor capacidad, puede ser usado para interconectar teléfonos IP, computadoras, servidores, *switches*, enrutadores y *switches* ATM, lo que permite una integración de la red LAN con la red WAN, en un entorno seguro y fácil de administrar.

**4.6.5 Planeación de la Capacidad**

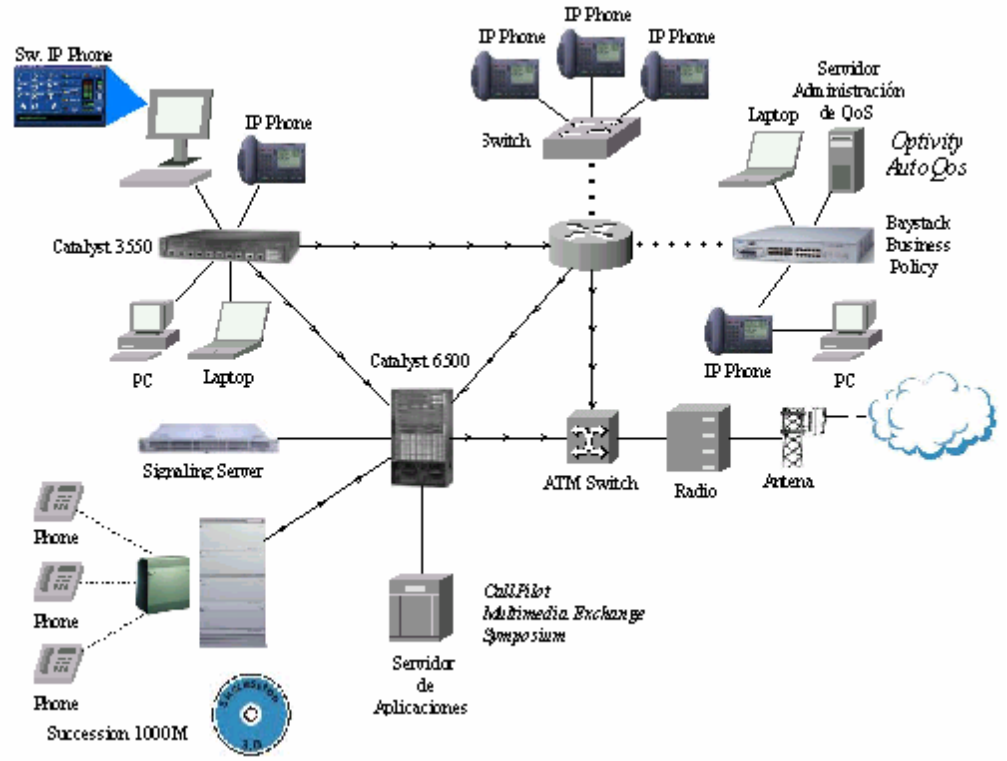
Debido a que este es un ejemplo hipotético y por cuestiones de privacidad de la información del tráfico y protocolos que manejan las redes de PEMEX, en este caso no se realizó un estudio para definir la planeación de la capacidad del sistema.

Para realizar esta se recomienda realizar un estudio riguroso del tráfico que deberá ser soportado por la nueva infraestructura convergente de comunicaciones y considerar las recomendaciones al respecto hechas por la guía de diseño aquí propuesta, principalmente en lo que respecta a la recomendación de no sobrepasar el 80% de la capacidad de los enlaces.

En caso de que no se pueda realizar un estudio de tráfico por alguna circunstancia y partiendo de que en esta implementación se aprovechara la infraestructura del antiguo sistema telefónico, se puede partir del antiguo esquema y realizar los cambios necesarios conforme se realizan las pruebas del sistema, tratando de aprovechar los enlaces WAN de la antigua red de conmutación de circuitos para transportar las llamadas de VoIP.

### 4.6.6 Topología de una Red VoIP para la Zona Marina

A continuación se muestra el esquema de una topología de una red IP propuesta que implementa VoIP brindando servicios de QoS de extremo a extremo, mediante un sistema simplificado para establecer y administrar las políticas de QoS y de seguridad, y que puede ser apropiado para las instalaciones de la zona marina de PEMEX.




*Topología de una Red VoIP para la Zona Marina*

La estrategia de migración a VoIP que se propone para las instalaciones de la zona marina de PEMEX es la de convertir los conmutadores Meridian 1 al sistema Succession 1000M mediante la actualización al software Succession 3.0 y la agregación de servidores de señalización. Esta opción es la que brinda mayores ventajas para los usuarios de la telefonía IP y que permite una migración tan rápida como se requiera, al permitir la subsistencia de los teléfonos y servicios del conmutador Meridian 1 así como la intercomunicación efectiva entre estos y los teléfonos IP. Esta opción protege la inversión en el sistema telefónico conmutado a la vez

que permite hacer uso de todas las ventajas de VoIP, por lo cual resulta una solución económica y efectiva para el cliente.

En este ejemplo se propone, para asegurar la calidad de voz del sistema, una topología de red que brinda calidad de servicio (QoS) de extremo a extremo mediante una topología simplificada y un sistema de implementación y administración de políticas de QoS que simplifica drásticamente la tarea de preparar la red de datos para la integración de servicios de voz y multimedia, que brinda mecanismos eficientes de seguridad y que asegura las recomendaciones de diseño técnico revisadas anteriormente. Para esto se integra un servidor encargado de la implementación y administración de políticas de red y de la administración del sistema Succession 1000M, este servidor puede incluir el sistema Optivity y/o el sistema AutoQoS dependiendo de si se usan *switches* de Nortel Networks, de Cisco o de ambos, mientras que para administrar la red telefónica se usara el sistema OTS (*Optivity Telephony Manager*).

Para satisfacer los objetivos del sistema se propone la integración de uno o varios servidores de servicios para telefonía, que incluyan a los sistemas CallPilot, Symposium y Multimedia Exchange para brindar los servicios suplementarios y de multimedia a los usuarios de VoIP, y también para los usuarios de telefonía de conmutación de circuitos. Este o estos servidores se encargaran de brindar los servicios de mensajería unificada, centro de llamadas y las aplicaciones telefónicas multimedia avanzadas para usuarios de VoIP.

En este ejemplo el sistema Succession 1000M se conecta a un *switch* Catalyst 6500, así como también el servidor de señalización, este sistema podría localizarse en cualquier parte de la red, pero se eligió este *switch* por su capacidad de procesamiento de paquetes y porque brinda conmutación de capa 2 y capa 3 brindando funciones de acceso al medio y de distribución mediante una topología simplificada, al mismo tiempo que brinda servicios de seguridad y de QoS. A este *switch* también se conectan el o los servidores de aplicaciones, que deben responder a los clientes lo antes posible, con este *switch* se busca lograr un mayor desempeño del sistema, evitando posibles cuellos de botella. Estos equipos pueden localizarse en el mismo cuarto de telecomunicaciones del antiguo sistema telefónico o pueden ubicarse en algún otro y conectarse mediante una interfaz Ethernet o de RDSI. Una opción al *switch* Catalyst 6500 es el *switch* Passport 8600 que tiene funciones y capacidades similares o algún otro que desempeñe funciones de conmutación multicapa y que implemente funciones de seguridad y QoS de extremo a extremo.

Para brindar los servicios de acceso al medio se recomienda que también se empleen *switches* multicapa que brinden servicios de seguridad y de QoS consistentes a los de las capas de distribución y *backbone*, en este caso se utiliza el *switch* Catalyst 3550 para ejemplificar. Este *switch* realiza funciones de conmutación de capa 2 y capa 3, y permite clasificar, marcar y dar prioridad a los paquetes de VoIP o de aplicaciones críticas, proporcionando un manejo del ancho de banda más efectivo al evitar la necesidad de redirigir el tráfico hacia otro dispositivo para realizar labores de enrutamiento. Adicionalmente este tipo de *switches* pueden ser empleados para suministrar la energía (alimentación) a los teléfonos IP a través del cable UTP.

Otra opción es usar *switches* como el Baystack Business Policy que aunque no realiza funciones de enrutamiento si brindan las funciones de seguridad y de QoS requeridas, clasificando, marcando y priorizando el tráfico consistentemente de tal manera que se puedan conectar todo tipo de elementos de red, como computadoras, servidores, teléfonos IP, etc., sin que se afecte el desempeño de las aplicaciones criticas o de las aplicaciones en tiempo real, ya que si se requiere que dichos paquetes tengan que ser enrutados, este *switch* los marca apropiadamente para que sean tratados con el nivel de prioridad correspondiente en el enrutador. Para suministrar energía a los teléfonos IP se puede utilizar el switch BayStack 460-PWR Power over-Ethernet que también proporciona servicios de QoS.

Otra opción es usar un *switch* convencional para interconectar únicamente teléfonos IP (no computadoras), de tal manera que el ancho de banda no pueda ser acaparado por otros equipos de red como computadoras o servidores que pudieran usar paquetes de gran tamaño, esta opción no es tan efectiva como la de los casos anteriores por no implementar funciones de seguridad y de QoS, sin embargo en una red jerárquica que implemente políticas de distribución y de *backbone* adecuados (en los enrutadores y *switch* ATM para este caso) esta es una buena solución.

Como se puede observar en el esquema, la interconexión de equipo de diferentes fabricantes es posible por el uso de los mismos estándares de comunicaciones, de QoS y de interfaces de interconexión, por lo cual se puede elegir libremente el equipo de red a utilizarse sin estar atado a un determinado fabricante.
Respecto a los teléfonos IP, estos se pueden agregar de varias maneras, una es mediante teléfonos IP de escritorio que se conectan directamente a un nodo de red mediante un conector RJ-45, otra forma es que compartan un nodo de red con una computadora mediante el *switch* que tienen integrado estos teléfonos IP de escritorio, otra forma es mediante teléfonos por software, que se instalan en computadoras multimedia (con bocina y micrófono) y que funcionan como clientes de los servidores de servicios. Esta última opción es la que permite disfrutar de los beneficios del sistema *Multimedia Exchange* y son los más fáciles de implementar al no requerir la instalación de nuevo equipo.

### 4.7 Análisis Financiero

Con esta implementación se busca proteger las inversiones realizadas en el sistema Meridian, tanto en el conmutador como en los servidores de servicios y en los teléfonos, a la vez que se busca brindar todas las ventajas de VoIP de una manera económica y efectiva. Al aprovechar toda la infraestructura del sistema Meridian, en su migración al sistema Succession 1000M, para la implementación de VoIP se obtienen grandes ahorros respecto a otras soluciones, que implicarían la adquisición de una IP PBX y de *gateways* para interconectar el sistema telefónico de VoIP con el de conmutación de circuitos. Esta opción permite una migración suave y tan rápida como se requiera, al permitir que los dos sistemas convivan transparentemente, de tal manera que el costo a una implementación puramente IP se puede ir distribuyendo a lo largo del tiempo.

Otros ahorros considerables se obtendrían al no ser necesario que el personal encargado de la administración del sistema reciba capacitación extra para la configuración y mantenimiento de algunos sistemas, ya que los sistemas del conmutador Meridian se mantienen igual en el nuevo sistema Succession 1000M, como el de mensajería unificada y el sistema de administración OTS, que es común para los sistemas Meridian 1 y Succession. Esto permite que tampoco los usuarios requieran capacitación para usar los servicios que les brindaba el sistema Meridian. Además como se explico anteriormente el uso del sistema OTS puede ahorrar hasta un 90% del esfuerzo para configurar el sistema Succession cuando se realiza la migración desde el sistema Meridian, lo cual también representa ahorros considerables.

Otra ventaja de esta opción son los teléfonos IP de escritorio, que incluyen un *switch* y que no requieren un nodo de red nuevo, ya que lo pueden compartir con otro equipo, esto representa ahorros económicos al evitar la costosa necesidad de instalar nuevo cableado. Además los teléfonos IP de software se pueden integrar fácilmente a cualquier equipo multimedia que tenga conexión a la red, por lo que el personal puede hacer uso del sistema sin la necesidad de adquirir un aparato telefónico.

Todo lo anterior garantiza que esta sea la opción de implementación más económica y efectiva para la implementación de esta tecnología en la zona marina.

Adicionalmente el precio de implementación de este sistema podría ser cubierto por los ahorros que se obtendrían por conceptos de administración y mantenimiento de la nueva red, y por el uso de las nuevas herramientas de comunicación, que en muchos casos permitirían ahorrar recursos al evitar traslados de personal para realizar juntas o tomar decisiones importantes, además de que el uso de este tipo de tecnología permitiría incrementar la productividad del personal.

### 4.8 Implementación y Pruebas

Antes de instalar el equipo y sistemas de VoIP es conveniente que se realicen pruebas a la infraestructura de red para comprobar que esta cumple con los requerimientos técnicos y de QoS requeridos.

Esta implementación requiere que el software del conmutador Meridian sea actualizado, por lo tanto el servicio telefónico tendrá que ser suspendido por lo menos el tiempo que lleve dicha actualización, por lo tanto es necesario planificar adecuadamente el momento de dicha actualización de tal manera que los usuarios

sean afectados lo menos posible, una vez que concluya la actualización, los usuarios de la red de conmutación de circuitos podrán seguir haciendo uso de la misma y puede empezar el proceso de implementación de VoIP

Una vez que se halla actualizado con éxito el software del sistema Meridian y que se haya instalado el servidor de señalización se recomienda realizar pruebas de este sistema básico mediante un pequeño grupo de teléfonos IP, de escritorio y de software, de tal manera que se pueda reportar la calidad de la voz del sistema, esto permitirá hacer los ajustes necesarios en la configuración inicial del sistema. El siguiente paso seria instalar y configurar los servidores de servicios y realizar las pruebas correspondientes con el mismo grupo de teléfonos IP, reportando de igual manera la calidad de dichos servicios.

Una vez que se haya asegurado que los usuarios de la red telefónica de conmutación de circuitos y los usuarios de VoIP de prueba se puedan comunicar efectivamente y que los servicios suplementarios y multimedia funcionan correctamente, se puede empezar a integrar al resto de los usuarios de VoIP, para después realizar las pruebas con todos los usuarios y realizar los ajustes necesarios mediante el sistema de administración OTS.

# Conclusiones

La evolución digital de las redes telefónicas de conmutación de circuitos ha permitido que estas actualmente se extiendan por todo el mundo para brindar servicios de comunicaciones de voz de gran calidad y de una manera prácticamente instantánea. La naturaleza del funcionamiento de este sistema requiere que se establezcan circuitos o rutas fijas entre los usuarios antes de que puedan iniciar una conversación. Estos circuitos son mantenidos mientras dura la llamada y no pueden ser compartidos por otros usuarios, asegurando la calidad de la voz transmitida pero también desperdiciando más de la mitad del ancho de banda, ya que las comunicaciones de voz requieren que un usuario hable mientras el otro escucha y viceversa, por lo que dichos circuitos se tienen inutilizados más de la mitad del tiempo.

La tecnología e infraestructura requerida para soportar la gran cantidad de usuarios de telefonía a nivel mundial resulta muy costosa y difícil de mantener, debido a cuestiones como la interconexión de las redes de diferentes países (que emplean una gran variedad de tecnologías y diversos medios de transmisión), la instalación del cableado (que tiene que cubrir grandes distancias y cuya instalación esta sujeta a estrictas reglamentaciones), el costo del mantenimiento y administración de los conmutadores y de las redes de transporte, y el pago de impuestos que tienen que hacer los usuarios por llamadas internacionales de larga distancia (ya que cada país cobra cuotas para permitir que dichas llamadas pasen por su infraestructura de red).

Es por lo anterior que durante los últimos años se han buscado alternativas más económicas y eficientes para brindar los servicios de comunicación de voz. De esta búsqueda surge la idea de transportar las llamadas de voz a través de redes de conmutación de paquetes. Dichas redes no requieren que se reserven circuitos para que se pueda llevar a cabo una comunicación, la información es segmentada en paquetes que contienen elementos de identificación o encabezados que permiten que en cada punto de la red que van atravesando se reconozca su origen y su destino y puedan ser encaminados o dirigidos hacia sus destinos por los dispositivos destinados para eso. Entonces los paquetes son enviados sin tener definida una ruta, lo que significa que pueden seguir diferentes rutas hacia su destino dependiendo de la condiciones de la red y que en el destino los paquetes tengan que ser reordenados y después reensamblados para recuperar la información.

Estas redes permiten hacer un mejor uso del ancho de banda ya que este es compartido por varios usuarios simultáneamente, sin embargo tienen el inconveniente para las aplicaciones en tiempo real, como la telefonía, de producir retardos de tránsito variables y de que los paquetes no siempre llegan a su destino en el mismo orden en que fueron enviados y/o que se produzcan perdidas de paquetes bajo condiciones de saturación en los enlaces.

Sin embargo el crecimiento y la fuerte implantación de las redes IP a nivel mundial, el desarrollo de técnicas avanzadas de digitalización de voz, mecanismos de control y priorización de tráfico, protocolos de transmisión en tiempo real, asi como la implementación comercial de estandares que permiten la calidad de servicio **QoS** en redes IP, han creado un entorno donde es posible transportar la voz sobre redes de conmutación de paquetes, principalmente sobre redes IP (en contraposición con la forma tradicional de transportar datos sobre redes de voz), dando origen a lo que se conoce como voz sobre IP o VoIP.

Las redes IP fueron creadas para permitir la comunicación entre sistemas y redes que emplean diferentes tecnologías, diferentes protocolos de comunicación y diferentes medios de transmisión. Debido a esta característica, y por el inmenso desarrollo de Internet, se ha elegido al protocolo IP como el protocolo universal de comunicaciones para las redes de datos, ya que soporta una gran variedad de servicios, como el transporte de datos, de audio y de video. En este contexto la telefonía puede ser considerada como un servicio más de la redes IP.

Existen otras alternativas a VoIP, como lo son VoFR (*Voice over Frame Relay*) y VoATM (*Voice over* ATM) que son tecnologías de capa 2 del modelo OSI, mientras que VoIP es una tecnología de capa 3 (y por lo tanto puede ser transportada por tecnologías de capa 2 como FR y ATM). VoIP se prefiere sobre VoFR y VoATM por su capacidad de interconexión con otras aplicaciones de voz o multimedia. VoFR y VoATM son buenas

tecnologías de transporte a nivel WAN, usualmente manejan un mayor ancho de banda que VoIP pero tienen la desventaja de que no pueden ser implementadas sobre redes LAN o hasta el usuario final, es por esto que VoIP es la forma de voz sobre paquetes que predomina actualmente y es la única opción cuando se requiere una implementación híbrida (interconexión con PBXs).

Actualmente se dispone de productos comerciales de alta calidad que permiten la implementación de sistemas telefónicos basados en IP, con una calidad similar a la proporcionada por las redes telefónicas conmutadas (RTC). Esta gran calidad telefónica que actualmente se puede lograr sobre redes IP ha sido uno de los avances principales que conducen a la convergencia de las redes de voz, vídeo, y de datos (una sola infraestructura para todos los servicios de comunicaciones).

Utilizar VoIP significa obtener grandes ahorros económicos al integrar dos infraestructuras de comunicación, de voz y datos, en una sola con una mejor escalabilidad y de más fácil mantenimiento, pero sobre todo significa la incorporación de nuevos servicios que integran voz y datos y que permiten a los usuarios tener mejores herramientas de comunicación.

El concepto de VoIP es relativamente simple, se trata de transformar la voz en paquetes de información manejables por una red IP. Básicamente una llamada de VoIP debe pasar por las siguientes etapas:

- Digitalización de la señal de audio o voz.
- Estimación de los niveles de energía de cada trama para que un detector de silencio decida si el bloque debe ser tratado como silencio o como parte de una conversación.
- Compresión de acuerdo a un algoritmo específico y encapsulado de las tramas de acuerdo al protocolo IP
- Transferencia a través de una red IP hasta el destino de la llamada.
- Decodificación en el destino de la señal de audio utilizando el mismo algoritmo empleado para la codificación.
- Conversión digital-analógica en el dispositivo de salida y entrega de la señal de audio a través de un auricular o bocina.

Los componentes principales de una red de VoIP son muy similares en funcionalidad a los de una red con conmutadores de circuitos. Las redes de VoIP deben realizar las mismas tareas que hace una RTC, además de realizar una función de interconexión (*gateway)* a la red telefónica existente. Además se requieren dispositivos que se encarguen del control de las llamadas (*gatekeeper/proxy*) y de garantizar la QoS. Aunque se usan diversas tecnologías y acercamientos, algunos de los mismos conceptos que constituyen la RTPC también crean las redes de VoIP.

Esta tecnología provee de poderosas herramientas de comunicación que permitirán a sus usuarios estar comunicados de una manera más efectiva y oportuna, sin importar en que parte del mundo se localicen. Esta tecnología permitirá a los usuarios colaborar en la toma de decisiones o en la elaboración de proyectos de una manera remota y efectiva, con aplicaciones de videoconferencias, con aplicaciones para compartir información y documentos en tiempo real, y otras aplicaciones que definitivamente impactaran en la productividad de los usuarios al ahorrar tiempo, dinero y esfuerzo al evitar la necesidad de viajar para solucionar ciertos problemas.

**Resultados**

El objetivo principal de esta tesis es la de servir de referencia para llevar a cabo la implementación exitosa de esta tecnología en las redes de telecomunicaciones de PEMEX, para esto se requiere tener una idea clara del funcionamiento de las tecnología involucradas por parte de los diseñadores. Para esto en el capitulo 1 se hace una revisión de las redes telefónicas de conmutación de circuitos actuales, en el capitulo 2 se hace un repaso de los aspectos más relevantes del funcionamiento de las redes IP y se describen los fundamentos de la QoS para estas redes, en el capitulo 3 se describen los fundamentos de VoIP y se analizan aspectos que son determinantes para asegurar la calidad de sus servicios, finalmente en el capitulo 4 se plantea una guía de diseño para este tipo de sistemas y se presenta un ejemplo practico, con lo cual se cumple con los objetivos planteados.

La meta para los diseñadores de redes de VoIP debe ser agregar las capacidades de las redes telefónicas conmutadas (transferencia de voz, señalización y servicios suplementarios) a las redes IP e interconectar éstos a la red telefónica pública y a las redes de voz privadas de tal manera que se mantengan los estándares de calidad actuales de la voz y se preserve las características que cada uno espera del teléfono, a la vez que se agregan nuevos servicios y sistemas orientados a incrementar la productividad de los usuarios.

Para esto la red IP debe asegurar criterios mínimos de funcionamiento incluyendo la minimización del rechazo de llamada, de los retardos de la red, de la pérdida de paquetes, y de la desconexión. Esto es requerido incluso durante condiciones de congestión o cuando múltiples usuarios deben compartir recursos de la red. El control de la llamada (señalización) debe hacer la llamada telefónica transparente de modo que los usuarios no necesiten saber que tecnología es la que implementa el servicio.

La primera etapa para la implementación exitosa de VoIP es preparar la infraestructura de red para el tráfico en tiempo real, como la voz, esta etapa se refiere básicamente a asegurar el transporte seguro y eficaz de las llamadas de voz, tanto en la red de datos como en la RTC, de tal manera que los usuarios tengan servicios de voz dentro y fuera de la red de VoIP. Una segunda etapa se refiere a la integración de teléfonos IP, aplicaciones de voz para computadoras y aplicaciones basadas en red que integran voz y datos. Las dos etapas pueden llevarse a cabo simultáneamente, pero **la preparación de la infraestructura de la red IP es la clave del proceso de planeación para asegurar la implementación exitosa de VoIP**.

Para lograr lo anterior la presente tesis sugiere una guía de diseño que esta basada en las recomendaciones de expertos de Cisco y Nortel Networks. Esta guía revisa los aspectos que deben ser considerados para evolucionar una red exclusiva de datos hacia una infraestructura de red multiservicio que pueda incluir tráfico de datos, voz y video, principalmente la integración de las redes de datos y telefónica. Este enfoque comienza con una evaluación de la red actual, entonces se fijan objetivos y metas, se evalúan las tecnologías disponibles, se hacen las consideraciones de diseño técnico para el soporte de comunicaciones en tiempo real, se realiza un análisis financiero y por último se realiza la planificación para la implementación y las pruebas del sistema.

Las recomendaciones de diseño técnico se pueden resumir como sigue:

- Asegurar un modelo jerárquico para la red de datos.
- Implementación de técnicas de calidad de servicio (QoS) consistentes a lo largo que toda la red para minimizar los componentes del retardo.
- Balanceo entre la calidad de la voz, el retardo y el ancho de banda.
- Ajuste de los parámetros para mantener el retardo y el *jitter* por debajo del umbral permitido.
- Planificación de la capacidad y ancho de banda requerido para el tráfico esperado en la red e implementación de técnicas de control de admisión de llamadas.

Una característica esencial en el diseño de la red IP es la de asegurar que la topología de la red este basada en un modelo jerárquico que permita la modularidad, es decir, que permita crear modelos de diseño (módulos) que puedan ser repetidos o modificados conforme crece la red, de tal manera que el costo y complejidad de hacer una actualización en la red quede restringido a una pequeña porción de toda la red. El aislamiento de fallos también es facilitado por este modelo al modular la red en elementos pequeños, fáciles de entender, que ayudan a identificar los puntos de fallo.

Este modelo incluye tres capas:

- El *backbone* (*core*) o médula de la red que proporciona un servicio de transporte óptimo entre sitios.
- La capa de distribución que proporciona una conectividad basada en políticas.
- La capa de acceso que es la que proporciona acceso a la red a los usuarios.

Como reglas generales **se recomienda que en el diseño de la capacidad de la red VoIP no se exceda el 80% de la capacidad en los enlaces seriales**, esto debido principalmente a la existencia de *overheads* invisibles y posibles problemas de sincronización, también hay que **asegurar que el retardo no sobrepase los 150 ms**, y de preferencia **emplear sistemas detectores de silencios y supresores de eco**.

Para mantener el nivel de servicio para una aplicación o servicio, los servicios de QoS deben ser implementados consistentemente a lo largo de toda la red. Las políticas de QoS a nivel de capa de red o IP deben ser mapeadas a las diferentes tecnologías de la capa de enlace, por ejemplo si se utiliza DiffServ para ofrecer QoS los diferentes servicios de calidad deben ser mapeados hacia las tecnologías de la capa de enlace como Ethernet y ATM para proveer un servicio de QoS lo más estable posible de extremo a extremo.

La implementación de la QoS puede ser muy complicada, principalmente por todas las tecnologías, estándares y arquitecturas de red que hay que considerar. La dificultad en la preparación de la red para la implementación de VoIP depende principalmente del equipo con que se cuente, en algunos casos en que se tienen sistemas que cuenten con herramientas de QoS, con herramientas de administración de ancho de banda, con herramientas de seguridad y/o que trabajan en varias capas de red, el proceso es más sencillo.

Para simplificar la implementación de QoS actualmente existen algunas herramientas que pueden manejar los parámetros de QoS para qué aplicaciones como las de voz y video tengan el ancho de banda que necesitan y cuando lo necesiten, un ejemplo es el *Nortel Networks Optivity Policy Services* (***OPS***). Este sistema permite crear políticas de QoS para optimizar la red para el transporte efectivo de todas las aplicaciones de una manera inteligente, también permite establecer políticas de seguridad para asegurar que solo el tráfico autorizado tenga acceso a la red y limitar o bloquear ciertos tipos de tráfico, como el que se presenta durante un ataque *denial of service* (ataque que satura un servicio). Mediante el software Cisco IOS, Cisco ofrece un conjunto de herramientas para QoS para satisfacer los requerimientos de aplicaciones de voz, video y datos. Una de estas herramientas es Cisco AutoQoS que permite simplificar la implementación de QoS

Las redes de PEMEX usualmente estas integradas por equipos y sistemas de diferentes fabricantes, además la administración de dichos sistemas se realiza de una manera centralizada y remota, lo cual las hace redes difíciles de mantener y administrar. Para facilitar la implementación de VoIP y garantizar el cumplimiento de los estándares de calidad de los sistemas telefónicos y de datos, en la presente tesis se proponen varios equipos o sistemas, cuyas características pueden ser muy útiles para estos fines, y adicionalmente se presenta un ejemplo de aplicación de la guía de diseño propuesta para la zona marina de PEMEX, que comprende instalaciones y plataformas marinas localizadas en los estados de Campeche, Yucatán y Tabasco.

A nivel WAN las instalaciones de la zona marina se comunican entre si mediante un sistema de enlaces de microondas digitales, que utilizan ATM como tecnología de transporte para los servicios de telefonía y datos, mientras que a nivel LAN las instalaciones se basan en FastEthernet y en el protocolo IP para las comunicaciones de datos, mientras que la red telefónica se basa en conmutadores *Meridian 1* de Nortel Networks.

En este caso se propuso una implementación híbrida de VoIP que permita la comunicación entre usuarios de la RTC y los usuarios de la red de VoIP de una manera transparente y que permita una migración paulatina hacia una implementación puramente IP, con la finalidad de proteger las inversiones en el sistema telefónico conmutado. La arquitectura de los conmutadores *Meridian* incluye capas de procesamiento, conmutación, acceso y control que permiten invertir en tecnologías VoIP sin impactar en la inversión que se ha hecho en el resto del sistema *Meridian*, lo que permite una migración suave y efectiva hacia VoIP y hacia una red integrada.

El sistema que se propone para la implementación de VoIP en la zona marina es el *Succession* de Nortel Networks, que es el sistema que mejor protege las inversiones hechas en el sistema *Meridian*, que mantiene el nivel acostumbrado de disponibilidad y servicios, que brinda una gran variedad de funciones, que soporta una gran cantidad de dispositivos como teléfonos y PBXs analógicos y digitales, que cuenta con las interfaces que actualmente se tienen en los sistemas de PEMEX, y que brinda además soporte para aplicaciones multimedia innovadoras.

El sistema *Succession* se basa en los estándares para VoIP H.323 y SIP (*Session Initiation Protocol*). Lo cual tiene las ventajas de que se puedan integrar equipos o aplicaciones de otros fabricantes a la red VoIP de una manera efectiva, ya que H.323 es el estándar más maduro y el que ha sido más ampliamente implementado, por otro lado el protocolo SIP permite aprovechar la nuevas aplicaciones multimedia para VoIP que han sido

desarrolladas hasta el momento, así como las que están siendo desarrolladas o que serán desarrolladas en el futuro.

En este caso se tiene la gran ventaja de que el sistema *Meridian* se puede migrar o transformar en el sistema *Succession* de una manera económica y flexible que permite la implementación de VoIP tan rápido como se requiera. Para el caso de las instalaciones nuevas se sugiere instalar el sistema *Succession*, que se puede interconectar transparentemente con los sistemas Meridian protegiendo así las inversiones en dicho sistema.

Para proveer funcionalidades de VoIP a los sistemas *Meridian* existen varias opciones desarrolladas para adaptarse a la velocidad con que se quieran integrar las redes de voz y de datos, una de estas opciones es la habilitación de la PBX para IP, otra opción es su interconexión con el sistema *Succession* y la opción más efectiva que es la actualización del sistema *Meridian* al sistema *Succession 1000M*

La estrategia de migración a VoIP que se propone para las instalaciones de la zona marina de PEMEX es la de convertir los conmutadores *Meridian 1* al sistema *Succession* 1000M mediante la actualización al software *Succession 3.0* y la agregación de servidores de señalización. Esta opción es la que brinda mayores ventajas para los usuarios de la telefonía IP y que permite una migración tan rápida como se requiera, al permitir la subsistencia de los teléfonos y servicios del conmutador *Meridian* 1 así como la intercomunicación efectiva entre estos y los teléfonos IP. Esta opción protege la inversión en el sistema telefónico conmutado a la vez que permite hacer uso de todas las ventajas de VoIP, por lo cual resulta una solución económica y efectiva para el cliente, además de que brinda grandes ventajas al momento de la implementación..

Uno de los factores de costo que a menudo no es reconocido en la migración de una red hacia un nuevo paradigma es la inversión hecha en la configuración del sistema y de los clientes IP, muchas soluciones VoIP requieren crear un ambiente de administración completamente nuevo o se tiene que trasladar el modelo de administración al nuevo sistema, usualmente las características entre el nuevo y el viejo son completamente diferentes por lo que se requiere invertir mucho tiempo para definir el plan de administración y de marcación.

En la migración del sistema *Meridian 1* al sistema *Succession 1000M* no ocurre lo anterior, ya que el sistema de administración común permite que mucha de la información sea retenida y usada para la definición del nuevo sistema, por ejemplo la información personal de los usuarios (nombre, dirección, departamento, etc.) pero se puede ir más lejos al reutilizar la información de la configuración de características y servicios. El antiguo plan de marcación puede ser extendido hacia los nuevos nodos *Succession* mediante una herramienta de análisis que puede usar el plan de marcación de un nodo *Meridian 1* como punto de partida para asignar los números a los nuevos clientes IP de acuerdo a dicho plan. Esto permite ahorrar hasta un 90% del esfuerzo requerido para definir las propiedades del sistema.

El software *Succession 3.0* está diseñado para trabajar de manera fluida con *Nortel Networks Multimedia Exchange* (MX), una solución de entrega de aplicaciones multimedia y colaborativas basadas en SIP. El protocolo SIP proporciona servicios basados en *web* mediante sesiones multimedia en tiempo real que pueden integrar voz, datos y video, SIP tiene una arquitectura basada en texto que agiliza el acceso a nuevos servicios con una gran flexibilidad y escalabilidad.

Los usuarios del sistema Succession pueden incorporar en sus computadoras un software de telefonía cliente y aprovechar las aplicaciones del servidor *web Multimedia Communication Server (MCS) 5100*, que incluye servicios de colaboración como conferencias, *whiteboard*, intercambio de archivos, *web push* y navegación conjunta, servicios de personalización como son control de llamadas, control de entrada de llamadas, administración de llamadas y enrutamiento, servicios multimedia como llamadas de video, identificación de llamada mediante fotografías, servicios de presencia y mensajes instantáneos. Esta solución esta orientada a mejorar la productividad de los usuarios, reducir tiempos de producción y facilitar la toma de decisiones.
Para el ejemplo práctico se propuso una topología de red que brinda calidad de servicio (QoS) de extremo a extremo (para asegurar la calidad de voz del sistema), mediante una topología simplificada y un sistema de implementación y administración de políticas de QoS que simplifica drásticamente la tarea de preparar la red de datos para la integración de servicios de voz y multimedia, que brinda mecanismos eficientes de seguridad y que asegura las recomendaciones de diseño técnico sugeridas. Para esto se integran servidores encargados

de la implementación y administración de políticas de red y de la administración del sistema *Succession 1000M*.

Para satisfacer los objetivos del sistema se propone la integración de varios servidores de servicios para telefonía, que incluyen a los sistemas para brindar los servicios suplementarios y de multimedia a los usuarios de VoIP, y también para los usuarios de telefonía de conmutación de circuitos. Este o estos servidores se encargan de brindar los servicios de mensajería unificada, centro de llamadas y las aplicaciones telefónicas multimedia avanzadas para usuarios de VoIP. Además se propone integrar un servidor que se encargue de la administración de las políticas de QoS.

**Acrónimos**

**A**

**AAL** (*ATM Adaptation Layer)*: Nivel de adaptación (capa 2) para servicios de voz, vídeo y datos hacia la red ATM. Se disponen variantes desde AAL 1 hasta AAL5.

**ACK** (*Acknowledgement*): Mensaje de reconocimiento para señalar que la información ha sido recibida correctamente.

**Add-Drop**: Operación que consiste en extraer e insertar canales tributarios sobre una señal que transita en una línea.

**ADM** (*Add-Drop Multiplexer*): Multiplexor que mira en al menos dos direcciones y que permite extraer e insertar algunos canales desde cada información principal.

**ADPCM** (*Adaptative Diferential PCM*): Codificador de señales digitales que utiliza una predicción adaptativa de la muestra y que codifica la diferencia entre la muestra y la predicción.

**ADSL** (*Asymmetric Digital Subscriber Line*): Tecnología que permite transmitir por cables de cobre una señal cuya velocidad es más alta de entrada al usuario que de salida.

**ANSI** (*American National Standard Institute*): Instituto de normalización de USA

**ARP** (*Address Resolution Protocol*): Protocolo de resolución de direcciones MAC e IP utilizado en el ámbito de redes LAN con protocolo IP.

**ARPA** (*Advanced Research Proyect* Agency): Agencia del gobierno de USA que generó las normas iniciales de la actual Internet. Anteriormente denominada Arpanet.

**ARQ** (*Automatic Repeat Request*): Sistema de solicitud de retransmisión automático de información aplicado en redes de paquetes cuando los mismos se reciben con errores.

**ASCII** (*Americ Stand Code Information Interchange*): Codificación de las teclas de un computador mediante una secuencia (carácter) de 7 bits más uno de paridad.

**ATM** (*Asynchronous Transfer Mode*): Red de transmisión de datos, voz y vídeo mediante celdas (paquetes de 53 bytes fijos).

**B**

**BGP** (*Border Gateway Protocol*): Protocolo de enrutamiento que se utiliza para resolución de tablas de enrutamiento en los enrutadores que se encuentran en el borde de la red IP.

**Bit** (*Binary Digit*): Dígito binario que significa que un elemento posee dos estados (0 y 1) posibles y con igual probabilidad de ocurrencia.

**Bps** (*Bits per second*): Unidad de medida de la velocidad de datos digitales. Usualmente se utilizan múltiplos como kbps, Mbps y Gbps.

**Bridge**: Componente de una red LAN que permite unir dos redes o segmentar una LAN demasiado grande. Actúa como filtro de direcciones IP.

**Broadcast**: Servicio de redes LAN e IP que permite enviar señales a todos los usuarios conectados sin necesidad de una conexión individual para cada uno.

**Buffer**: Memoria intermedia que permite escribir y leer los datos con un reloj distinto y en forma independiente.

**BW** (*Bandwidth*): Característica de un sistema de comunicaciones que indica la cantidad de información que transporta.

**C**

**Cancelador de Eco**: Circuito electrónico que permite mejorar la forma de onda de la señal recibida cuando existe eco (reflexión) en el enlace de transmisión.

**CAS** (*Channel Asociated Signaling*): Método de señalización utilizado en los circuitos digitales donde la señalización se transmite junto a la señal vocal. Es reemplazado por SS7.

**CBR** (*Constant Bit Rate*): Servicio de velocidad de información constante. Se contrapone con el servicio VBR que tiene una velocidad variable dependiendo de las necesidades.

**CCS** (*Common Channel Signaling*): Sistema de señalización que utiliza un canal de datos común a todas las conexiones telefónicas. También conocido como SS7. en lugar de fibras ópticas.

**CDMA** (*Code Division Multiple Access*): Forma de acceso a un medio común de enlace donde cada usuario utiliza un código ortogonal con los restantes.

**CIR** (*Committed Information Rate*): Tasa de información garantizada en una red Frame Relay. El caso de CIR-cero equivale a no garantizar una tasa mínima de datos en la red.

**Codec** (*Encoder/Decoder*): Denominación genérica utilizada para cualquier circuito que realiza una codificación y decodificación de datos.

**Control de error:** Proceso por el cual es posible detectar que la información ha sido recibida con errores. Los errores pueden dar lugar a la retransmisión o al descarte de datos.
**Control de flujo:** Proceso por el cual el receptor puede controlar la emisión del transmisor de datos.
**CoS** (*Class of Service*): Denominación genérica que permite clasificar los tipos de servicios que se entregan en una red de datos.
**CPU** (*Central Procesing Unit*): Unidad de procesamiento central de una computadora o equipamiento electrónico.
**CRC** (*Cyclic Redundancy Check*): Método de cálculo de bits de paridad que se utiliza para la detección de errores en las redes de datos por paquetes.
**CSMA/CD** (*Carrier Sense Multiple Access/Collision Detect*): Tipo de acceso múltiple que detecta la presencia de señal y las colisiones entre transmisiones utilizado en las LAN de tipo Ethernet.
**CTS** (*Clear To Send*): Comando utilizado sobre la interfaz de datos RS-232 para indicar la disponibilidad a recibir datos. Es una respuesta al comando RTS.
**D**
**DCC** (*Data Communications Channel*): Canal de comunicación de datos insertado dentro de la trama STM-1 en la red SDH para transportar información de gestión de TMN.
**DCE** (*Data Communication Equipment*): Equipo de comunicación de datos. Identifica por ejemplo al módem de datos frente a la PC.
**Diafonía**: Efecto por el cual una línea induce señal sobre una vecina y produce interferencia.Ver también FEXT y NEXT.
**Disponibilidad:** Periodo de tiempo donde el canal se encuentra en condiciones de transporta señal con la calidad deseada. Se mide en porcentaje (por ejemplo 99.99%).
**DNS** (*Domain Name System*): Sistema que permite organizar los nombres de Internet. Contiene un máximo de 63 caracteres; 3 indican el dominio (.com) y 2 indican el país (.mx).
**DSE** (*Data Switch Equipment*): Este componente complementa los elementos de un canal de datos simplificado: el terminal DTE y el equipo de comunicaciones DCE.
**DSI** (*Digital Speech Interpolation*): Técnica que permite eliminar los instantes de silencio en una comunicación telefónica y reducir la ocupación a menos de la mitad del tiempo en promedio.
**DTE** (*Data Terminal Equipment*): Identifica al equipo terminal de datos (una PC) frente al equipo de comunicaciones DCE (el módem de datos por ejemplo).
**DTMF** (*Dual Tone Multi-Frequency*): Sistema de señalización que utiliza dos tonos de frecuencia dentro de la banda vocal para cada tecla del teléfono.
**Dúplex**: Forma de comunicación que involucra señales en ambas direcciones. Similar al concepto de bidireccional.
**E**
**E1** (*European 1*): Denominación comercial de un circuito de 2048 kbps y que por multiplexación da lugar a la velocidad E3 de 34.386 kb/s (34 Mb/s).
**EIA** (*Electronic Industries Association*): Organismo que reúne a empresas industriales de USA y que determinan normas de facto. Para las telecomunicaciones es EIA-TIA.
**E-mail** (*Electronic Mail*): Servicio de correspondencia digital utilizado frecuentemente en las redes IP y en la Internet. Utiliza el protocolo SMTP.
**Erlang:** Unidad de medida de tráfico en telefonía. Un erlang equivale a la ocupación permanente del canal telefónico.
**Ethernet**: Red de área local normalizada en IEEE 802.3.
**ETSI** (*European Telecom Standard Institute*): Instituto para el ámbito de Europa que normaliza las telecomunicaciones. Similar a la ITU-T.
**F**
**Facsímil o Fax:** Formato de conversión digital de un documento por lectura de puntos en blanco y negro. Cada punto se denomina PELS.
**FAS** (*Frame Alignment Signal*): Secuencia conocida de bits que se insertan al inicio de una trama para mantener el alineamiento entre transmisor y receptor de datos. Usado en la STM-1.
**FastEthernet:** Basado en la norma Ethernet, permite la interconexión a 100 Mbps mediante el uso de cables de cobre (en una LAN) o fibra óptica.
**FCC** (*Federal Communications Commission*): Comisión del gobierno de USA que se ocupa de las regulaciones en el ámbito de las comunicaciones.

**FDD** (*Frequency Division Duplexion*): Forma de transmisión dúplex (en ambos sentidos) que utiliza distintas frecuencias. La separación entre frecuencias se denomina Shift.
**FDDI** (*Fiber Distributed Data Interface*): Red de área metropolitana que utiliza un anillo unidireccional de fibras ópticas a la velocidad de 100 Mbps.
**FDM** (*Frequency Division Multiplexer*): Tipo de multiplexores utilizados en la era de las comunicaciones analógicas donde cada usuario tenía asignada una frecuencia distinta.
**FDMA** (*Frequency Division Multiple Access*): Tipo de acceso a un medio común (por ejemplo un satélite) donde cada transmisor utiliza una frecuencia distinta.
**FEC** (*Forward Error Correction*): Denominación genérica para distintos tipos de formas de corrección de errores donde se envían bits adicionales para reconocer el error.
**FEXT** (*Far-End CrossTalk*): Diafonía producida sobre el terminal remoto distante entre pares que transmiten en la misma dirección.
**Flag:** Bandera o alineamiento de paquete. Secuencia fija (01111110) que inicia los paquetes en la mayoría de las redes de datos.
**FM** (*Frequency Modulation*): Técnica de modulación donde la frecuencia de la portadora cambia de acuerdo con la variación de la señal modulante.
**Frame Relay:** Red de datos derivada de la red X.25 que permite accesos desde 64 kbps hasta 2 Mbps. Ofrece servicios punto a punto y del tipo PVC.
**FSK** (*Frequency Shift Keying*): Técnica de modulación de frecuencia FM donde la señal modulante es una señal digital y por ello la salida son saltos de frecuencia.
**FTP** (*File Transfer Protocol*): Protocolo definido en el ámbito de Internet para permitir la transferencia de archivos entre terminales.

**G**

**Gatekeeper:** Identifica al centro de control de H.323 (VoIP, FoIP, etc). Se ocupa del procesamiento, autentificación, tarifa, ancho de banda, etc.
**GigabitEthernet:** Red de datos que permite la interconexión de redes LAN utilizando el mismo protocolo Ethernet pero a la velocidad de 1000 Mbps por fibras ópticas.

**H**

**Handoff:** Proceso por el cual un móvil dentro de un sistema de telefonía celular puede cambiar de celda sin interrupciones de comunicación.
**Hardware:** Circuitos que componen un equipamiento y que soportan las funciones del software.
**HDB3** (*High Density Bipolar*): Formato de codificación de señales digitales (usado en E1 a 2 Mbps mediante conductores metálicos).
**HDLC** (*High Level Dat Link Control*): Protocolo de referencia para la capa 2 del modelo OSI que da lugar a los protocolos LAP y LLC.
**HDSL** (*High-bit-rate Digital Subscriber Loop*): Un tipo de acceso al usuario a alta velocidad utilizando la planta externa de cobre convencional de las operadoras telefónicas.
**HEC** (*Header Error Control*): Byte usado en ATM para la detección y corrección de dos errores en el encabezado de 5 bytes.
**Hold Over:** Forma de oscilación controlada por una tensión memorizada en un generador de temporización cuando se pierden las fuentes programadas.
**HTTP** (*HiperText Transfer Protocol*): Protocolo de transferencia utilizado para el servicio Web (www) en Internet. El lenguaje de escritura es el HTML.
**Hub**: Concentrador utilizado en las redes LAN de tipo Ethernet con topología en estrella y cableado estructurado mediante pares trenzados (10BaseT).

**I**

**IANA** (*Internet Assigned Numbers Authority*): Autoridad dependiente del IAB que asigna y controla las direcciones de Internet a nivel mundial.
**ICMP** (*Internet Control Message Protocol*): Protocolo asociado al IP en el ámbito de Internet y que sirve para efectuar reportes de error o detección de actividad (ping).
**IEC** (*Internacional Electrotechnical Commission*): Comisión internacional que se ocupa de normas de calidad. Entre otras se tienen las normas de control de calidad de fibras ópticas.
**IEEE** (*Institute Electrical and Electronic Engineers*): Instituto internacional que estudia aspectos de las comunicaciones. Dispone de las normas IEEE 802.x referidas a redes de datos.
**IEEE 802.x:** Grupo de normas para redes LAN: 802.3 para Ethernet; 802.5 para Token Ring; 802.6 para MAN; etc.

**IETF** (*Internet Engineering Task Force*): Grupo de estudio en el ámbito de Internet que se ocupa de las normas conocidas como RFC.
**IN** (*Intelligent Network*): Denominación usada para describir a las redes de telefonía convencionales que aportan servicios similares a la ISDN. Requiere el sistema de señalización SS7.
**Interleaver:** Circuito que permite distribuir los datos en el tiempo (creando una diversidad temporal) y reducir el efecto de las ráfagas (burst) de errores.
**Internet:** Red de datos extendida mundialmente que utiliza los protocolos TCP/IP. Permite los servicios de e-mail, web, telnet, etc.
**Internetworking:** Denominación del proceso que permite interconectar redes de distinto tipo mediante equipos que trabajan con diversidad de protocolos (routers).
**IP** (*Internet Protocol*): Protocolo de capa 3 definido en el ámbito de la Internet y que se ocupa de las direcciones (4 bytes) de usuario.
**IPsec** (*IP Security*): Denominación genérica que involucra los procesos por los cuales se incrementa la seguridad en la transferencia de datos en Internet.
**IPX/SPX** (*Internet Packet Exchange/Sequenced PX*): Protocolos correspondientes a las capas 3 y 4 en las redes Novell. Son similares a los IP y TCP de Internet.
**ISDN** (*Integrated Service Digital Network*): Servicio de acceso al usuario a velocidad de 144 kbps (2B+D) que aprovecha la planta externa convencional y la señalización SS7.
**IS-IS** (*Intermediate System-to-IS*): Tipo de protocolo de resolución de rutas usado en el ámbito del modelo OSI para el protocolo CLNS.
**ISO** (*International Standard Organization*): Organización internacional que trabaja en conjunto con ITU-T para la definición de normas en el ámbito de las comunicaciones y otras disciplinas.
**ISP** (*Internet Service Provider*): Referido a una empresa que entrega servicios de Internet en forma pública mediante puntos de presencia POP.
**ISUP** (*ISDN User Part*): Protocolo (capa 4) de la suite de señalización SS7 que se ocupa de los mensajes de usuario ISDN (incluye los usuarios de telefonía convencional).
**ITU-T** (*Internacional Telecommunication Union*): Organismo dependiente de la ONU y que se ocupa de las normalizaciones en el ámbito de las telecomunicaciones con sede en Ginebra, Suiza.

**J**

**Jitter**: Fluctuación de fase de una señal digital. El jitter corresponde a una fluctuación de alta velocidad (superior a 10 Hz).
**JPEG** (*Joint Photographic Expert Group*): Grupo de normalización dentro de la ISO que generó la forma de codificación de imágenes con extensión jpg.

**L**

**LAN** (*Local Área Network*): Red de interconexión de elementos informáticos en un área de localización reducida. Por ejemplo Ethernet y Token Ring.
**LLC** (*Logical Link Control*): Protocolo definido en el estándar IEEE 802.2 y aplicado en la capa 2 (sobre MAC) para las redes LAN. Realiza funciones de retransmisión de paquetes con errores.
**LO** (*Local Oscilador*): Oscilador local en un equipo de radioenlace. Denominación útil tanto para la etapa de frecuencia intermedia como de radiofrecuencia.
**LOF** (*Loss Of Frame*): Alarma local emitida el equipo de recepción detecta en forma errónea un número determinado de palabras de alineamiento de trama FAS.
**Log** (*Login/Logon*): Procedimiento por el cual se inicia una sesión para el acceso a un sistema. El procedimiento de cierre se denomina *Logout*.
**LOP** (*Loss Of Pointer*): Alarma local emitida en un equipo SDH cuando el puntero se lee con error un determinado número de veces consecutivas.
**LOS** (*Loss Of Signal*): Alarma local emitida cuando se detecta la falta de señal de entrada a nivel eléctrico u óptico.

**M**

**MAC** (*Medium Access Control*): Protocolo de capa 2 definido en el estándar IEEE 802.1. Las direcciones MAC de 6 bytes sirven para identificación de los componentes en una LAN.
**MAN** (*Metropolitan Area Network*): Es una red que cubre un área equivalente a una ciudad. Puede realizarse mediante IEEE 802.6, FDDI, ATM, GigabitEthernet, etc.
**MAP** (*Mobile Application Part*): Protocolo utilizado para señalización en sistemas celulares. Pertenece a la familia de protocolos SS7.

**MIB** (*Management Information Base*): Base de información de datos definido en los protocolos de gestión de redes (por ejemplo en SNMP y CMIP).
**MIPS** (*Million Instructions Per Second*): Unidad de medida que permite indicar la cantidad de instrucciones que puede manejar un procesador por segundo.
**Modem** (*Modulator-Demodulator*): Identifica al conjunto del modulador y demodulador. Usado tanta para redes de datos como para enlaces de microondas.
**MPEG** (*Moving Pictures Experts Group*): Formato de codificación de imágenes en movimiento desarrollado en el ámbito de la ISO y de extensa aplicación. Utiliza la extensión mpg.
**MS-DOS** (*Microsoft-Disk Operating System*): Sistema operativo DOS de Microsoft MS que constituye la base del sistema Windows.
**MTBF** (*Mean Time Between Failure*): Unidad de medida de falla de equipos. Identifica en período medio entre fallas expresado en horas.
**MTP** (*Message Transfer Part*): Se trata de las capas 1,2 y 3 del modelo OSI para la familia de protocolos de señalización SS7.
**MTTR** (*Mean Time To Repear*): El tiempo medio de reparación expresado en horas está determinado por la organización del mantenimiento.
**Multicast:** Servicio en redes LAN e IP que permite enviar una señal a un grupo cerrado de usuarios sin necesidad de conectar uno a uno.
**MUX** (*Multiplexor*): Denominación de un equipo o circuito que realiza la multiplexación de varias entradas en una sola salida.

**N**

**NAT** (*Network Address Translation*): Metodología por la cual en una red IP se pueden utilizar direcciones no normalizadas en el interior de la red y normalizadas en la salida al exterior.
**NEXT** (*Near-End CrossTalk*): Diafonía producida entre conductores que transmiten señales en distinto sentido y que afecta al receptor localizado en el terminal cercano.
**NIC** (*Network Interface Card*): Denominación genérica para una unidad (tarjeta) que sirve para conectar un equipo hacia una red externa.
**NNI** (*Network-Node Interface*): Tipo de interfaz definida en ATM y que corresponde a un nodo hacia la red. La otra interfaz es UNI y difiere en el primer byte del encabezado.
**NT** (*Network Terminal*): Denominación referida en ISDN a la unidad extrema de la red en el usuario. Hacia un lado se conecta con la central y al otro al equipo terminal TE.

**O**

**Offset:** Denominación genérica utilizada cuando se quiere señalar un corrimiento entre un parámetro y otro. Ejemplo: offset de fragmentación en IP.
**OSI** (*Open Systems Interconnect*): Modelo de 7 capas para las redes de datos desarrollado en 1976 por la ISO y adoptado 1por la ITU-T para los desarrollos posteriores.
**OSPF** (*Open Shortest Path First*): Protocolo de resolución de enrutamiento usado por los enrutadores en una red IP y que se basa en el algoritmo del próximo paso.
**Overflow:** Estado de una memoria elástica (buffer) cuando se llena o se vacía (underflow) debido a la distinta velocidad de entrada y salida de datos.

**P**

**PBX** (*Private Branch Exchange*): Central de conmutación privada normalmente interconectada con la red pública o con otra PBX mediante enlaces punto-a-punto.
**Padding:** Señal de compensación que se utiliza en diversas aplicaciones para ocupar los tiempo de relleno o igualar velocidades.
**PC** (*Personal Computer*): Computador personal (desktop, notebook, etc) que contiene la totalidad de las funciones en su interior.
**PCM** (*Pulse Code Modulation*): Proceso de codificación digital de las señales analógicas que consiste en el muestreo y la codificación de muestras.
**PCMCIA** (*Personal Computer Memory Card International Association*): Equivalente a NIC. Corresponde a una tarjeta que se coloca generalmente en las notebooks para interconectarlo a la red.
**PDH** (*Plesiochronous Digital Hierarchy*): Jerarquía digital que iniciando en E1 (2 Mbps) multiplexa a velocidades de 8 Mbps, 34 Mbps y 140 Mbps. Es reemplazada por SDH.
**PDU** (*Protocol Data Unit*): PDU equivale a la denominación paquete de datos (o mensaje, celda, trama, datagrama, etc, dependiendo de la red).

**PHY** (*Physical Layer*): Capa 1 del modelo de capas. Se ocupa de la adaptación del PDU al medio de transmisión específico.
**PM** (*Phase Modulation*): Modulación donde la portadora modifica la fase en función de la señal modulante. Si la modulante es una señal digital se tiene PSK.
**POH** (*Path OverHead*): Grupo de 9 Bytes colocados al inicio del contenedor virtual VC-4 en la trama STM-1 de SDH. Se usa para informaciones de servicio.
**Pointer:** Puntero que señala la posición del contenedor VC-4 dentro de la trama STM-1. Si la red SDH está sincronizada el puntero está fijo.
**POP** (*Point of Presence*): Se refiere al punto donde un operador de Internet ISP tiene disponible el acceso de los usuarios.
**PPP** (*Point-to-Point Protocol*): Protocolo definido en Internet para la capa 2 del modelo OSI. Permite la corrección de errores y se utiliza para acceso dial-up a un ISP.
**PPS** (*Packet per Second*): Unidad de medida que sirve para indicar la capacidad de procesamiento de paquetes de un circuito.
**Predictor:** Algoritmo de cálculo que predice el estado de una futura señal en base a los valores anteriores. Usado tanto para telefonía como en vídeo.
**PSTN** (*Public Switched Telephone Network*): Denominación genérica para las redes de telefonía pública convencionales.
**PSU** (*Power Supply Unit*): Se refiere a las unidades en los equipos que entregan la alimentación al resto de las unidades. Pueden ser conversores DC/DC o AC/DC.
**PVC** (*Permanent Virtual Circuit*): Circuito para transferencia de datos establecido en forma permanente entre dos o más puntos de ingreso de usuarios.
**Q**
**QoS** (*Quality of Service*): Concepto que permite asegurar determinadas prestaciones al usuario, como ser una tasa de datos mínima de transporte en la red.
**R**
**RAM** (*Random Access Memory*): Tipo de memoria de lectura y escritura. Los datos se borran si se elimina la alimentación del circuito.
**RF** (*Radio Frequency*): Denominación normalmente genérica que identifica a las señales de radio tanto de baja como de alta frecuencia (microondas).
**RFC** (*Request For Comments*): Publicaciones en el ámbito de Internet que contienen informaciones que son sometidas a evaluación. No constituyen estándares.
**RFI** (*Remote Failure Indicador*): Alarma remota usada en SDH que señala una falla grave en el receptor. Es conocida también como FERF.
**RIP** (*Routing Information Protocol*): Este protocolo asociado al IP en Internet es el primero que permitió la comunicación entre enrutadores para actualizar las tablas de ruta en forma periódica.
**RJ-11/RJ-45** (*Registered Jack*): Tipos de conectores de 6 y 8 contactos usados en cableado estructurado para telefonía (RJ-11) y redes LAN (RJ-45).
**Roaming:** Proceso por el cual un usuario de una red de telefonía celular puede acceder a otra mediante un convenio entre empresas.
**ROM** (*Read Only Memory*): Memoria de solo lectura. Puede tratarse por ejemplo de discos CD-ROM.
**Router:** Componente de una red IP que permite la interconexión de redes mediante un direccionamiento dinámico. Utiliza los protocolos de routing.
**RS-232:** Interfaz definida por EIA y permite la conexión entre el DTE y DCE. Es equivalente a las normas ITU-T V.24/V.28 e ISO-2110.
**RSVP** (*Resource ReserVation Protocol*): Protocolo utilizado en las redes IP para reservación de ancho de banda en amplicaciones que requieren mantener un estado de tiempo real.
**RTP** (*Real-Time Transport Protocol*): Protocolo utilizado en las redes IP para transportar servicios de tiempo real como ser la telefonía o videoteléfono.
**RTS** (*Request To Send*): Señal de comando en la interfaz RS-232 que permite solicitar al equipo de comunicaciones de datos DCE la autorización para emitir datos. Respuesta CTS.
**S**
**SCCP** (*Signaling Connection Control Part*): Protocolo que pertenece a la suite del SS7 (CCS) y que permite dar servicios ligados al control del enlace de señalización.
**SDH** (*Synchronous Digital Hierarchy*): Jerarquía de multiplexación que parte desde STM-1 a la velocidad de 155.520 kbps y se despliega en STM-4 (622 Mbps) y STM-16 (2488 Mbps).

**Señalización**: Conjunto de informaciones intercambiada para supervisión, direccionamiento y explotación de la red telefónica. Ver CAS y CCS (SS7).
**Símplex:** Forma de comunicación que involucra señales en una sola dirección. Similar al concepto de unidireccional.
**Slip:** Deslizamiento. Se trata de la duplicación o pérdida de datos cuando la memoria buffer se llena o se vacía.
**SMTP** (*Simple Mail Transfer Protocol*): Protocolo de transferencia de correo electrónico dentro del ámbito de Internet. Permite el servicio e-mail.
**SNA** (*System Network Architecture*): Arquitectura de protocolos diseñados por IBM. Es de características similares a Internet o a OSI.
**SNMP** (*Simple Network Management Protocol*): Protocolo desarrollado en el ámbito de Internet para la gestión de componentes de red (routers, switches, etc).
**Software:** Soporte lógico de un equipamiento que se memoriza para ser ejecutado durante la operación del mismo.
**SOH** (*Section Over Head*): Encabezado de la trama STM-1 en la red sincrónica SDH y que sirve para transportar informaciones de servicio (alarmas, paridad, gestión, etc.).
**SONET** (*Synchronous Optical Network*): Denominación usada en USA para la red sincrónica SDH. El nivel de Sonet OC-3 es equivalente al STM-1 de la ITU-T.
**SPC** (*Stored Program Control*): Técnica utilizada para controlar las centrales de conmutación telefónicas donde el corazón de la central es un CPU con programa almacenado en memoria.
**SS7** (*Signaling System 7*): El sistema de señalización No7 es el actualmente utilizada en las redes de telefonía digital para brindar servicios de valor agregado.
**STM** (*Synchronous Transport Modul*): Módulo de transporte sincrónico de 155 Mbps que determina el primer nivel de la jerarquía digital sincrónica SDH.
**STP** (*Shielded Twist Pair*): Par de cobre trenzado para evitar los efectos de la diafonía y que se encuentra dentro de una pantalla acoplada a tierra. Se utiliza en cableado estructurado.
**Stuffing:** Proceso por el cual una señal tributaria puede ser ingresado en un multiplexor que tiene distinto reloj (señal plesiócrona).
**Supresor de Eco:** Circuito analógico que reduce el efecto del eco en una comunicación atenuando la recepción cuando se está hablando.
**SVC** (*Switched Virtual Circuit*): Servicio ofrecido por una red de datos que permite conectar y desconectar la sesión a solicitud del cliente. Se contrapone al PVC.
**Switch:** Matriz de conmutación genérica que permite la conexión entre una puerta de entrada y otra de salida.
**T**
**TCAP** (*Transaction Capabilities Application Part*): Protocolo de la suite del SS7 (CCS).
**TCP/IP** (*Transfer Control Protocol/Internet Protocol*): Protocolos del ámbito de Internet que forman el núcleo del funcionamiento. Corresponden a las capas 4 y 3 respectivamente del modelo OSI.
**TDD** (*Time Division Duplexion*): Procedimiento de transmisión dúplex que utiliza el mismo canal pero distinto tiempo para la transmisión y recepción de la señal.
**TDM** (*Time Division Multiplexer*): Procedimiento de multiplexación de varios usuarios que utiliza la división del tiempo en intervalos reservados a cada usuario.
**TDMA** (*Time Division Multiple Access*): Procedimiento de acceso sobre un mismo medio (por ejemplo satelital) mediante el uso de TDM.
**TE** (*Terminal Equipment*): Denominación genérica utilizada en las redes ISDN para identificar el equipo del usuario que se conecta al terminal de red NT.
**Telnet:** Servicio que brinda Internet y que permite un acceso remoto a un terminal. Se trata de un terminal virtual definido en RFC-854.
**TIE** (*Time Interval Error*): Es el corrimiento de tiempo de un reloj respecto a una fuente de estabilidad superior en un intervalo de tiempo de medida.
**Tributaria:** Denominación genérica que describe a la señal de usuario que se ingresa a un equipo de transmisión.
**Trunking:** Sistema de telefonía móvil que permite la comunicación entre un grupo cerrado de usuarios.
**TST** (*Time-Space-Time*): Estructura de la red de switch de las centrales de conmutación telefónicas con 3 etapas basadas en conmutación temporal y espacial.
**TTL** (*Time To Live*): En el protocolo IP identifica al tiempo de vida que posee un datagrama para llegar a destino antes de ser eliminado de la red y notificada dicha acción.

**U**

**UI** (*Unitary Interval*): Unidad de medida para el jitter. Un intervalo unitario UI equivale a un corrimiento de fase igual al ancho de un bit.

**UNI** (*User Network Interface*): Interfaz definida en el ámbito de las redes ATM que conecta al usuario con la red. El encabezado es diferente a la interfaz NNI.

**Upgrade:** Proceso de actualización del software o hardware de un equipamiento.

**UPS** (*Uninterruptable Power Supply*): Fuente de alimentación de energía que permite mantener una reserva de energía para casos de corte de la red pública.

**UTP** (*Unshielded Twisted Pair*): Se trata de pares de cobre trenzados sin pantalla exterior para utilizar en cableado estructurado.

**V**

**VAN** (*Value Added Network*): El concepto de red de valor agregado se refiere a aquellas redes que ofrecen servicios además de transporte de datos.

**VBR** (*Variable Bit Rate*): Servicio ofrecido en ATM donde la velocidad de entrada de datos es variable. Por ejemplo, telefonía y vídeo con codificación dependiente de la actividad.

**VCI/VPI** (*Virtual Channel/Path Identifier*): Identificadores utilizados en el encabezado de la celda ATM para efectuar el direccionamiento dentro de la red. Similar a DLCI en Frame Relay.

**VF** (*Voice Frequency*): Referido a la banda de frecuencias ocupada por la señal vocal; normalmente se refiere al canal telefónico desde 300 a 3400 Hz.

**VLAN** (*Virtual LAN*): Servicio previsto en una red IP para interconexión de LAN con un máximo de seguridad y velocidad.

**VoIP** (*Voice over Internet Protocol*): Servicio de transmisión de señal vocal mediante el uso de paquetes en una red IP. Utiliza los protocolos RTP y RSVP.

**VPN** (*Virtual Private Network*): Referido al servicio de interconectar dos o más redes de usuario mediante una red pública pero manteniendo la privacidad y calidad.

**W**

**WAN** (*Wide Area Network*): Denominación genérica utilizada para una red de datos que ocupa un área extensa, generalmente a nivel nacional o internacional.

**WDM** (*Wavelength Division Multiplexing*): Multiplexación utilizada en los sistemas con fibras ópticas que permite colocar varias portadoras luminosas en la misma fibra. Ver también DWDM.

**Wireless:** Denominación genérica para sistemas de comunicaciones que no utilizan hilos y que por ello trabajan con ondas electromágnéticas o con luz.

**WWW** (*Word Wire Web*): Servicio del tipo hipertexto para transmisión de texto, sonido e imágenes mediante el protocolo HTTP.

**X**

**X.25:** Red de datos por paquetes normalizada por el ITU-T entre 1976-1988 para accesos a baja velocidad (hasta 64 kbps).

**Bibliografía**

"Telecommunications". Warren Hioki. Prentice Hall. 1998. USA

"An Engineering Approach to Computer Networking. ATM Networks, the Internet and the Telephone Network". S. Keshav. Addison-Wesley. 1998. USA

"Computer Networks. A System Aproach". Larry L. Peterson, Bruce S. Davie. Morgan Kaufmann Publisers. 1996. USA.

"Fundamentals of Telecommunications". Roger L. Freeman. Wiley-Intercince Publication. 1999. USA

"Networks and Telecommunications, Design and Operation". Martin P. Clark. John Wiley & Sons. 1998. USA.

"Redes Globales de Información con Internet y TCP/IP. Principios Básicos, Protocolos y Arquitectura". Douglas E. Comer. Prentice Hall. 1996. México.

**Referencias Electrónicas**

**www.redes.upv.es**
Pagina de la unidad docente de redes de computadores de la Universidad Politécnica de Valencia (UPV).

**www.it.uc3m.es**
Pagina del departamento de telemática de la Universidad Carlos III de Madrid

**www.cting.upm.es**
Pagina de la cátedra de telefonía para Internet de nueva generación de la Universidad Politécnica de Madrid (UPM)

**www.redeya.com**
Tutoriales y cursos de diversos temas.

**www.ericsson.com**
Pagina de fabricante de equipo de telecomunicaciones que brinda información de productos, tecnologías y servicios.

**www.openh323.org**
Pagina que brinda información del estándar para VoIP H.323 de la ITU, contiene tutoriales y documentación técnica relacionada.

**www.recursosvoip.com**
Pagina dedicada a lo relacionado con la tecnología y las aplicaciones de la Voz sobre IP, contiene tutoriales, libros, documentación técnica, enlaces y noticias.

**www.openphone.org**
Pagina dedicada a desarrollar soluciones de telefonía por Internet.

**www.voip-calculator.com**
Pagina que ofrece recursos gratuitos para VoIP, libros, *white papers* y calculadores de ancho de banda en línea para VoIP.

**www.cisco.com**
Pagina de fabricante de equipo de telecomunicaciones que ofrece información de productos, soluciones y tecnologías así como documentación y soporte técnicos.
**www.nortelnetworks.com**

Pagina de fabricante de sistemas de telecomunicaciones que brinda información de sus productos y soluciones, así como documentación y soporte técnicos.

**www.itu.int**
Pagina de la Unión Internacional de Telecomunicaciones, organismo de normalización encargado de reglamentar sistemas de telecomunicaciones a nivel mundial y organismo que definió el estándar para VoIP H.323.

**www.ietf.org**
Pagina de la IETF (Internet Engineering Task Force) que es una comunidad internacional encargada de la evolución de la arquitectura de Internet y de su funcionamiento. Este organismo fue el encargado de desarrollar el protocolo para VoIP SIP.

**www.ieee.org**
Pagina del Instituto de Ingenieros Eléctrico-Electrónicos, organismo dedicado a la investigación y desarrollo de tecnologías electrónicas e informáticas. Este organismo ha desarrollado estándares de comunicación como Ethernet.