UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES ARAGON

"CONSTRUCCIÓN DE UNA RED CONVERGENTE UTILIZANDO PROTOCOLOS DISTINTOS A TRAVÉS DEL ENRUTAMIENTO IP"

T E S I S

QUE PARA OBTENER EL TITULO DE
INGENIERO MECANICO ELECTRICISTA
(ÁREA ELÉCTRICA - ELECTRÓNICA)
PRESENTA:

ALFREDO VILLANUEVA ISLAS

ASESOR: Ing. Adrián Paredes Romero

MEXICO , 2008

Antes que nada debo decir:

DIOS MIO GRACIAS POR DEJARME CUMPLIR ESTA META

Gracias, por siempre llevarme de la mano, por hacerme aprender de lo bueno y de lo malo, por nunca dejarme caer, si no por el contrario, por hacer de mi el hombre que ahora soy.

El día de hoy y pese a muchos contratiempos veo concluido uno de los más grandes proyectos de mi vida. se que para muchos éste es sólo el inicio de una tesis, sin embargo para mi, este trabajo significa un principio y un fin.

Un principio, refiriéndome al primer proyecto a nivel profesional que muestro y que le puede ser útil de alguna manera a la sociedad y fin, por que gracias a este trabajo concluyó uno de los ciclos más importantes como estudiante.

Gracias a mis padres por que gracias a su apoyo y consejos he llegado a realizar la más grande de mis metas, la cual constituye la herencia más valiosa que pudiera recibir.

El día de hoy se que la vida no es fácil, sin embargo no tengo palabras para agradecerle a la vida que me haya mandado como guías a estas grandes mujeres mi madre y mi abuelita. Gracias por nunca dejar de confiar y creer en mi, gracias, porque sin su apoyo, comprensión y cariño incondicionales, esto no sería posible.

A todos y cada uno de los miembros de mi familia, especialmente a Pepe, Pablo y Luis ya que han sido faros de luz y guía en mi camino; gracias por siempre brindarme un buen consejo y su apoyo incondicional más que como primos como mis hermanos.

Gracias especialmente a mi novia la mujer que cambio mi vida llenándome de fe y esperanza y siendo participe en todos mis logros y derrotas, te amo juanita, gracias por estar a mi lado.

Gracias a mi asesor, Adrian Paredes por su gran apoyo, por creer en este proyecto por sus consejos como amigo y profesor.

GRACIAS a todas las personas que directa e indirectamente han contribuido no sólo en la elaboración del trabajo, sino en mi formación personal y profesional.

A todos en general por estar a mi lado, y nuevamente

GRACIAS DIOS

Alfredo Villanueva Islas.

ÍNDICE

Capitulo 4: Construcción de una red convergente a través de enrutamiento IP, utilizando protocolos distintos

INTRODUCCIÓN

El almacenamiento y análisis de Información ha sido uno de los grandes problemas a que se ha enfrentado el Hombre desde que inventó la Escritura. No fue sino hasta la segunda mitad del Siglo XX que el Hombre ha podido resolver en parte este problema gracias a la invención del Ordenador.

En la Década de los años cincuenta, el Hombre dio un gran salto en este problema al inventar el Ordenador Personal. Ahora, la Información podía ser enviada en grandes cantidades a una localidad central donde se realizaba el procesamiento de la misma. El problema era que esta información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser "acarreada" al Departamento de Proceso de Datos).

Con la aparición de las terminales en la década de los sesenta se logró la comunicación directa entre los Usuarios y la Unidad Central de Proceso, logrando con esto una comunicación más rápida y eficiente, pero se encontró con un problema, entre más terminales y periféricos se agregaban a los Ordenadores, la velocidad de respuesta de las mismas comenzó a decaer.

Hacia la mitad de la década de los setenta la refinada tecnología del silicón e integración en miniatura permitió a los fabricantes de Ordenadores construir más inteligencia en máquinas más pequeñas.

Estas máquinas llamadas Microordenadores, descongestionaron a las viejas máquinas centrales y ahora cada Usuario tenía su propio Microordenador en su escritorio.

Al principio de la década de los ochenta los microordenadores habían evolucionado por completo el concepto de la Computación Electrónica así como sus aplicaciones y mercados. Los Gerentes de los Departamentos de Informática fueron perdiendo el control de la Información ya que ahora el proceso de la información no estaba centralizado.

Esta época se podría denominar como la era del "Disco Flexible" (Floppy Disk). Los Vendedores de microordenadores proclamaban "en estos 30 discos el Usuario puede almacenar la información de todos sus archivos".

Sin embargo, de alguna manera se había retrocedido en la forma de procesar la Información, ya que ahora había que "acarrear" la Información almacenada de los discos de un microordenador hacia el otro, y también la relativa poca capacidad de los discos hacía difícil el manejo de grandes cantidades de Información.

Con la llegada de la "Tecnología Winchester" (almacenamiento de Información en Disco Duro) se lograron dispositivos que podían almacenar grandes de Información que iban desde 5 hasta 100 Megabytes. Una desventaja de esta tecnología era el alto costo que significaría la adquisición de un disco duro de tipo Winchester.

En este entonces fue cuando nació la idea que permitiría a múltiples Usuarios compartir los costos y beneficios de un disco de tipo Winchester. Las primeras Redes Locales estaban basadas en "Disk Server's". Estos permitían a cada Usuario el mismo acceso a

todas las partes del disco. Esto causaba obvios problemas de la seguridad y de integridad en los datos.

La Compañía Novell fue la primera en introducir un "File Server" en el cual todos los Usuarios pueden tener acceso a la misma Información, compartiendo archivos pero con niveles de seguridad, lo cual permitía que la seguridad e integridad de la Información no se violara.

Novel™ basó su investigación y desarrollo en la idea de que son los "Programas y Paquetes" de la Red y no de la "Arquitectura" que hacia la diferencia en la operación de la Red. Esto se ha podido constatar y en la actualidad Novel soporta más de 20 tipos diferentes de Redes en base a la variedad de sus Sistemas Operativos, (Novel, 1995).
El mundo de las Redes de Área Local (LAN) nació de la necesidad de compartir recursos entre los Ordenadores y los usuarios para hacer más eficiente, económico y administrable un Sistema de Ordenadores.

La expansión de la Industria de las Redes Locales durante los últimos seis años ha sido explosiva. Se estima que sólo en los Estados Unidos de América existen sobre de 100 Fabricantes de Sistemas Completos, otras Empresas ofrecen componentes de Red individuales. Son más de 250 las Empresas dedicadas al negocio de Redes Locales y sus componentes.

La idea básica de una Red de Área Local (LAN) es facilitar el acceso a todos y desde todos los Equipos Terminales de Datos (ETD) de la Oficina, entre los que se encuentran no sólo los Ordenadores, sino también otros dispositivos presentes en casi todas las Oficinas: Impresoras, Trazadores Gráficos, Archivos Electrónicos, Bases de Datos, así como compartir recursos disponibles dentro de la Red.

CAPÍTULO 1.
TOPICOS GENERALES SOBRE REDES.

1.1.- Introducción.

Los servicios no suelen estar limitados por la técnica (muy avanzada en estos momentos) y capaz de resolver casi todos los problemas, sino por la imaginación del operador, y a cualquiera se le puede ocurrir crear y ofrecer a sus clientes (y usuarios) un servicio nuevo; por lo tanto, intentar clasificar los servicios es algo realmente complicado.

Hasta hace relativamente poco tiempo era muy común clasificarlos en servicios de voz, de texto, de vídeo o imagen; pero esto es una clasificación antigua. Los servicios están cambiando continuamente a la vez que surgen nuevos, de manera que intentar clasificarlos se complicó y no hay reglas fijas para ello, sino distintos puntos de ver la situación en un momento determinado.

Las Redes de Ordenadores (locales o remotas) surgieron para hacer posible compartir de forma eficiente los recursos informáticos (Arquitectura de Sistemas, Paquetes y Programas, y finalmente los Datos), de los usuarios. En general, esos recursos son sistemas heterogéneos: los equipos de fabricantes tienen características diferentes, utilizan y ejecutan Programas con características específicas y distintas para las aplicaciones deseadas por los usuarios, y manipulan y producen datos con formatos incompatibles. Así mismo, equipos idénticos de un único fabricante, que se integran en aplicaciones distintas, pueden presentar características heterogéneas.

Esa heterogeneidad de los sistemas beneficia al usuario, que no está así limitado a un único tipo de sistemas para sus distintas aplicaciones. Así, se puede seleccionar el sistema que mejor se adapte a las condiciones de aplicación que interesen y el presupuesto disponible.

Por otro lado, tal heterogeneidad dificulta considerablemente la interconexión de equipos de fabricantes diferentes, según Menascé, (1994).

La interconexión de "redes", a su vez, contribuye a hacer más difícil el problema, ya que puede haber redes diferentes con servicios de transmisión diferentes, que requieran interfases diferentes. En necesario, pues, una manera por la cual, el problema de las heterogeneidades no haga inviable la interconexión de sistemas distintos. La incompatibilidad de equipos y/o redes fue inicialmente resuelta a través del uso de convertidores.

1.2 Ventajas de una red LAN

La Red de Área Local (LAN) se configura de modo que proporcione los Canales y Protocolos de Comunicación necesarios para el intercambio de datos entre Ordenadores y Terminales.

Una Red Local de Microordenadores según Green (1992), es la interconexión de Estaciones de Trabajo que permite la comunicación entre ellas y compartir recursos en forma coordinada e integral, aprovechando la base instalada de Ordenadores. Las ventajas que ofrece este tipo de Red de Ordenadores son las siguientes:

1- Compartir recursos ("Hardware y Software"). Se tiene información y dispositivos a los cuales se puede acceder.

2.- Intercambiar información.

3.- Respaldar datos.

4.-Tener flexibilidad en el manejo de la información.

5.- Crecimiento modular (se puede empezar con una Red pequeña).

6.- Facilidad de adquisición (principalmente por el Sector Público, ya que los Ordenadores se arman en México).

7.- Son sistemas que permiten cambiar de recursos sin muchas dificultades.

8.- Servicios de Correo Electrónico y Mensajería.

1.3. - Elementos de una Red LAN

Los elementos básicos de una Red de Área Local (LAN) son, según Tanenbaum, (1991):

1.- Las Estaciones de Trabajo (Ordenadores).

2.- El Servidor de la Red (Ordenador tipo AT).

3.- Los Cables de Comunicación.

4.- Las Tarjetas de Interfase.

5.- El Sistema Operativo.

1.3.1 Ordenadores

Son Microordenadores que utiliza el usuario para Procesar su información. Estos Microordenadores pueden ser de tipo AT, con o sin Disco Duro. Para procesar la información, el usuario puede hacer uso de los recursos de su microordenador o acceder a la Red para utilizar unidades de memoria, impresoras, graficadores y Módems.

1.3.2 Servidor de red

Es un microordenador de alto rendimiento que tiene uno o varios discos duros de alta velocidad, gran capacidad de memoria y varios puertos para conectar periféricos. Este microordenador ofrece sus recursos a los demás usuarios.

Puede haber uno o varios Servidores en la misma Red, y dependiendo del tamaño de la Red, el Servidor puede ser un Ordenador con un Microprocesador PENTIUM® de alta capacidad.
Se tienen los siguientes tipos de servidores para una Red de Área Local (LAN):

a). Dedicado o no Dedicado.
b). Centralizado o distribuido.

Las funciones del servidor dedicado son exclusivamente administrar los recursos de la Red y controlar el acceso a datos y programas de aplicación por parte de los usuarios de la Red.
Por otra parte, un servidor no dedicado es aquel que además, se utiliza también como una Estación de Trabajo de la Red. Es poco recomendable utilizar el Servidor en modo no dedicado, ya que hace más lento el funcionamiento de la Red.

Las Redes con Servidor centralizado, utilizan una sólo Ordenador como Servidor de Archivos, Servidor de Impresoras y Administrador de la Red.

Las Redes con varias Estaciones de Trabajo, y gran tráfico de información, utilizan como Servidor Distribuido dos o más Ordenadores en donde alguna de ellas, se encarga de Administrar el uso de Impresoras, otra para Administrar Archivos y proporcionar Programas de Aplicación y posiblemente una tercera, para Comunicación con otras Redes o "Mainframes".

Una de las ventajas de las Redes de Ordenadores, es que se puede aumentar la capacidad de almacenamiento con sólo agregar más equipos y que la ubicación de éstos, se puede ajustar a la distribución física de los Departamentos de la Empresa que utilice la Red.

1.3.3. Cable de comunicación

Es el Medio Físico que se utiliza para enviar o recibir mensajes de un Ordenador a otro. Son tres los medios de Comunicación para Redes Locales de Ordenadores y son:

a). Cable Trenzado o Telefónico.
b). Cable Coaxial.
c). Fibra Óptica.

1.3.4 Tarjetas de interfaz

Las tarjetas de interfase de Red NIC (Network Interface Card), son una pieza de la Arquitectura ("Hardware' que va dentro del Ordenador y que provee la conexión física a la Red.

La tarjeta de interfase toma los datos del Ordenador, los convierte a un formato apropiado para poder ser transportados y los envía por el cable, a otra tarjeta de interfase. Esta tarjeta los convierte nuevamente al formato original y los envía al Ordenador. Las funciones de la tarjeta de interfase son las siguientes:

a). Comunicaciones de la Tarjeta de Interfase hacia el Ordenador.
b). Almacenamiento en Memoria.
c) Construcción de paquetes
d) Conversión Serie/Paralelo
e) Codificación y Decodificación
f) Acceder al cable
g) "Handshaking"
h) Transmisión - Recepción.

1.3.5 Sistema Operativo de la Red

Es un conjunto de programas que residen en el Servidor, y que se encargan de comunicar a las Estaciones de Trabajo entre sí, garantizar la integridad de la información y controlar el uso de los recursos de la Red.

Hay muchos Sistemas Operativos, cada uno con características propias, que los diferencian de otros. Los más populares son: Sistema Operativo Novel Network®, IBM PC LAN® y el LAN MANAGER®, WINOOWS NT®, UNIX®, L1NUX®, SUN SOLARIS®, etcétera.

1.4 Topologías y Métodos para Acceder a las Redes.

Según Madron (1997): "La Topología de una Red, es la forma física de conectar las Estaciones de Trabajo, adoptada por la persona que diseña la Red, así mismo, las Estaciones de Trabajo se comunican a la Red por un Método de Acceso Específico que depende del tipo de Red de que se trate".

Los Métodos para Acceder son técnicas utilizadas por las Estaciones de Trabajo, para compartir el canal de comunicación. Los tipos de Redes más importantes de acuerdo a la Topología son:

1.- Red Tipo Anillo.
2.- Red Tipo Bus ó Lineal.
3.- Red Tipo Árbol ó Estrella.

La elección de uno ú otro tipo de Red influye en algunas características de la Red, tales como:

1.- La flexibilidad de la Red para aceptar más Estaciones de Trabajo.
2.- El tráfico máximo de información que acepta la Red, sin que se produzcan interferencias continuas.
3.- Los tiempos máximos de Transmisión - Recepción.
4.- El precio de la Red.- Una Topología mal elegida, eleva los costos de la Red.

1.5 Características de las Topologías de una Red.

1.5.1 Red Tipo Anillo.

"En esta Topología, las Estaciones de Trabajo y el Servidor están conectados a través de un sólo Cable de Comunicación de trayectoria cerrada, en donde la información fluye en un sólo sentido.

El Método para Acceder al Cable se llama TOKEN-RING, en el cual, si una Estación de Trabajo quiere transmitir datos, envía un arreglo de bits de información (TOKEN) que son recibidos por el Ordenador más cercano, la cual los retransmite y los envía al siguiente Ordenador; y así sucesivamente hasta que el mensaje llega a su destinatario". (Giozza; De Araújo; Moura, 1996).

Con este Método para Acceder se tienen las siguientes ventajas:

1.- Los tiempos máximos de espera están definidos.
2.- Como el Servidor sondea primero cuál Estación de Trabajo quiere transmitir, no existen interferencias entre las Estaciones de Trabajo.
3.- Es un Método de Acceso útil en Redes con gran carga de trabajo.
4.- Los nodos se conectan en forma circular.
5.- Cada uno de los nodos retransmite a su vecino.
6.- Si un nodo falla, afecta el funcionamiento de la Red.
7.- La ruptura de un cable afecta a toda la Red.
8.- Se necesita que una máquina sea "MONITOR" y esto se decide según criterios.

La figura 1.1 muestra la topología de anillo

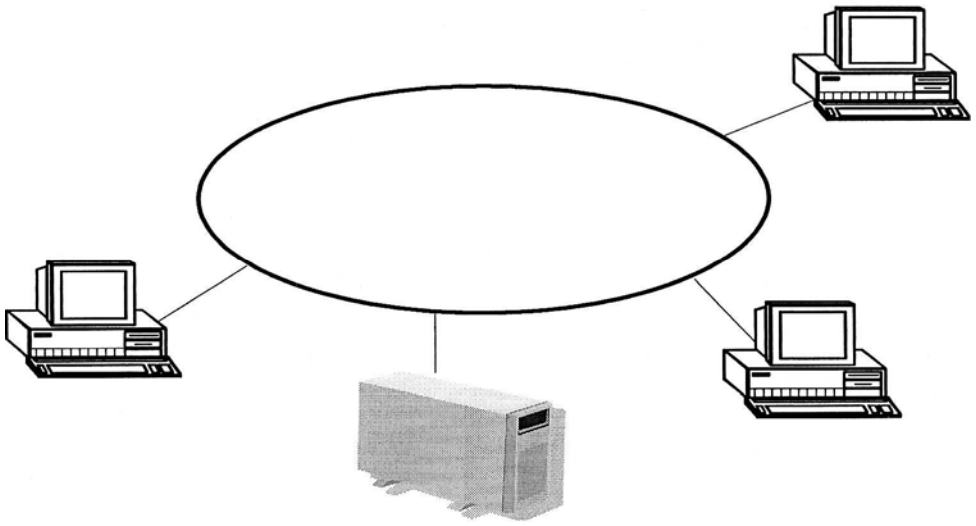


Figura 1.1 Topología de anillo

1.5.2.- Red Tipo Bus o Lineal.

"Este tipo de Redes tienen un sólo bus ó Cable Común de Comunicación, que transporta la información de todas las Estaciones de Trabajo conectadas a él. Estas Redes pueden utilizar el Método para Acceder CSMA/CO (Carrier Sense Multiple Access With / Colision Detection) ó el "TOKEN PASSING}}.

En el Método para Acceder de Forma Múltiple en el Sentido del Portador con Detección de Colisión, las Estaciones de Trabajo que desean transmitir compiten entre sí para utilizar el Cable de Comunicación}}. (Conant, 1996).

Cuando una Estación de Trabajo transmite, espera una confirmación de que su mensaje fue recibido correctamente, pero si esto no sucede, quiere decir que hubo una "Colisión}} en el cable debido a que dos ó más Estaciones de Trabajo, transmitieron al mismo tiempo.

Una vez detectada la "Colisión}} de datos de los Ordenadores involucrados, esperan un tiempo aleatorio y diferente en cada una para retransmitir el mensaje, con lo que se garantiza el que no exista otra colisión.

La principal desventaja de este Método de Transferir Información, es que los tiempos de espera pueden llegar a ser muy grandes en condiciones de alto tráfico de información. Las características principales de esta Topología son:

1.- Es la Topología más simple. Un cable lineal con varios dispositivos conectados a lo largo de él.

2.- Las transmisiones de un nodo viajan en ambos sentidos.

3.- Los nodos no retransmiten la información.

4.- Si un nodo falla, no afecta el funcionamiento de la Red.

5.- La ruptura en el cable afecta a toda la Red.

La figura 1.2 muestra este tipo de topología

Figura 1.2.- Topología de Bus.

1.5.3.- Red Tipo Árbol o Estrella.

"La Red tipo Árbol se conoce también como Anillo Modificado, lo cual se debe a que esta Red es una combinación de la Red de Anillo y la Red tipo Lineal. Se dice que físicamente es una Red Lineal, porque tiene un bus central de comunicaciones al que se conectan las Estaciones de Trabajo en forma directa o a través de ramificaciones.
Por otra parte, su Método para Acceder, llamado TOKEN PASSING, hace que lógicamente funcione como si fuera una Red tipo Anillo". (Bates, 1994).

El Método para Acceder llamado "TOKEN PASSING", consiste en la transmisión de tramos de bits (TOKEN's) de una Estación de Trabajo a otra; pero a diferencia de la Red Anillo, a cada Estación de Trabajo se le asigna un turno para transmitir que puede ser diferente al de su ubicación física dentro de la Red. Las características más importantes de esta Topología son:

1.- Los nodos se conectan a un Concentrador Central.
2.- La falla de un nodo no afecta la Red.
3.- La ruptura de un cable afecta sólo al nodo conectado a él.
4.- El tráfico de información aumenta conforme se incrementan los puertos.
5.- El repetidor Reenvía la información n-1 veces a través del repetidor.

La figura 1.3 muestra la topología de árbol

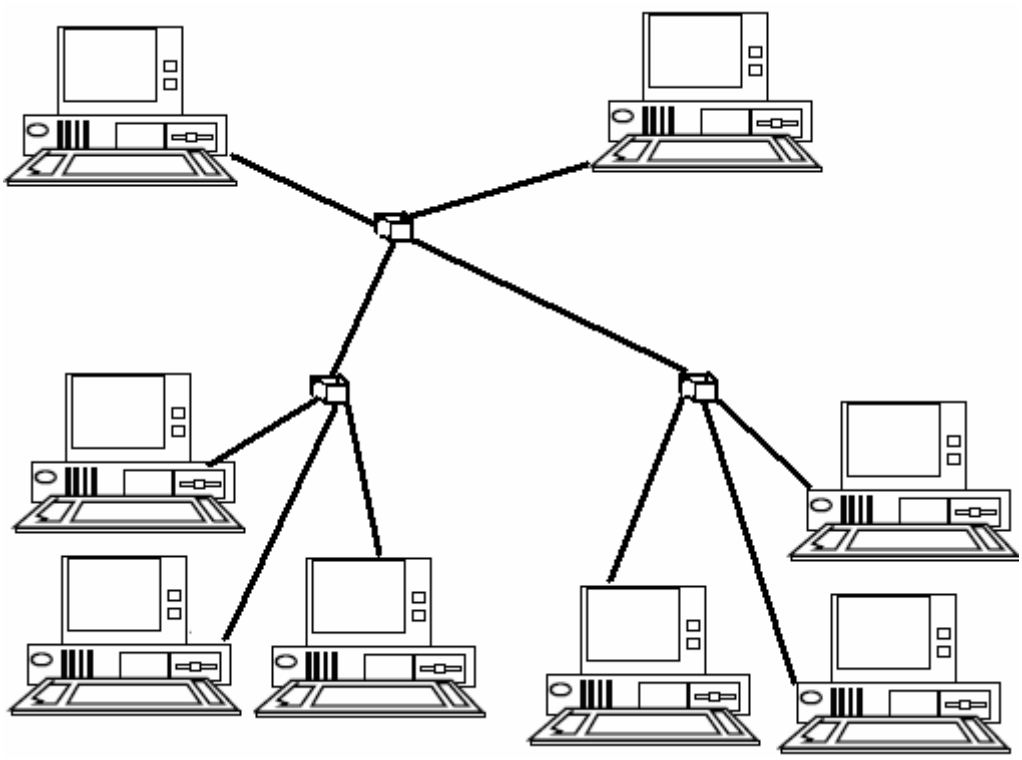


Figura 1.3 Topología de árbol

1.5.4 Redes LAN y topologías

Aunque las diferencias entre las Redes de Área Local (LAN) son grandes, todas ellas comparten varias características comunes, según (Black, 1994), son las siguientes:

1.- Una Red de Área Local (LAN) proporciona la facilidad mediante la cual se interconectan los Microprocesadores, el almacenamiento auxiliar, los dispositivos de facsímil, las impresoras, las copiadoras inteligentes, los equipos de fotocomposición, los teléfonos y los dispositivos de vídeo para comunicarse entre sí. Algunas Redes de Área Local (LAN) interconectan cientos de dispositivos.

2.- El objetivo supuesto de todas las Redes de Área Local (LAN), es permitir a las Organizaciones tener grandes ganancias en productividad y ahorros en costos mediante las eficiencias inherentes de la compartición de recursos.

Una Red de Área Local (LAN) es una Red de Comunicaciones entre elementos al mismo nivel debido a que todos los dispositivos de la Red tienen iguales condiciones para acceder a todos los servicios de la Red.

3.- Debido a que son de propiedad privada y se instalan de manera que no interfieran con las comunicaciones de otras Redes, las Redes de Área Local (LAN) no están sujetas a la Jurisdicción de las Agencias Reguladoras Federales o Estatales.

4.- Las Redes de Área Local (LAN) generalmente están limitadas a un sólo edificio o a un complejo de edificios, aunque algunos dispositivos de la Red pueden extenderse hasta 50 millas. Esto significa que una Red de Área Local (LAN) puede conectar dispositivos de comunicación ubicados en diferentes pisos de un edificio, en edificios adyacentes o en la misma Ciudad.

5.- Las velocidades de transmisión típicamente se encuentran entre 1 y 10 MBits/seg. Sin embargo, algunas Redes de Área Local (LAN) emplean velocidades de transmisión que superan bastante a los 10 Mbits/seg. Como podría sospecharse, entre mayor sea la velocidad de datos, mayor ser el costo de la Red de Área Local (LAN).

6.- Las Topologías de Bus y de Anillo emplean un cable compartido. Esto significa que no puede haber dos mensajes en el cable en el mismo lugar, y al mismo tiempo, sin que se presente una colisión entre ellos, ocasionando la destrucción de ambos mensajes.

Los dispositivos de alguna manera, deben transmitir mensajes de acuerdo a un esquema de acceso, tomando turnos para el uso del cable. El principal esquema para acceder para el cable en el caso de un Bus es la contención. Para un Anillo es el pase de (TOKEN's). Una Estrella utiliza un Concentrador Central para controlar la entrada.

1.6. Técnicas de Comunicación.

La transmisión de bits de información a través del Cable de Comunicación, se realiza en dos formas: En Banda Base yen Banda Ancha. (De Prycker, 1993).

La mayor parte de las Redes Locales trabajan en Banda Base; es decir, utilizan Señales Digitales para transmitir su información a lo largo del cable. La ventaja de utilizar Señales Digitales es que el costo y la complejidad de la Red disminuyen, porque dado que el Ordenador también trabaja con Señales Digitales, los módulos de conexión al cable son sencillos.

En las Redes de Banda Ancha, las Señales Digitales del Ordenador se tienen que convertir en Señales Analógicas usando un Módem para poder ser transmitidas a través del cable.

El ritmo de frecuencia que ocupan estas Señales al ser transmitidas por el cable, es pequeño comparado con el rango de frecuencias (ancho de banda), que puede manejar el Cable de Comunicaciones, lo cual permite que otras Señales Analógicas (Voz, TV, Fax), de frecuencias distintas puedan ser transmitidas simultáneamente por el mismo cable.

Algunos Bancos prefieren gastar en una Red de Banda Ancha, para poder conectar sus Ordenadores, Teléfonos y Cámaras de TV por un mismo cable, y reducir así los costos de instalación.

Las características de las Redes que operan en Banda Base son:

1.- Son de fácil mantenimiento e instalación, ya que no se requieren Módems.
2.- El número máximo de Ordenadores conectadas a la Red es reducido.

3.- Las distancias máximas entre elementos de la Red son más pequeñas que las de Redes en Banda Ancha.
4.- Aceptan sólo Señales Digitales.

Las características de las Redes que operan en Banda Ancha son:

1.- Permite conectar más elementos a la Red y utilizar cables de conexión de longitudes mayores.
2.- Se pueden transmitir varias señales (Voz, Datos, TV, Fax), por el mismo cable simultáneamente.
3.- Las velocidades globales de comunicación son altas.
4.- Utilizan un cable para transmitir y uno para recibir, ó un sólo cable con un rango de frecuencia para transmitir y otro para recibir, ya que las Señales de Información viajan en un sólo sentido.
5.- Debido a la utilización de equipos para Modular y Demodular la Señal, filtros de frecuencia y amplificadores, la instalación y mantenimiento de estas Redes es más costoso y complejo.

1.7. - Redes Locales en el Mercado.

Cuando se desea contar con una Red Local de Ordenadores, se puede elegir entre tres opciones establecidas y por los Estándares Internacionales. Cada tipo de Red se diferencia, no sólo por su Topología y Método de Acceso, sino también por características especiales que las hacen más apropiadas en ciertos casos. Los tipos más comunes son:

- ARCNET
- Ethernet
- Token Ring

1.7.1.- Red Local ARCNET.

La Red ARCNET (A TTACHED RESOURCE COMPUTER NETWORK), es una Red Local tipo Árbol capaz de interconectar hasta 255 nadas. Por nodo se refiere a cualquier dispositivo conectado a la Red como Periféricos y Estaciones de Trabajo. (Black, 1999). Las principales características de esta Red son:

1.- Topología: Estructura de Árbol.
2.- Velocidad: 2.5 Mbits/segundo.
3.- Tiempo de Respuesta: Determinístico.
4.- Método de Acceso: Token Passing.
5.- Medio de Transmisión: Cable Coaxial de 93 Óhms.
6.- Modo de Transmisión: Banda Base.

Las unidades repetidoras de ARCNET se clasifican en pasivas y en activas; las activas a su vez se clasifican en internas y externas.

a). Unidades repetidoras pasivas.- Cuando la distancia que debe cubrirse entre los nadas más lejanos de una Red, no sobrepasa los 60 Metros, y además el número de nadas no excede a cuatro, es posible conectar una unidad repetidora pasiva, la cual tiene cuatro puertos con un alcance de 30 Metros en cada uno de ellos.

Esta unidad debe ser conectada directamente a las tarjetas de Red o a un puerto de un repetidor activo; esto significa, que no se pueden conectar dos pasivos entre sí, ni tampoco dos o más activos por medio de un pasivo.

b). Unidades repetidoras activas.- Tienen un alcance por puerto de 600 Metros, lo cual las hace ideales para instalaciones donde la distancia sea un factor importante.

Por otro lado, tienen la capacidad de ser interconectados entre ellos y con repetidores pasivos, lo cual brinda la posibilidad de contar con el crecimiento que se requiera en cualquier tipo de instalación. Estos alimentadores pueden ser internos o externos y requieren alimentación eléctrica.

Regularmente los repetidores activos, poseen ocho puertos y los pasivos cuatro. Mientras el activo amplifica la señal a sus niveles óptimos, el pasivo sólo divide la señal (técnicamente hace un acoplamiento de impedancias en un sencillo circuito de 4 resistencias). Las principales ventajas de la Red Local A RCNET son:

1.- Es una Red de uso general.
2.- Tiempo de respuesta estable bajo carga de trabajo.
3.- Flexibilidad en crecimiento.
4.- Excelente costo-beneficio.

1.7.2.- Red Local ETHERNET.

La Red Local ETHERNET es una Red tipo Bus o Lineal, y recibe este nombre en analogía a la Teoría del Éter de la transmisión de la luz, para Black (1999), las principales características de este tipo de red son:

1.- Topología: Bus o Lineal.
2.- Medio Físico: Cable Coaxial de 50 Óhms.
3.- Modo de Transmisión: Banda Base.
4.- Método de Acceso: CSMA/CD.
5.- Velocidad de Transmisión: 10 Mbits/segundo.

El crecimiento total de la Red es de 86 nadas repartidos en tres segmentos de una distancia no mayor a 200 Metros cada uno, unidos por dos repetidores, siendo éste el número máximo de ellos.

Un segmento es un cierto tramo de cable, al que se agregan elementos de conexión hacia los Ordenadores (Transceiver's), y que en los extremos se les coloca dispositivos terminadores.

Un segmento está limitado a soportar un máximo de 30 nadas; sin embargo, este número puede duplicarse o triplicarse al colocar uno o dos repetidores; estos elementos están considerados como un nodo más entre cada segmento al que están conectados, por lo tanto, al agregar dos repetidores, se tienen 4 nadas, menos del total de 90, así que el número máximo es 86.

Esta Red puede trabajar a una velocidad promedio de1 0 Mbits/segundo, lo cual la hace ideal para cargas pesadas de acceso a la Red; sin embargo, debido a que utiliza el Método de Acceso CSMA/CD, su funcionalidad va decayendo rápidamente a medida que el número de usuarios en la Red se incrementa, es por esto que esta Topología se recomienda cuando la carga de trabajo es pesada, pero el número de Estaciones de Trabajo activas no es mayor de 10 a 15.

El Cable de Comunicación utilizado es el cable coaxial de 50 Óhms, que viene en dos versiones:

1.- Cable grueso: Hasta 500 Metros/Segmento. Mínimo 2.5 Metros de distancia entre estaciones de trabajo. Requiere un "Transceíver" por estación, y dos terminadores por segmento.

2.- Cable delgado: Hasta 300 Metros/Segmento. Mínimo 3 Metros de distancia entre estaciones. Requiere un conectar tipo "**T**" por Estación y dos terminadores por segmento.

Para un cableado E THERNET, se recomienda lo siguiente:

1.- Un segmento no debe exceder los 185 Metros.
2.- Se puede tener un total de 5 segmentos conectados por repetidores, tres segmentos activos y dos pasivos.
3.- La distancia total de la Red, no debe exceder de 555 Metros.
4.- La mínima distancia de cable entre dos nadas, debe ser de 0.5 Metros.
5.- El número máximo de nadas por segmento es 30.
6.- El número total de nadas por Red es de 86.

Las principales ventajas de la Red Ethernet son:

1.- Garantiza conectividad a otros ambientes (uso específico).
2.- Excelente rendimiento con pocos nadas.
3.- Está apoyado por varias Empresas Transnacionales de importancia.

Y sus principales desventajas:
1.- Tiempo de respuesta decreciente bajo carga de trabajo.
2.- Es necesario anticipar y dejar cableado el crecimiento de la Red.

1.7.3.- Red TOKEN-RING.

Esta Red fue patrocinada por IBM y apareció a finales de 1985. Sus principales características son las siguientes: (Latif: Rowlance: y Adams, 1992).

1.- Topología: Anillo.
2.- Modo de Transmisión: Banda Base.
3.- Número Máximo de Nadas: 72.
4.- Velocidad de Transmisión: 4 Mbits/Segundo.

El dispositivo básico de la Red es conocido como MUA (Multi Acces Unit) cuya finalidad es la de mantener el Anillo cerrado pese a que algunas Estaciones de Trabajo no estén prendidas o estén fallando. Esta Red es altamente recomendada cuando se tiene la necesidad de que la Red se comunique con un MiniOrdenador o un "Mainframe" IBM.

Los MAU's que se ofrecen en el mercado son de 4 puertos, lo cual significa que únicamente se pueden tener cuatro máquinas conectadas a éste; sin embargo, si se requiere de más equipo en la Red, es necesario que se coloquen más unidades de este tipo.

Para que siga respetando la estructura de Anillo, es necesario que se sigan conectando las Unidades Centralizadoras entre sí, para ello cada unidad posee dos puertos adicionales mediante los cuales es posible la interconexión.

Las características del cableado para una Red Token-Ring son:

1.- Cable tipo 3 (AWG 22/24) de dos pares trenzados (Telefónico).
2.- El máximo número de nadas es 72.
3.- El máximo número de MAU's conectados en cascada es de 18.
4.- La distancia máxima de cableado entre el MAU y la Estación de Trabajo es de 150 Metros.
5.- La distancia máxima entre MAU's es de 150 Metros.

Las principales ventajas de la Red Token-Ring son:

1.- Tiempo de respuesta estable.
2.- Conecta gran cantidad de nadas.
3.- Conectividad a otros productos 18M.
4.- El Sistema Operativo IBM PC LAN, está diseñado específicamente para esta Red.
5.- Su principal desventaja es el alto costo de la Red.

CAPITULO 2:
FUNDAMENTOS DE LA TRANSMISIÓN DE DATOS SOBRE TECNOLOGíA IP (DoIP)

2.1 Orígenes y Evolución del Protocolo TCP/IP

Aunque el Modelo de Referencia OSI está universalmente reconocido, el Estándar abierto histórica y técnicamente de Internet es el Protocolo para el Control de la Transmisión/Protocolo Internet, (TCP/IP). El Modelo de Referencia TCP/lP y el Protocolo TCP/lP apilan la posible comunicación de datos entre dos ordenadores de cualquier parte del mundo, a casi la velocidad de la luz. El Modelo TCP/lP tiene una importancia histórica, al igual que las Normas que permitieron florecer a las industrias de telefonía, electricidad, ferrocarril, televisión y vídeo.

Los diseñadores de TCP/IP creyeron que los Protocolos de nivel superior deberían incluir los detalles de las Capas de Presentación y de Sesión, y crearon una Capa de Aplicación que manejaba los protocolos de nivel superior, los temas de representación, de codificación y el control del diálogo. TCP/lP combina todos los temas relacionados con la aplicación en una sola capa, asegurando así que los datos serán empaquetados correctamente por la capa siguiente. A esta Capa también se le conoce como Capa de Proceso.

Esta tecnología tiene su origen en el Gobierno de los Estados Unidos de Norte América, concretamente en su Departamento de Defensa (000). La DARPA (Defense Advanced Research Projects) comenzó a trabajar con una Internet (red de redes) a mediados de los años 70.
Las dos razones principales por las que el departamento de defensa creó el estándar de los protocolos de comunicación para una arquitectura fueron las siguientes:

- Una rápida proliferación de las computadoras y otros elementos de procesamiento de señales dentro de la milicia y la necesidad de conectar equipos de diferentes fabricantes.
- El creciente uso de redes de comunicaciones en la milicia y la necesidad de una variedad de tecnologías de interconexión.

El decremento del costo del “hardware” de las computadoras y su creciente poder había provocado un aumento en el uso de las minicomputadoras y microcomputadoras para manejar una amplia variedad de tareas. El reforzar esto provocó la superioridad del procesamiento distribuido de datos sobre los “mainframes” tradicionales y su proceso centralizado de datos. Las principales ventajas que el procesamiento distribuido ofrecía en ése momento son: alto rendimiento y la disponibilidad de aplicaciones. Así pues, se pensó en comunicar los equipos de procesamiento de datos de varios fabricantes entre sí; tradicionalmente el software de comunicaciones desarrollado por un fabricante no era compatible con el de los demás. Al mismo tiempo, hubo un rápido incremento en el uso de redes de comunicaciones de datos dentro del DoD.

Para enfrentar estas necesidades, el 000, a través de la Agencia de Comunicaciones de la Defensa (DCA - Defense Communications Agency) desarrolló un conjunto de protocolos militares estándares que ofrecen las siguientes ventajas:

- Interoperabilidad
- Eficiencia y productividad del fabricante
- Competitividad

2.1.1.- Uso de los Protocolos del Departamento de Defensa (DoD) por Instalaciones No Militares.

Un desarrollo interesante e inesperado ha incrementado el uso de TCP/IP en aplicaciones no militares. Esto se debe a la introducción de la Arquitectura de Sistemas de Redes (SNA - System Network Architecture) por parte de IBM en 1974 o a la introducción de otras arquitecturas propietarias de comunicaciones creadas por otros fabricantes que obligan al cliente a permanecer ligado al hardware del mismo.

Este tipo de arquitecturas propietarias ha forzado a los fabricantes y a sus clientes a usar estándares internacionales basados en la arquitectura del modelo OSI. Sin embargo, para sorpresa de muchos observadores, una gran cantidad de clientes se ha optado por la familia de protocolos TCP/lP.

2.1.2 Cronología

1969: DoD construye una red de área amplia de cuatro nodos: ARPANET, para demostrar la factibilidad de la tecnología de intercambio de paquetes. Fue un éxito.

1972: Se da a conocer ARPANET al público y comienzan los trabajos para el desarrollo de una segunda generación de protocolos para usar la experiencia obtenida. Esta red se usó varios años para proyectos de investigación científicos y del ejército.

1980: La Universidad de California en Berkeley recibió el patrocinio del 000 para el mejoramiento del sistema operativo UNIX con capacidades de cómputo distribuido, éste sistema operativo había sido desarrollado originalmente en los Laboratorios Bell y posteriormente esta Universidad lo adoptó. El resultado fue el desarrollo de sistema UNIX 4.1 BSD, el cual corría en máquinas VAX de DEC. Este sistema operativo entre otras mejoras incluía soporte para redes locales a través de NCP y TCP.

1982: Se especificó una familia de nuevos protocolos, sujetos a exhaustivos experimentos. Los dos principales miembros de esta familia fueron el Protocolo de Control de Transmisiones (TCP - Transmission Control Protocol) y el Protocolo Internet (IP - Internet Protocol). Actualmente a estos protocolos se les conoce como la familia de protocolos TCP/lP.

1983: Se comienza a utilizar el protocolo TCP/lP en la red ARPANET del 000 como el protocolo estándar al mismo tiempo se derivaba MILNET, una segunda red surgida de la ARPANET. MILNET se encargaba de las tareas relacionodos con la investigación militar y, junto con ARPANET y otras redes clasificadas, se conocieron como la Red de Datos de la Defensa (DON - Defense Data Network). Existen gateways (compuertas) entre ARPANET y MILNET para facilitar el intercambio de información entre ellas.

Las oficinas del ARPA se responsabilizaron de las actividades de investigación y desarrollo de varios grupos académicos y comerciales, entre los que se encontraban SRI Internacional, de la Universidad de Stanford, la UCLA, el MIT, la corporación RANO, la Universidad de California en Santa Bárbara, la Universidad de Utah y otros. Estos grupos desarrollaron gran parte de los conceptos que actualmente permiten la comunicación en redes locales y remotas.

En realidad, TCP/IP es la segunda generación de protocolos desarrollada por la comunidad ARPA. La primera generación fueron aquéllos protocolos creados en diferentes hosts independientes, tales como los protocolos punto a punto (Network Control Protocol, precursor de TCP/IP) y el de punto a multipunto (lMP, precursor de X.25).

2.2 Familia ("Stack") de Protocolos TCP/IP

TCP/IP es una colección de protocolos. Debe su nombre a sus dos protocolos más conocidos; TCP o Transmission Control Protocol, corresponde a la capa 4 del modelo de OSI (la capa de transporte) y ofrece transmisión confiable de datos. IP o Internet Protocol trabaja en la capa 3 del Modelo OSI (capa de enlace de red) y ofrece el servicio de datagramas sin conexión.

2.2.1.- TCP/IP y la Internet.

Las redes se han convertido en una parte fundamental, (se puede decir la más importante), de los sistemas de información de hoy. Forman la espina dorsal ("Backbone') para compartir información dentro de empresas, grupos empresariales y científicos.

La mayoría de estas redes fueron instaladas en la década de los 60 y 70, cuando el diseño de red era el asunto de investigación más importante relacionado a la computación. Dio lugar a múltiples modelos de "Networking" tales como tecnología de conmutación de paquetes, detección colisiones en redes de área local, redes jerárquicas de la empresa, y muchas otras tecnologías excelentes.

Desde el inicio de 70, otro aspecto de "Networking" tendió a ser importante: protocolo en capas, que permite que las aplicaciones se comuniquen una con otra. Un rango completo de arquitecturas de modelos fue propuesto e implementados por varios equipos de investigadores y fabricantes de computadoras.

El resultado de todos estos grandes conocimientos técnicos es que cualquier grupo de usuarios puede encontrar hoy una red física y una conveniente arquitectura de modelo para sus necesidades específicas. Esto se extiende desde líneas asíncronas baratas sin otra recuperación de error que una función de la paridad de bit por bit, hasta amplias funciones de las redes de área amplia (públicas o privadas) con protocolos confiables tales como redes públicas de conmutación de paquetes o redes privadas SNA, para redes de área local de alta velocidad pero distancia limitada.

El compartir esta información es una situación complicada cuando un grupo de usuarios desea extender su sistema de información a otro grupo de usuarios quienes tienen una tecnología y red protocolos diferentes. Consecuentemente, si pudieran acordar en un tipo de tecnología de red para interconectar físicamente las dos localidades, sus aplicaciones todavía no podrían comunicarse porque tienen diferentes protocolos.

Esta situación fue reconocida a principios de los años 70´s por un grupo de investigadores de los Estados Unidos de América, que llegaron con un nuevo principio: "Internetworking". Otras organizaciones oficiales llegaron a estar implicadas en esta área de interconectar redes, tales como ITU-T (antes CCITT) e ISO. Todos estuvieron tratando de definir un conjunto de protocolos, distribuidos en una suite bien definida, de modo que la aplicación pudiera comunicarse con otras aplicaciones, sin importar la tecnología de red subyacente y el sistema operativo donde estas aplicaciones corren.

Hoy, el Internet el World Wide Web y la supercarretera de la información, son términos familiares para millones de personas en todo el mundo. TCP/IP es la familia de protocolos desarrollada para Internet.

2.3 Asociación de TCP/IP con OSI

Todos los protocolos de comunicación de datos tienen el mismo objetivo: mover datos entre aplicaciones sobre diferentes dispositivos. Diferentes métodos han sido desarrollados para cumplir con este objetivo, cada protocolo debe proveer la funcionalidad marcada en las capas del Modelo de Referencia OSI.

TCP ofrece servicios de la capa de transporte, e IP los de la capa de red. Fueron desarrollados para propósitos de la IFIP, el Technical Committee Working Group y la DARPA, la cual originalmente había combinado las funciones de conexión entre redes y las de transporte confiable dentro de un solo protocolo. El subsecuente desarrollo de otros protocolos de transporte separó estas funciones para que el IP se encargara de la función de interconexión entre redes donde TCP proporcionaría los circuitos virtuales confiables.

En la figura 2.1 se puede observar el Modelo de Referencia OSI contra la familia de protocolos TCP/lP.

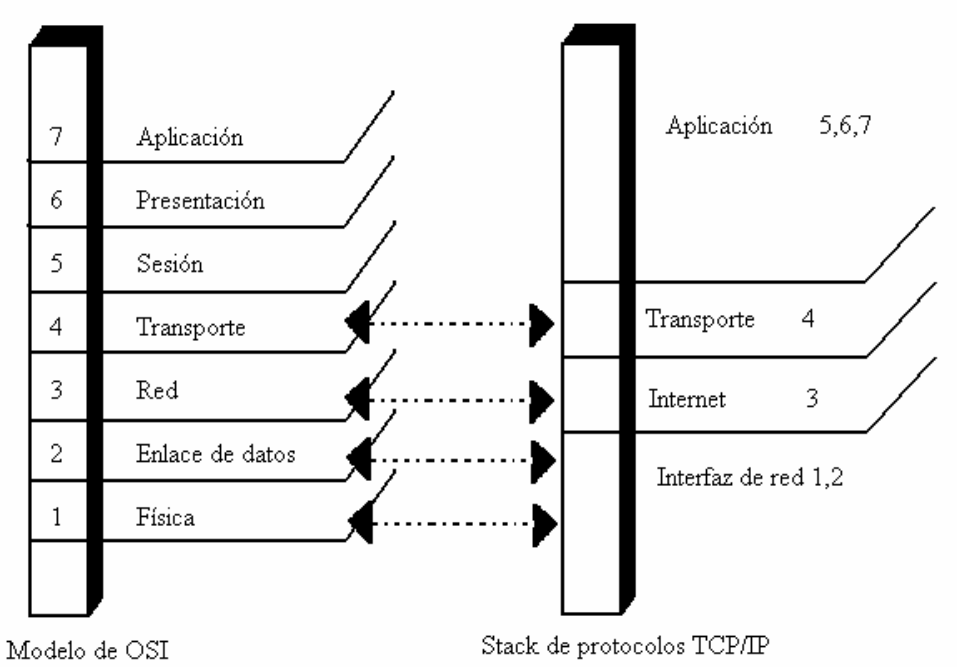


Figura 2.1 Modelo de referencia OSI y Stack de protocolos TCP/IP

2.4.- Componentes de Redes TCP/IP.

TCP/lP es un protocolo definido principalmente por las siguientes capas:

- Capa de Acceso a Red.
- Capa de “/nternetwork”.
- Capa de Transporte.
- Capa de Aplicación.

La Capa de Acceso a Red es la capa más baja en el modelo de referencia. Los servicios de los dos principales protocolos (TCP e IP) son aumentados por las aplicaciones de los niveles superiores. Como se había visto, TCP/lP se refiere a una gran familia de servicios y protocolos. Estos protocolos aparecen en la figura 2.2, la cual muestra que IP y los protocolos de los niveles superiores se pueden implantar en diversos tipos de redes.

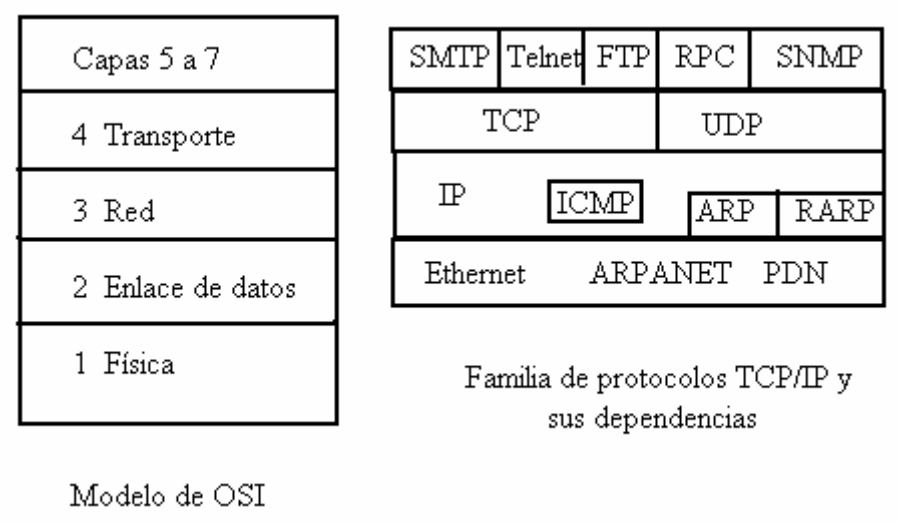


Figura 2.2 Familia de servicios y protocolos

A continuación se muestra una lista con los nombres de los protocolos más comunes y los servicios que ofrecen:

- IP (Internet Protocol). Entrega de datagramas sin conexión.
- ICMP (Internet Control Message Protocol). Usado por los “gate ways “ y “hosts” para evaluar las condiciones de funcionamiento de los servicios IP.
- ARP (Address Resolution Protocol). Mapea una dirección IP a su dirección Ethernet asociada.
- RARP (Reverse ARP). Mapea una dirección Ethernet a su dirección IP asociada.
- TCP (Transmission Control Protocol). Protocolo orientado a la Conexión con acuse de recibo.
- UDP (User Datagram Protocol) Protocolo sin conexión no confiable.
- SMTP (Simple Mail Transfer Protocol) Envío y recepción de correo.
- FTP (File Transfer Protocol) Intercambio de archivos completos.
- TELNET (Telecommunications Network) Terminal virtual para acceso interactivo a servidores remotos.
- NFS (Network File System) Sistemas de Archivos Distribuidos.
- SNMP (Simple Network Management Protocol) Servicios de Administración Centralizada de Sistemas Remotos.

2.5 Capa de Internet protocol (IP).

La relación de IP con el Modelo de OSI se representa como se muestra en la figura 2.3

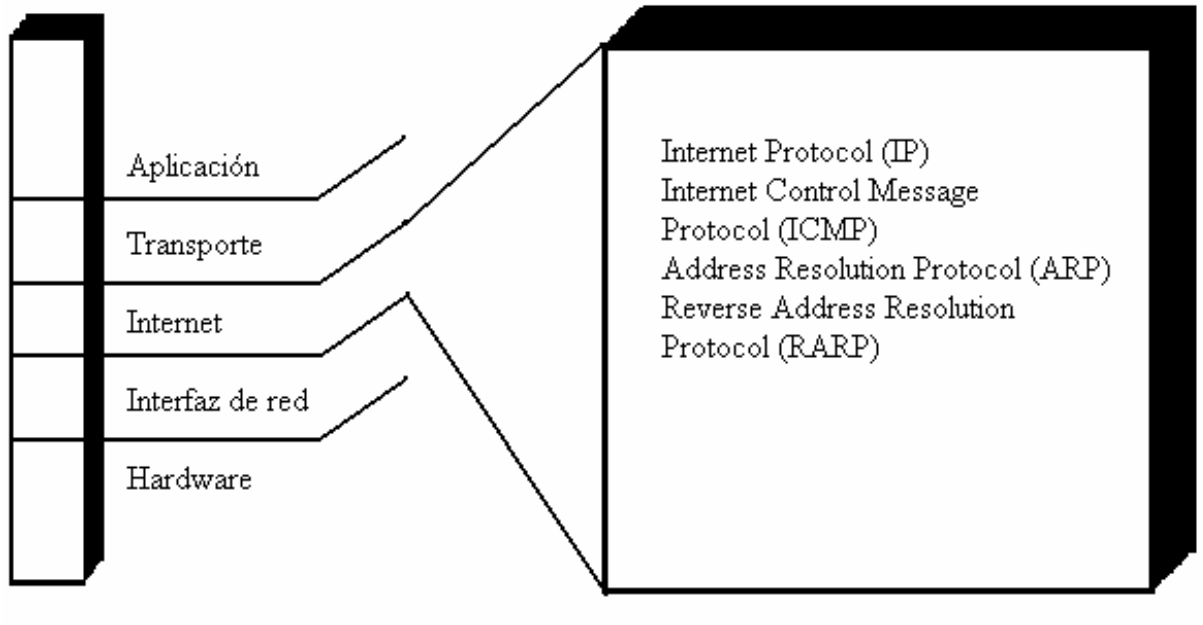


Figura 2.3 Relación IP y OSI

El Internet Protocol (IP), esta definido por el RFC 791, y es el corazón de la capa de Internet. IP provee un esquema de direccionamiento conocido como IP "Address" o dirección lógica. Tiene el propósito de conocer la dirección a la cual se desea enviar u obtener información.

La analogía entre una red física y una Internet TCP/lP es muy fuerte. En una red física, la unidad de transferencia es un "Frame" que contiene un encabezado y datos, donde el encabezado proporciona información tal como las direcciones fuente y destino (físicas).

La Internet le llama datagrama de Internet a su unidad básica de transferencia, al que frecuentemente se le llama datagrama IP o simplemente datagrama. Al igual que un "Frame" típico de una red física, un datagrama se divide en áreas del encabezado y de datos.

El encabezado del datagrama contiene las direcciones fuente y destino y un campo de tipo que identifica el contenido del datagrama. La diferencia, por supuesto, es que el encabezado del datagrama contiene direcciones IP mientras que el encabezado de un "Frame" contiene direcciones físicas. La figura 2.4 muestra la disposición de los campos del datagrama.

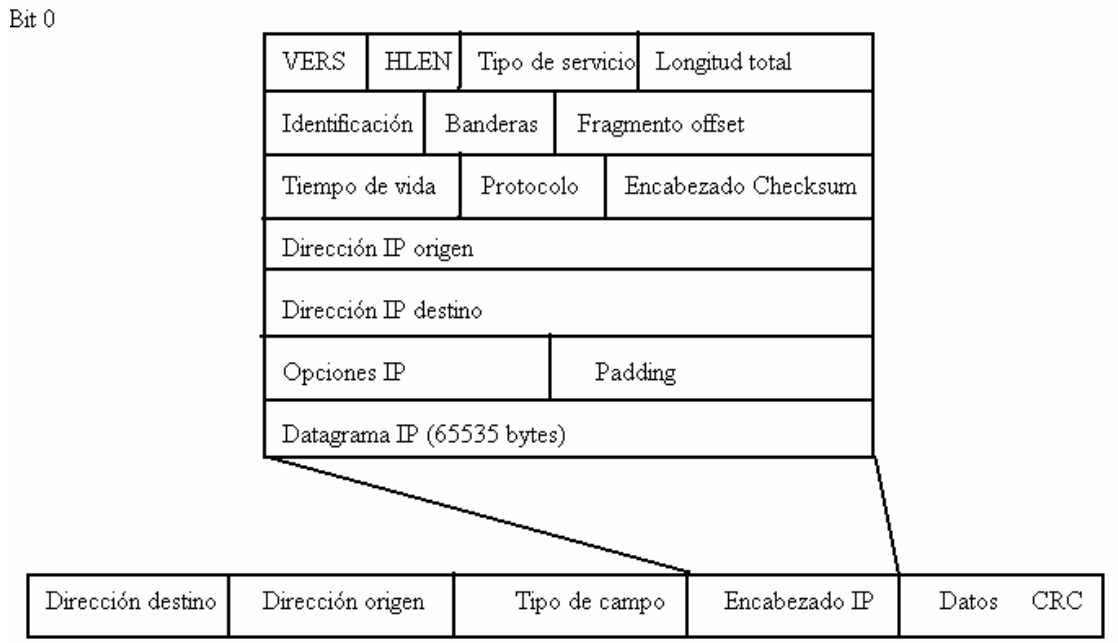


Figura 2.4 Campos del datagrama

2.5.1 "Frame" de Internet Protocol (IP).

Los campos relevantes de la porción de la cabecera de IP son:

- Versión, se está utilizando la versión 4 lo que indica que el direccionamiento de IP es de 32 bits.
- Identificación, en caso de ser fragmentado algún paquete entre los puntos intermedios el mismo debe ser reensamblado y se usa este campo para identificar información del mismo.
- Protocolo, tipo de protocolo que usaran las capas superiores.
- Checksum, método de verificar la integridad de la cabecera.
- Direcciones IP fuente y destino dirección IP de 4 bytes o su equivalente en bits (32).
- Tamaño del datagrama, MTU de la Red y Fragmentación.

En el mejor de los casos, el datagrama IP entero cabría en un "Frame" del servicio que se está utilizando haciendo la transmisión a través de la red eficiente. Para lograr tal eficiencia, los diseñadores de IP tuvieron que seleccionar un tamaño máximo de datagrama que le permitiera siempre caber en un "Frame".

Para entender el problema, se necesita un hecho acerca del hardware de red: cada tecnología de intercambio de paquetes pone un límite en la cantidad de datos que se pueden transportar en un "Frame" físico. Por ejemplo, Ethernet limita las transferencias a 1500 octetos[7] de datos mientras que proNET permite 2044 octetos por Frame. A este límite se le llama MTU (Maximum Transfer Unit) de la red. Los MTU pueden ser pequeños: algunas tecnologías limitan las transferencias a 128 octetos o menos. El limitar los datagramas para que quepan en el MTU más pequeño de la Internet, haría las transferencias ineficientes cuando esos datagramas pasaran por redes que pudieran llevar "frames" de mayor tamaño.

Sin embargo, permitir que los datagramas sean más grandes que el MTU mínimo en una Internet significa que un datagrama no siempre cabrá en un solo 'Frame" de la red.

La elección debería ser obvia: el objetivo en el diseño de Internet es ocultar las tecnologías de red subyacentes y hacer la comunicación conveniente para el usuario. Así, en lugar de diseñar datagramas que se adhieran a las restricciones de las redes físicas, el software de TCP/IP escoge un tamaño inicial de datagrama conveniente y busca la manera de dividir los datagramas más grandes en piezas más pequeñas cuando el datagrama necesite atravesar una red que tenga un MTU pequeño. Las pequeñas piezas en las que se divide un datagrama se llaman fragmentos, y el proceso de dividir un datagrama se conoce como fragmentación, esto se ilustra en la figura 2.5.

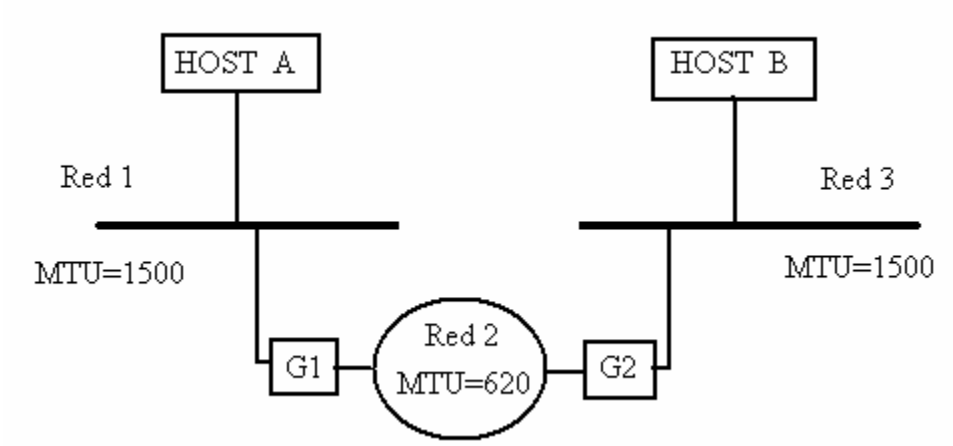


Figura 2.5 Fragmentación

En una internet TCP/lP, una vez que un datagrama se ha fragmentado, los fragmentos viajan como datagramas separados todo el camino hasta el destino final donde son reensamblados. Este procedimiento es posible por el campo que identifica al datagrama.

Siempre que una máquina inyecta un datagrama a la Internet, le da un tiempo de vida máximo para que el datagrama pueda sobrevivir. Los “gateways” y “hosts” que procesan los datagramas deben decrementar este valor a medida que el tiempo pasa y eliminar el datagrama de la Internet cuando su tiempo de vida expira.

2.5.2 Direccionamiento IP

Las redes interconectadas no tienen ninguna razón para disponer del mismo mecanismo de direccionamiento de los nodos. Por lo tanto, es necesario dar una dirección lógica (dirección IP) a cada nodo.
Una dirección IP está compuesta de 4 bytes (32 bits) y esta dividida en dos partes, los bits más significativos (MSBs) identifican una RED en particular y los demás bits especifican un NODO perteneciente a esa red.
Todos los nodos que se localizan en la misma red, deben coincidir en la parte correspondiente a la dirección de Red, sin embargo la parte que identifica a la dirección de Nodo debe ser diferente.
Estos 32 bits de dirección IP se escriben normalmente como cuatro números decimales, en el rango de O a 255, separados por un punto, uno para cada byte de dirección: Se expresa en formato X.X.X.X . El máximo valor para cada octeto es de 255. Por ejemplo 192.100.180.15

Para aprovechar de manera más eficiente el espacio de direccionamiento IP y ajustar el tamaño de las redes a las necesidades individuales de cada entidad, el InterNIC clasificó las redes de Internet en cinco clases de direccionamiento, Clase A, Clase B, Clase C, Clase D, Clase E. Cada red Clase A agrupa alrededor de 16,000,000 direcciones únicas, la clase B agrupa aproximadamente 65,000, y la clase C solo agrupa 254 direcciones diferentes. La Clase a la que pertenece una dirección de IP define cuantos de los 32 bits deberán ser interpretados como dirección de Red y cuantos como dirección de Nodo .

Clase A	R.N.N.N	8 bits red – 24 bits nodo
Clase B	R.R.N.N	16 bits red – 16 bits nodo
Clase C	R.R.R.N	24 bits red – 8 bits nodo

Los bits más significativos de la porción de red determinan la clase de dirección; esto se muestra en las siguientes tablas, así como las clases de dirección IP y sus respectivos rangos:

Clase	primer octeto
A	0XXXXXXX
B	10XXXXXX
C	110XXXXX

Clase	Primer byte de la dirección
A	1-127
B	128-191
C	192-223

Ejemplos:

128.128.45.6	204.87.205.129
Clase B	Clase C
Red 128.128	Red 204.87.205
Nodo 45.6	Nodo 129

2.5.2.1 Redes Clase A.

Para las redes clase A, el primer bit siempre es O, los siguientes 7 bits, determinan el número de RED, y los siguientes 24 bits, determinan el número de nodo.

De este modo el direccionamiento de la clase A debe de tener un rango de números de dirección de 1.0.0.0 hasta 126.0.0.0, la primera y la última dirección (O.x.x.x y 127.x.x.x) están reservadas. Esto es 126 posibles redes clase A.

El número de direcciones por red clase A es de 16,777,214, esto es dos menos que dos elevado a la potencia 24, debido a que los números de host 0.0.0 y 255.255.255 (La primera y la última dirección de cada red), están reservadas.

2.5.2.2 Redes Clase B.

Para una dirección clase B los primeros dos bits son 10, mientras que los siguientes 14 bits identifican el número de red y los 16 restantes el número de “host”. La clase B incluye los números de red en el rango de 128.1.0.0 al 191.254.0.0, la primera y la última dirección (128.0.x.x y 191.255.x.x) están reservadas.

Esto permite un total de 16,382 redes con un total de 65,534 direcciones de “host” cada una (La primera y la última dirección de cada red, están reservadas).

2.5.2.3. Redes Clase C

Para una red clase C, los tres primeros bits de la dirección son 1, 1 Y 0, los siguientes 21 bits identifican la red y los últimos 8 el “host”. Así, el direccionamiento de la clase e incluye los números de red en el rango que va de 192.0.1.0 hasta 223.255.254.0, la primera y la última dirección (192.0.0.x y 223.255.255.x) están reservadas. Esto permite un total de 2,080,798 redes

clase C, con un total de 254 direcciones de “host”. (La primera y la última dirección de cada red, están reservadas).

2.5.2.4 Redes Clase D y E

Finalmente, tenemos las direcciones de la clase D y la clase E. Las de clase D empiezan en 224.0.0.0 y se usa para “Multicast”. A diferencia de un “Unicast” (mensaje para uno nodo) y de un “Broadcast” (mensaje para todos los nodos) un ‘multicast’ es un mensaje para un grupo de nodos. Las direcciones de la clase E empiezan en 240.0.0.0 y se usan frecuentemente sólo para propósitos experimentales.

2.6.- Restricciones en Direcciones IP

Los nodos deben tener dirección de nodo diferente a la CERO (puros bits en cero). La dirección de nodo con puros unos se reserva para “Broadcasts “. En ocasiones, tenemos que dividir una red grande en varias pequeñas para:

- Reducción de tráfico.
- Optimizar prestaciones (“performance’).
- Simplificar la administración.

Para esto, recurrimos al uso de subredes, que no son otra cosa más que una extensión a la dirección de Red. Para hacer la extensión se utilizan la máscara de red (“Netmask’).

Una dirección de IP es de 32 bits, escritos como 4 octetos separados con un punto. Una máscara de red también es de 32 bits, escritos como 4 octetos. La máscara de red se construye de la siguiente forma:

1 binario en posiciones de dirección de Red
0 binario en posiciones de dirección de nodo

La máscara de red indica que bits de la dirección de Nodo se deberán de interpretar como dirección de red.

Las máscaras de red por default son:

CLASE	DIRECCION	MASCARILLA
A	RN.N.N	255.0.0.0
B	RRN.N	255.255.0.0
C	RRR.N	255.255.255.0

Para la interpretación de las direcciones de IP por un Ruteador (“Rou ter[Jl]), se aplica un AND lógico entre la dirección de IP y la máscara de red, con esto lo que se hace es eliminar la dirección de Nodo y solo dejar la dirección de Red.

Operación del AND lógico:

0&0=0
0&1=0
1&0=0
1&1=1

Ejemplo:

Interpretación de las direcciones IP				
131.108.66.16	10000011	01101100	01000010	10100000
255.255.0.0	11111111	11111111	00000000	00000000
AND	10000011	01101100	00000000	00000000
	131	108	0	0
	Red	Red	Nodo	Nodo

2.6.1 Direcciones IP Especiales o Reservadas.

Existen dos direcciones IP que tienen una interpretación particular, cualquiera que sea el tamaño de la red.

La dirección donde todos los bits son 0's permite hacer referencia a la red o a la máquina actual (0.0.0.0).

La dirección donde todos los bits son iguales a 1 se utiliza para direccionar un mensaje a todas las máquinas de la red ("Broadcast"), esto es: 255.255.255.255, el "Broadcast" se puede decir que es una dirección en la que todos los integrantes del segmento de red al que se pertenece deben de prestar atención, con la finalidad de procesar los datos que se están enviando, y al mismo tiempo saber si un nodo es el que debe responder a tal solicitud.

2.7 Resolución de Direcciones

2.7.1 "Address Resolution Protocol" (ARP).

Tomando como referencia al paquete de ETHERNET versión 2, y prestando atención en el encapsulamiento de la porción de las direcciones destino y origen del mismo.

Dirección de destino	Dirección de origen	Tipo de servicIo	Datos, incluyendo IP	CRC
6 bytes, MA Address	6 bytes, MAC Address	2 bytes	MTU, hasta 1500 bytes	4 bytes

La información en el concepto de un datagrama, incluye la porción de IP y la información de capas superiores de transporte o aplicativos ya definidos.

Veáse a más a detalle un encapsulamiento total por parte de Ethernet, desde la definición de inicio hasta el término de del datagrama del mismo, Los datos están incluidos desde que parte final del campo de tipo de servicio, sin embargo para establecer la comunicación, entre dos "hosts" es necesaria la dirección MAC tanto del origen como del destino. La dirección MAC del origen, es por razón obvia conocida.

Para poder establecer la comunicación entre dos "hosts" es indispensable conocer la dirección MAC de destino, por lo que se envía a la red un paquete para obtener la dirección MAC de destino, a este servicio se le llama ARP, Address Resolution Protocol. De una dirección IP conocida se puede obtener una dirección MAC desconocida. La figura 2.6 muestra el formato de un mensaje ARP sobre Ethernet.

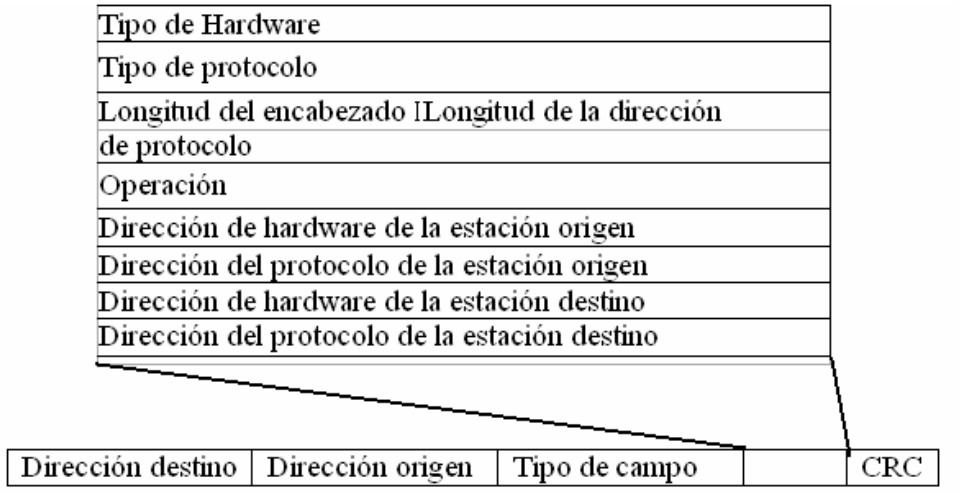


Figura 2.6 Formato de un mensaje ARP sobre Ethernet

Hay que hacer notar que el servicio de solicitud de la red es un servicio de ETHERNET y la dirección de destino también debe llevar un campo, mismo que se llena con una dirección de "Broadcast".

ARP permite la designación de tipos específicos de tarjetas de red (Ethernet, Token Ring, etcétera). De esta manera, cuando el "host" solicitante recibe un datagrama ARP también puede obtener información del tipo de tarjeta que aquélla máquina esté usando. Sobre el servicio de red que está utilizando.

2.7.2 "Reverse Address Resolution Protocol" (RARP).

Lo contrario al trabajo realizado por ARP en donde se conoce la dirección física pero no se conoce la dirección IP. Los mensajes de este protocolo tienen el mismo formato que los de ARP. Un ejemplo del uso de RARP es, el caso de una estación de trabajo sin disco duro ("Diskless').

Cuando la estación es inicializada, leerá su dirección física de ROM pero necesitará conocer su dirección IP, entonces manda un mensaje RARP a todas las máquinas ("Broadcast') solicitando su dirección IP. En este caso deberá existir un servidor que reconozca el mensaje de la estación, cambie el código del mensaje a Respuesta de Solicitud y que copie la dirección IP de la estación desde sus tablas de mapeo internas hacia el mensaje RARP y lo envíe de regreso.

2.8 Mensajes de Control

2.8.1 "Internet Control Message Protocol" (lCMP)

Un Datagrama viaja de un ruteador a otro hasta llegar a aquel que pueda enviar al datagrama directamente a su destino final. Si un ruteador no puede enviar un datagrama, o si el ruteador detecta una condición inusual que impida al ruteador enviar el mensaje (ejemplo, congestión en la red), el ruteador necesita informar al "host" origen ("host" donde se origino el mensaje), para que éste ignore esta situación o corrija el problema. Esta sección discute el mecanismo que ruteadores y "hosts" usan para comunicar tal información de control. Los ruteadores utilizan tal mecanismo para reportar problemas y los "hosts" lo usan para probar si el destino puede ser alcanzado.

2.8.2 Servicios de ICMP (Internet Control Messaging Protocol)

El Internet Control Messaging Protocol (ICMP), es un protocolo de la capa de Internet (capa 3) que proporciona mensajes de reporte de error y otro tipo de información relevante al ruteo y envío de paquetes IP. ICMP está descrito en el RFC 792 y actualizado en el RFC 950.

Cuando un ruteador o un “host” destino debe informar al “host” fuente sobre los errores en el envío o ruteo del datagrama, usa ICMP. ICMP se caracteriza por:

Usa IP como si fuera un protocolo de nivel superior (esto es, los mensajes de ICMP están encapsulados en datagramas IP). Sin embargo ICMP es una parte integral de IP y debe ser implementada por cada modulo de IP.

Es usado para reportar algunos errores, no para hacer confiable a IP. Los datagramas pueden ser no enviados y no existir algún reporte al respecto. La confiabilidad debe ser implementada por protocolos de nivel superior que usa IP.

Puede reportar errores sobre cualquier datagrama IP con excepción de mensajes ICMP, para evitar repeticiones infinitas.

Sus mensajes nunca se envían en respuesta a datagramas que tienen una dirección destino “Broadcast” o “Multicast”.

Sus mensajes nunca se envían en respuesta a un datagrama que no contenga una dirección IP fuente, que representa un “host” único. Esto es, la dirección fuente no puede ser cero, una dirección “Ioopback”, una dirección “Broadcast” o “Multicast”.

El RFC 792 establece que los mensajes ICMP pueden ser generados para reportar errores en el procesamiento de datagramas IP. En la practica, los ruteadores por lo general siempre generaran mensajes ICMP para errores, pero para los “hosts”, el número de mensajes ICMP generados es dependiente de la aplicación.

Los mensajes ICMP están descritos en el RFC 792 y el RFC 950. Los mensajes ICMP se envían en datagramas IP. El encabezado de IP siempre tiene el número de protocolo 1, indicando ICMP y el tipo de servicio cero (rutina). El campo de datos de IP contendrá el mensaje actual ICMP en el formato mostrado en la figura 2.7.

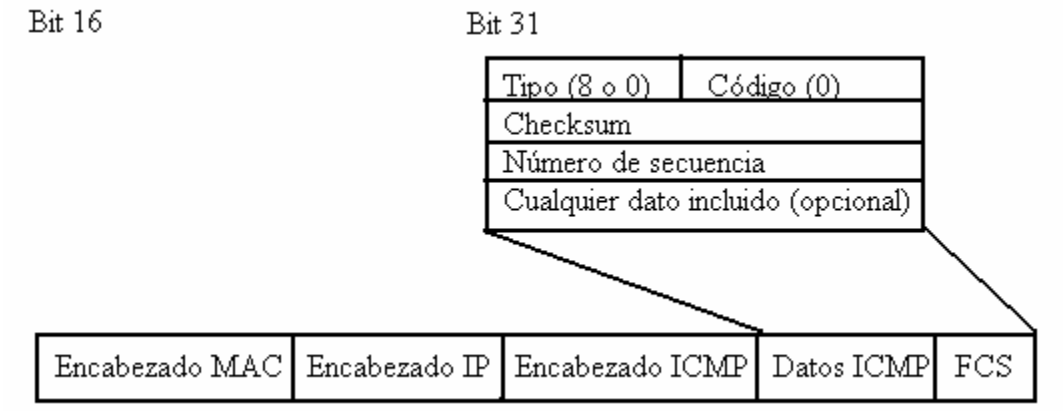


Figura 2.7 Formato del paquete ICMP para respuesta a solicitud

De la figura 2.7, se puede determinar que:

“Tipo” especifica el tipo de mensaje (Echo reply, Destination unreachable, Source quench, Redirect, echo, Router advertisement, Router solicitation, Time exceeded, Parameter problem, Time stamp request, Time stamp reply, Address mask request, Address mask reply , Traceroute, Datagram conversion error, Mobile host redirect, IPv6 Where-Are-you, IPv6 I-am-Here, Mobile registration request, Mobile registration reply, Domain name request, Domain name reply, SKIP, Photuris)

“Código” contiene el código de error para el datagrama reportado por este mensaje ICMP.

“Suma de control” contiene los 16 bits, control de suma del mensaje entero ICMP. Este algoritmo es el mismo que es usado por UDP y TCP, así como por IP.

“Datos” contiene información para este mensaje ICMP. Típicamente contendrá una parte del mensaje IP original para el cual este mensaje ICMP fue generado. La longitud de los datos puede ser determinada desde la longitud del datagrama IP que contiene el mensaje menos la longitud del encabezado de IP.

2.9.- Panorama General de IPv6

Esta sección presenta un panorama de la siguiente generación de Protocolo Internet (Internet Protocol Next Generation, IPnG). IPnG fue recomendado por el “IPnG Area Oirectors del Internet Engineering Task Force” (IETF) en la reunión de Toronto en Julio 25 de 1994, y documentada en el RFC 1752, “La Recomendación para el IPnG”. La recomendación fue aprobada por “The Internet Engineering Steering Group” en Noviembre 17 de 1994 y declarada una Norma (estándar).

El nombre formal de este protocolo es IPv6. La actual versión del protocolo Interne es versión 4 (referido como IPv4). El objetivo de esta sección es darle al lector un panorama del protocolo IPnG.

2.9.1 Limitaciones del Modelo de Direcciones IP

El Internet ha crecido sumamente rápido en años recientes, en 1994 tenia más de 32000 redes conectadas, con más de 3.8 millones de computadoras en más de 90 paises. IPv4 con un campo de direcciones de 32 bits provee más de 4 mil millones de direcciones posibles, parecería que el esquema de direcciones IP es más que adecuado para la tarea de direccionar todos los datagramas de los “hosts” en el Internet, desafortunadamente esto no es asi, por varias razones, incluyendo las siguientes:

El direccionamiento IP está dividido en dos partes, número de red y número de “host”, el cual es administrado separadamente. Aunque el espacio de direcciones dentro de una red puede ser ocupada esparcidamente, tan lejano como el espacio de direcciones IP le permita, si un número de red es usado entonces todas las direcciones dentro de esa red son ocupadas.

El espacio de direcciones para las redes esta estructurado en clase de redes A, B, C de diferente tamaño, el espacio dentro de cada una de estas clases requiere ser considerado separadamente.

El esquema de direccionamiento IP requiere que a todas las redes IP les sea asignado un número de red único, aunque actualmente estén o no conectadas al Internet.

El crecimiento de TCP/lP (usado en nuevas áreas), podría resultar en una explosión rápida del número requerido de direcciones IP. Por ejemplo, el uso extendido de TCP/lP para conectar terminales electrónicas punto de venta o para recibir cable por televisión podría incrementar enormemente el número de “hosts” IP.

El esquema de direccionamiento IPv4 con una única dirección IP por cada “host” (no ruteador) podría cambiar en un futuro (RFC 1681).

Estos factores significan que el espacio de direcciones es mucho más restringido de lo que el análisis puede indicar. Este problema es conocido como “Agotamiento de las direcciones IP”.

2.9.2.- IP la Siquiente Generación (lPnG).

Métodos para resolver el problema de agotamiento de direcciones IP ya se están empleando, pero eventualmente, el espacio de direcciones IP será agotado.

E2ETF (“Internet Engineering Task Force’) tiene un grupo trabajando sobre las expectativas del tiempo de vida del esquema de direcciones IP (“Address Lifetime Expectetions”, ALE) con el propósito de proporcionar una fecha estimada cuando las direcciones IP se agoten, actualmente las expectativas son (como lo informó ALE en diciembre de 1994) son que el espacio de direcciones IP estará agotado en algún momento entre el 2005 y el 2011.

Antes que esto pase un reemplazo a la versión actual de IP (IPv4), fue necesario. Este reemplazo es conocido como IP: la Nueva Generación (IP: “The Next Generation”, IPnG), la versión actual es conocida como IP (versión 4), referida como IPv4.

Existen varios grupos de trabajo relacionados con el funcionamiento de IPng; estos grupos son temporales y se espera que sean unidos a otros grupos de trabajo en otras áreas cuando el proceso de definición de IPnG concluya.

En Julio de 1994 en la reunión del IETF en Toronto, el IPnG “Area Directors” del IETF presento el RFC 1752 - la recomendación para el IP “Next Generation Protocol”. La recomendación fue aprobada por el IETF en Noviembre de 1994 y se hizo una norma (estándar).

Estos eventos fueron la culminación de mucho trabajo y discusión, el cual involucro a muchas partes interesadas. El consejo de administración publicó el RFC 1550-IP, donde se establecen los requerimientos para IPnG. Los requerimientos más importantes son:

Un espacio de direcciones dramáticamente más grande: al menos 10 redes (superscript 9), preferentemente 10 (superscript 12); y al menos 10 “hosts” (superscript 12), preferentemente 10 (superscript 15). Al menos 1 billón de redes, preferentemente 1000 billones; y al menos 1000 veces como host. Esto permitiría incrementar considerablemente el uso de las direcciones IP y al mismo tiempo permite que el espacio de direcciones IP sea extensamente poblado permitiendo a las direcciones IPnG tener más estructura que la posible en IPv4. IPnG debe:

- Permitir el encapsulamiento de su propio paquete o de otros protocolos.
- Permitir agregar clases de servicios para distinguir tipos de datos que están siendo transmitidos, como por ejemplo, tráfico isócrono como real-time audio y vídeo.

- Proporcionar direccionamiento “Multicast”, de forma que este completamente más integrado con el resto del conjunto (“suite’) de protocolos que la implementaron actual.

- Proporcionar Autentificación (“Authentication’) y Encriptación (“Encryption’).

- Preservar las virtudes de IPv4: robustez, independencia de las características físicas de la red, alto desempeño, topología flexible, extensibilidad, servicio de datagramas, direccionamiento globalmente único, un protocolo de control internamente construido, estándares libremente disponibles.

- Comprender un plan de transición sencillo en su implementación.

- Coexistir con IPv4.

2.9.3 IP Versión 6 (IPv6)

Existieron tres propuestas principales para IPnG: Common Architecture for the Internet (CATNIP), TCP and UDP whit Bigger Address (TUBA), Simple Internet Protocol Plus (SIPP).

El Consejo de Administración determinó que las tres propuestas fueron insuficientes para cumplir con la lista de requerimientos aceptada, pero que SIPP, como se definió en RFC1710, era la propuesta más cercana a la lista de requerimientos.

Después de algunos cambios a la propuesta original, por la instancia de usar 128 bits en lugar de 64 bits de direccionamiento, el Consejo de Administración de IPnG dictaminó que SIPP era la base para IPnG y que características de las otras propuestas podrían ser agregadas para cubrir el resto de los requerimientos. La solución propuesta fue llamada IP Versión 6(IPv6).

IPv6 usa el término paquete en lugar de datagrama, pero el significado es el mismo, aunque los formatos son diferentes. IPv6 introduce un nuevo término, nodo, para un sistema corriendo IPv6, que puede ser un “host” un ruteador. Un “host” IPv6 es un nodo que no reenvía paquetes IPv6 los cuales no están explícitamente direccionados hacia él. Un ruteador es un nodo el cual reenvía paquetes IP no direccionodos hacia él.

2.9.3.1 Formato del Encabezado de IP, (IPv6 Header)

IPv6 incrementa la longitud del encabezado (“header”) de IP de 20 bytes a 40 bytes. El encabezado de IPv6 contiene dos direcciones de 16-bytes cada una (origen y destino) precedidas por 8 bytes de información de control.

El encabezado de Ipv4 tiene dos direcciones de 4 bytes cada una precedida por 12 bytes de información de control y seguido posiblemente por datos de opción. La reducción del control de información y la eliminación de opciones en el encabezado tiene por objeto optimizar el procesamiento de la mayoría de los datagramas (paquetes). Los campos frecuentemente no usados han sido removidos del encabezado, fueron movidos al encabezado opcional de extensiones.

Los campos del encabezado de IPv6 son:

- Vers: 4-bits número de versión del protocolo Internet: 6

- Flow Label: 28-bits ver descripción ella sección Flow Label

- Payload Length: La longitud del paquete in bytes (no incluido el encabezado) codificado como un entero sin signo de 16 bits, si la longitud es mayor a 64KB este campo es 0 y un encabezado opcional proporcional la longitud real.

- Next Header: Indica el tipo de encabezado inmediatamente después de este encabezado. Este encabezado es el mismo que el usado para el número de protocolo en IPv4.

El siguiente encabezado también es usado para indicar la presencia del encabezado de extensión, el cual proporciona el mecanismo para agregar información adicional al paquete de IPv6. Los siguientes valores son importantes:

41 IPv6 Header
43 IPv6 Routing Header
44 IPv6 Fragment Header
51 IPv6 Authentication Header
? IPv6 End-to-End Options Header
? IPv6 ICMP Packet

Los valores, excepto los últimos dos, están incluidos en STO 2 (Assigned Internet Numbers), Aunque la edición actual de STO 2 (RFC 1700) menciona como protocolo a SIP o SIPP. Cabe hacer mención de algunos conceptos importantes:

- "Hop Limit" es el campo TTL en IPv4, pero no es medido en saltos ni segundos. Fue cambiado por dos razones: IP normalmente envía los datagramas más rápido que un salto por segundo y el valor de TTL es siempre decrementado en cada salto, en la práctica es medido en saltos y no en segundos. Muchas implementaciones de IP, no expiran datagramas de salida, sobre la base de tiempo transcurrido.

- "Source Address" es una dirección de 128-bits.

- "Destination Address" es una dirección de 128-bits. Una comparación entre el encabezado de Ipv4 e Ipv6 mostrara que existen campos en el encabezado de IPv4 no tienen campos equivalentes en IPv6.

- "Type of service". El tipo de servicio que será manipulado usando el concepto de flujo (flow).

- "Identification, Fragmentation y Fragment Offset" son los paquetes fragmentados, y tienen un encabezado de extensión mucho mejor que el de Información de Fragmentación en el encabezado de IPv6. Esto reduce el tamaño del encabezado básico de IPv6. Los protocolos de alto nivel, particularmente TCP, tienden a evitar la fragmentación de datagramas, esto reduce los "overhead" para el caso normal, Ipv6 no fragmenta los paquetes en la ruta hacia sus destinos, únicamente en la fuente ("source').

- "Header Checksum" .Debido a que los protocolos de transporte implementan "checksum", y porque IPv6 incluye un encabezado opcional de autentificación que se puede utilizar para asegurar la integridad, IPv6 no proporciona monitoreo del "checksum" de los paquetes de IP. TCP y UDP incluyen un pseudo encabezado IP en el "checksum" que ellos usan, en este caso, el encabezado de IP en IPv4 es verificado dos veces. TCP y UDP, y cualquier otro protocolo que usa los mecanismos de "checksum", trabajando sobre IPv6 continuarán usando un pseudo encabezado IP aunque, el formato del pseudo encabezado IPv6 será diferente del encabezado de IPv4. ICMP e IGMP y

cualquier otro protocolo que no utilice un pseudo encabezado IP sobre IPv4 usara un pseudo encabezado IPv6 en su “checksum”.

- “Options”. Todos los valores opcionales asociados con paquetes IPV6 están contenidos en encabezados de extensión asegurando que el encabezado básico IP es siempre del mismo tamaño.

2.9.3.2 Tamaño del Paquete

Todos los nodos IPv6 se esperan que dinámicamente determinen la Unidad Máxima de Transferencia (MTU) soportado por todos los enlaces a lo largo de una ruta (como se describe en el RFC 1191 - Path MTU Discovery) y los nodos fuente únicamente enviaran paquetes que no excedan el MTU de la ruta.

De esta forma, los ruteadores IPv6 no fragmentaran los paquetes entre en los múltiples saltos de la ruta para alcanzar el destino final, haciendo más eficiente el uso de rutas que cruzan diversos medios físicos de transmisión.

Actualmente, se propone que IPv6 requiera que cada enlace soporte un MTU de 576 bytes, pero este valor como muchos otros valores de IPv6 pueden cambiar.

2.9.3.3 Encabezados de Extensión

Los encabezados de extensión se colocan entre el encabezado del paquete de IPv6 y los datos que especifican el protocolo de nivel superior. Forman parte del campo “payload length”. Cada encabezado tiene un campo de 8 bits “Next Header” como el encabezado IPv6, el cual identifica el tipo de encabezados siguientes.

La longitud de cada encabezado (el cual es siempre múltiplo de 8 bytes) es codificada posteriormente en él, en un formato específico para ese tipo de encabezado. Existe un número limitado de encabezados de extensión. Estos pueden estar presentes una vez (únicamente una vez) en el paquete IPv6. Cuando el campo “Next Header” contiene un valor diferente a un “header” de extensión, esto indica el fin de los encabezados de IPv6 y el inicio de los datos del protocolo de capa superior.

IPv6 permite encapsular IPv6 con IPv6 (“tunneling’). Esto es hecho con un “Next Header” de valor 41 (IPv6). El paquete encapsulado de Ipv6 puede tener su propio encabezado de extensión. Ya que el tamaño de un paquete es calculado por el nodo que lo origina para igualar el MTU de la ruta, los ruteadores IPv6 no deben agregar encabezados de extensión a un paquete; en lugar de eso deben encapsular el paquete recibido dentro de un paquete Ipv6 que el mismo genere (el cual puede ser fragmentado si es necesario).

Con la excepción del encabezado “Hop-by-Hop” (este debe estar inmediatamente después del encabezado IP si existe), los encabezados de extensión no son procesados por ningún ruteador en la ruta del paquete, excepto por el ruteador final.

IPv6 usa un formato común llamado el “Type-Iength-Value” (TLV), formato para campos de longitud variable, estos se pueden encontrar en los encabezados de opción “Hop-by-Hop” y “En d-to-En d”. La opción tiene un encabezado de 2 bytes:

- Type se refiere al tipo de opción. Todos los tipos de opción tienen el mismo formato: xx. Un número de 2 bits indicando como debe ser tratado un nodo Ipv6 que no reconoce la opción. Éstas pueden ser:

0 Salta la opción y continúa.
1 Descarta el paquete silenciosamente.
2 Descarta el paquete e informa al dispositivo que lo envío con un mensaje ICMP "Unrecognized Type".
3 Descarta el paquete e informa al dispositivo que envío el paquete un mensaje ICMP "Unrecognized Type" a menos que la dirección destino sea una dirección de "Multicast".
y Este bit tiene un significado específico solo para el encabezado "Hopby-Hop". Si esta colocado, indica que el valor de la opción puede cambiar en la ruta y por lo tanto debe ser excluido de cualquier calculo de integridad, desarrollado en el paquete. Puesto que los ruteadores intermedios únicamente examinan los encabezados "Hop-by-Hop", solo las opciones "Hop-by-Hop" pueden ser validamente cambiadas en la ruta.

- ZZZZZ. Los bits restantes que definen la opción.
- Length. La longitud del valor de la opción.
- Value. El valor de la opción. Esto depende del tipo.

Para implementar el desempeño de una implementación de Ipv6, opciones individuales se alinean de tal forma que valores multi-byte son colocados en sus limites naturales.

En muchos casos, en que los encabezados de la opción son más grandes de lo necesario, pero debe permitir que los nodos procesen datagramas más rápidamente. Para permitir esta alineación, todas las implementaciones IPv6 deben reconocer dos opciones que completan ("padding'):

Un byte X'00' usado para completar un solo byte. Mayores secuencias de completar deben ser echas con el PadN option.

- PadN. Una opción en el formato TLV. Su valor X'01'. La longitud del byte proporciona el número de bytes a completar después de los 2 bytes como mínimo que se requiera.

2.9.3.4 Direccionamiento IPv6

IPv6 proporciona un esquema de direcciones de 128 bits de longitud. A diferencia de IPv4 que tiene una forma estrictamente codificada sobre la base de clases de direcciones indicadas por el bit de mayor orden en la dirección, las direcciones IPv6 no están estructuradas de esta forma.

Están diseñadas para ser usadas con "Classless InterDomain Routing" (CIDR). El espacio de direcciones IPv6 es tan suficientemente grande que puede encerrar un rango muy grande de espacios de direcciones ya existentes y propuestas. En conjunto con CIDR, parte principal del direccionamiento IPv6, por ejemplo, el primer byte indicaría el tipo de direccionamiento. Tales tipos incluirían asociar el espacio de direccionamiento actual IPv4 a IPv6, direcciones OSI NSAPs, Novel! IPX. Además el encabezado del ruteo de IPv6 permite a IP encapsular de manera arbitraria información sobre direccionamiento en cada paquete. Esto podría extender el esquema de IPv6 a direcciones de sistemas hipotéticos que no pueden ser asociados al espacio de direcciones IP. Dada la longitud del campo de dirección IPv6, es poco probable que esto sea necesario en un futuro próximo.

Técnicamente, la direcciones IPv6 son identificadores de 128 bits para interfaces y grupo de interfaces. Esto es equivalente a elevar al cuadrado dos veces el espacio de direcciones IPv4;

verdaderamente un número muy grande de direcciones. El protocolo IPv6 define tres tipos de direcciones: Unicast, Anycast y multicast.

- Unicast addresses. IPv6 reconoce tres tipos principales. Una dirección “unicast” es un identificador para una sola interfaz. Los tres tipos de dirección “unicast” son direcciones basadas en proveedores (“provider-based’), direcciones de uso local del sitio (site-Iocal-use) y direcciones de uso local del enlace (link-local-use).

- Anycast addresses. Un nuevo tipo de dirección la cual es un identificador (un simple valor) asignado a más de una interfaz. El conjunto de interfaces a una dirección de “anycast” típicamente pertenecen a más de una computadora. Cuando un paquete se envía a una dirección de “anycast”, el protocolo de ruteo usado en ese momento envía el paquete a la interfaz más cercana identificada por esa dirección. La interfaz más cercana es determinada por la medida de distancia del protocolo de ruteo.

- Multicast addresses. El formato de la dirección permite la posibilidad de trillones de códigos de grupos de “multicast”. Una dirección de “m ulticast” es un identificador para un conjunto de interfazs que típicamente pertenecen a diferentes nodos. Cada código de grupo de “multicast” identifica dos o más recipientes de paquetes. Además, una dirección de “multicast” particular puede ser confinado a un solo sistema, restringido dentro de un sitio específico, asociado con un enlace de red particular o distribuido mundialmente. Cuando un paquete es enviado a una dirección de “multicast”, el protocolo envía el paquete a todas las interfaces identificadas por esa dirección.

La nueva dirección “multicast” de IPv6 reemplaza a la dirección “broadcast” como es usada en IPv4. IPv6 usa el mismo modelo para subredes como lo hace IPv4:

- Una subred puede ser asociada con solo un enlace
- Múltiples subredes pueden ser asignadas al mismo enlace.

2.9.3.5 Reglas del Direccionamiento

Todos los tipos de direcciones IPv6 son asignados a interfaces, no a nodos. Cada interfaz pertenece a un solo nodo. Esto significa que puede identificar un nodo por su dirección “unicast” de su interfaz.

Una dirección “unicast” IPv6 hace referencia a una única interfaz. Una sola interfaz puede tener múltiples direcciones IPv6 de cualquier tipo de las direcciones de IPv6. No obstante, y como excepción, una sola dirección “unicast” puede ser asignada a múltiples interfaces físicas bajo las siguientes condiciones:

Cuando compartir carga sobre múltiples interfaces físicas es necesario. Cuando las aplicaciones tratan las múltiples interfaces físicas como una sola interfaz. Los ruteadores tienen interfaces no numeradas sobre enlaces “Point-to-Point”.

Esto significa que direcciones IPv6 no son asignados a la interfaz. Ruteadores “Point-to-Point” ni requieren direcciones si no son fuente o destino de datagramas IPv6.

2.9.3.6 Representación de Direcciones IPv6.

Las direcciones Ipv4 tradicionalmente eran representadas en notación decimal con puntos; cada dirección de 32-bits esta dividida en cuatro secciones de 8-bits, un número decimal entre O y 255 representa cada sección. Por ejemplo

192.168.95.143.

La dirección IPv6 de 128-bits utiliza un método diferente para representar la dirección. Existen tres formas para representar la dirección IPv6.

La Forma Preferida es la dirección IPv6 completa en valores hexadecimales. Como se define en el RFC 1884, la forma preferida es X:X:X:X:X:X:X:X, donde la X representa los valores hexadecimales de cada componente de 16-bits de la dirección. Por ejemplo, una dirección IPv6 podría tener la siguiente forma:

FEDC:BA98:7654:321 0:FEDC:BA98:7654:3210

Los dos puntos separan cada sección y cuatro números hexadecimales presentan cada sección de 16-bits. Algunas veces una sección de 16-bits esta formada principalmente por ceros en un campo individual, pero debe existir al menos un número representación de una dirección como se muestra en el ejemplo:

1 080:0:0:0:8:800:200C:417 A

La Forma Reducida substituye cadenas de ceros con una sintaxis especial para reducir los ceros Esta forma utiliza dobles dos puntos (::) Para indicar múltiples grupos de ceros de 16-bits El doble dos puntos puede ser usado una vez en una dirección. La dirección puede ser simplificada como sigue:

1 080:0:0:0:8:800:200C:417 A

Según lo descrito anteriormente: 1080::8:800:200C:417A

Los dobles dos puntos pueden ser usados para reducir los primeros y/o últimos ceros en una dirección. La siguiente tabla muestra la simplificación de algunos ceros en una dirección usando dobles dos puntos.

Dirección	es	Puede ser representada como
1080:0:0:0:800:200C:417A	Dirección Unicast	1008::8:800:200C:417A
FF01:0:0:0:0:0:0:43	Dirección Multicast	FF01::43
0:0:0:0:0:0:0:1	Dirección Loopback	::1
0:0:0:0:0:0:0:0	Dirección no especificada	::

La forma combinada es conveniente usarla para ambientes de nodos combinados de IPv4 e IPv6. Esta forma se puede representar X:X:X:X:X:X:D.D.D.D. Las X´s representan los valores hexadecimales de los seis componentes de más alto orden de la dirección.

Las D´s representan el valor estándar de la representación decimal de los cuatro componentes de ocho bits de la dirección. La siguiente tabla muestra la representación combinada:

Dirección combinada	Forma compuesta
0:0:0:0:0:0:13.1.68.3	::13.1.68.3
0:0:0:0:FFFF:129.144.52.38	::FFFF:129.144.52.38

Por otro lado, así como IPv4, IPv6 puede tener un prefijo de dirección. Un prefijo de dirección IPv6 está definido como una dirección IPv6 y alguna indicación de los bits contiguos más significativos dentro de la porción de esta dirección. La representación de un prefijo de dirección IPv6 es similar a la forma que los prefijos IPv4 son escritos en notación CIDR.

Las direcciones IPv6 pueden ser escritas usando cualquiera de las formas previamente descritas, con una diferencia: si la dirección escrita finaliza en dobles dos puntos, estos pueden ser omitidos.

La longitud del prefijo es un valor decimal. Especifica el número de bits contiguos más a la izquierda de la dirección que comprende el prefijo. El siguiente ejemplo muestra la representación legal del prefijo de 60-bits 12AB00000000CD30.

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30::/60
12AB:0:0:CD30/60

La siguiente tabla muestra algunas representaciones que no son legales para este prefijo de 60 bits.

Prefijo de dirección ilegal	Razón
12AB::CD30/60	Se pueden omitir los primeros ceros pero no los últimos, dentro de cualquier porción de 16-bits de la dirección.
12AB::CD30/60	Direcciones a la izquierda del"/" se expanden a 12AB: 0000 :0000: 0000: 0000: 0000: 0000: C 030
12AB::CD3/60	Direcciones a la izquierda del "/" se expanden a 12AB: 0000: 0000: 0000: 0000: 0000: 0000: OCD3

La dirección de un nodo y el prefijo de subred de un nodo pueden ser combinados y escritos como se muestra a continuación.

Dirección del nodo:	12AB:0:0:CD30: 123:4567:89AB:CDEF
Número de subred del nodo:	12AB:0:0:CD30/60
Dirección combinada y abreviada:	12AB:0:0:CD30:123:4567:89AB:CDEF/60

2.9.3.7 Tipos de Dirección y Asignación

Los primeros bits de una dirección IPv6 indican el tipo específico de dirección. El campo de longitud variable comprende estos primeros bits y es llamado el Prefijo de Formato (Formato Perfil, FP). En la siguiente tabla se muestra la asignación inicial de estos prefijos.

Asignación	Prefijo (binario)	Fracción del espacio de
Reservado	00000000	1/256
No asignado	00000001	1/256
Reservado para asignación NSAP	0000001	1/128
Reservado para asignación IPX	0000010	1/128
No asignado	0000011	1/128
No asignado	0000 1	1/32
No asignado	0001	1/16
No asignado	001	1/8
Dirección Unicast	010	1/8
Provider-based no asignada	011	1/8
Reservada para dirección Unicast Geographic-based	100	1/8
No asignada	101	1/8
No asignada	110	1/8
No asignada	1110	1/16
No asignada	1111 O	1/32
No asignada	111110	1/64
No asignada	1111110	1/128
No asignada	1111 1110 O	1/512
Dirección Link-Local-Use	1111111010	1/1024
Dirección Site-Local-Use	1111111011	1/1024
Dirección Multicast	11111111	1/256

La dirección del “loopback”, la dirección IPv6 con la dirección Ipv4 integrada y la dirección no especificada, son especificadas fuera del espacio del prefijo de formato (FP) 0000 0000. El 15% del espacio de direcciones es inicialmente asignado para soportar la asignación directa de las direcciones del proveedor, direcciones de uso local y direcciones “multicast”.

Además, como se puede ver en la tabla existen espacios de direcciones reservados para NSAP, direcciones IPX y direcciones geográficas. El resto del espacio de direcciones no esta asignado, para uso futuro. Tal uso puede incluir la expansión de usos existentes y la introducción de nuevos usos tales como localidades separadas e identificadoras.

El valor del octeto de mayor orden de la dirección diferencia a una dirección “unicast” de una dirección “multicast”. Un valor de FF (11111111) identifica a una dirección como una dirección de “multicast”; cualquier otro valor identifica a una dirección como una dirección de “unicast”.

Debido a que las direcciones de “anycast” derivan del espacio de direcciones “unicast”, son sintácticamente idénticas a éstas.

2.10 Interconexión de Redes (“Internetworking”)

El origen de las subredes ha sido un misterio para muchos administradores de sistemas. Parece que estas son una maraña de bits, bytes y mascaras que no valen la pena.

Sin embargo, si se proyecta tener acceso a Internet entonces las direcciones IP (“Internet Protocol’) y el enmascaramiento de subredes son tópicos con los que se debe estar familiarizado. Mientras la red crece, se incrementa la cantidad de segmentos y se requieren más direcciones de red, ya que cada segmento requiere un rango propio de ellas.

El InterNIC se encarga de asignar estas direcciones, sin embargo, no pueden otorgar un número de direcciones ilimitadas, ya que el espacio de direccionamiento de Internet esta llegando a su límite.

Un método de fomentar la conservación de direcciones es dividir una red en segmentos o subredes. Esto permite incrementar el número de segmentos independientes sin necesidad de más números de red IP.

En la práctica, no se ponen en red 16 millones de nodos para una red clase A ó 65000 en una red clase B, frecuentemente lo que se hace es dividir este tipo de redes en subredes (la subdivisión de redes es soportada por muchos sistemas operativos).

Para dividir una red en subredes, se utilizan parte de los bits que identifican al “host”, para denotar un número de subred. De esta forma la identificación total de un “host”, que inicialmente estaba dada por el número de red y el número de “host”, ahora queda definida por el número de red, el número de subred y el número de “host”.

La cantidad de bits que se utilizan para la subred, determina el número de subredes en los que se dividirá la red original. Este número esta dado por 2 elevado a la cantidad de bits utilizados. Por ejemplo si se toman 3 bits, el número de subredes será 8. El resto de los bits usados inicialmente para el “host”, identificarán el número de “host” en cada subred.

En el caso especifico de una red clase A, los 16,777,216 “hosts” se podrían agrupar en varias subredes. Por ejemplo, podemos utilizar los 16 bits de mayor valor (M8Bs More 8ignificative Bits) de la porción que le corresponde al “host” en una red clase A, para denotar el número de la subred y los 8 más bajos para el “host”, como se ve en la siguiente tabla:

RED CLASE A	SUBRED DE 16 BIT8	H0ST DE 8 BITS
←----------→	←----------→	←----------→
XXXXXXXX	XXXXXXXX.XXXXXXXX	XXXXXXXX
“host ” de una red de clase A		

Este esquema permitiría hasta 65,534 subredes utilizables (las subredes 0.0 y 255.255 están reservadas) y cada una con 254 “hosts” útiles (las direcciones O y 255 de cada subred están reservados). Obviamente se podría plantear cualquier otro esquema, para obtener un número diferente de subredes y “hosts” por subred.

2.10.1 La Máscara de Subred

La máscara de subred es usada para determinar el número de bits (de una dirección IP) que se utilizan para la subred y el “host”. La máscara tiene un valor de 32 bits (similar a una dirección IP) y esta formada por unos para la porción de red y subred y ceros para la porción de “host”.

Por ejemplo, en la dirección IP clase B 191.70.55.130, sin aplicar ningún esquema de subdivisión la mascara de red asociada por default será 255.255.0.0, aplicando el operador AND lógico, entre la dirección del “host” y la mascara definida, obtenemos la dirección de la red.

Es decir la máscara retiene los bits de la red y enmascara los bits de “host”, como lo ilustra la siguiente tabla:

191	70	55	130	Dirección IP del host
10111111	10000110	0011 0111	10000010	BITs host IP
11111111	11111111	00000000	00000000	Mascara por Default clase B
10111111	10000110	00000000	00000000	BITS de la red clase B
191	70	0	0	Dirección IP de la red clase B
Máscaras				

Se pueden utilizar distintos esquemas de partición, esto dará diferentes mascaras, que ahora se denominan de mascaras de subred.

La siguiente tabla muestra como la mascara aplicada a una dirección cualquiera dentro de esta red, determina el número de red y subred a la que pertenece un “host”.

191	70	55	130	Dirección IP del host
10111111	10000110	0011 0111	10000010	BITs host IP
11111111	11111111	11111111	00000000	Mascara de subred
10111111	10000110	0011 0111	00000000	BITS de la subred
191	70	55	0	Dirección IP de la subred
Máscara Aplicada a una Dirección en una Red.				

Esta división, permite determinar fácilmente a partir de una dirección IP en notación punteada el número de subred del penúltimo byte y el número de “host” del último byte.

No se tiene que utilizar un byte completo exclusivamente para denotar el número de subred, se pueden utilizar cualquier número de bits, Si la porción inicial de bits para el “host” es H, y se utilizan S bits para denotar la subred, entonces queda H - S bits para el número de “host” con subred.

Si se usa una máscara que permite más subredes (512), tiene la desventaja de tener menos “hosts” (128) por cada subred:

191	70	55	130	Dirección IP del host
10111111	10000110	0011 0111	10000010	BITs host IP
11111111	11111111	11111111	10000000	Máscara de subred
10111111	10000110	0011 0111	10000000	BITS de la subred
191	70	55	128	Dirección IP de la subred
Máscara que Permite más Subredes.				

2.10.2 Subredes contra Nodos

El RFC 950 determina que al realizar el “subnetmasking” no deberán utilizarse ni la primera subred, ni la última subred al obtener los números de subredes.

La división en subredes permite segmentar el tráfico en diferentes redes, sin embargo una de sus principales desventajas, es que se pierden muchas direcciones dado que se debe recordar las reglas importantes:

- La primera y la última subred no se pueden utilizar (en su totalidad). Esto se debe a que son usadas para situaciones de direccionamiento especial. La última dirección de la red original (todos los bits en unos), corresponde a la última dirección de la última subred, esta se utiliza para mandar una señal de “broadcast” a todas las subredes directamente.

- La primera dirección de la red original (todos los bits en ceros), corresponde a la primera dirección de la primera subred, ésta se utiliza para identificar a la red original.

- La primera y la última dirección de cada subred, están reservadas. La primera dirección de cada subred está reservada para identificar a la subred, mientras que la última se utiliza para mandar un “broadcast” a todas los “hosts” de la subred.

Por lo que si N es el tamaño de cada subred y S representa el número de subredes, se perderán 2N+ 2(S-2) direcciones. Por ejemplo, si se decide partir una red clase B en 256 subredes de 256 direcciones cada una, se pierden todas las direcciones de la primera y la última subred, esto es 512, pero por otra parte también se pierden la primera y la última dirección de las 254 subredes restantes, esto es 254*2=508, por lo que se pierde un total de 512+508=1020 direcciones sacrificadas para realizar la partición. Esto no es muy crítico en redes clase A o B, pero sí en redes clase e donde el número de direcciones disponibles es crítico.

A continuación se presenta una tabla que permite observar diferentes configuraciones entre el número de subredes y “hosts” con diferentes máscaras de subred para las clases de direccionamiento B y C.

# Bits de máscara.	Máscara de subred.	# Subredes.	# Hosts por subred.
18	255.255.192.0	2	16382
19	255.255.224.0	6	8190
20	255.255.240.0	14	4094
21	255.255.248.0	30	2046
22	255.255.252.0	62	1022
23	255.255.254.0	126	510
24	255.255.255.0	254	254
25	255.255.255.128	510	126
26	255.255.255.192	1022	62
27	255.255.255.224	2046	30
28	255.255.255.240	4094	14
29	255.255.255.248	8190	6
30	255.255.255.252	16382	2
Subred Clase A.			

En esta tabla, se eliminan en cada caso, las dos subredes reservadas (primera y última) y las dos direcciones reservadas de cada subred (primera y última), quedando como sigue:

# Bits de mascara	Mascara de subred	# Subredes	# Hosts por subred
26	255.255.255.192	2	62
27	255.255.255.224	6	30
28	255.255.255.240	14	14
29	255.255.255.248	30	6
30	255.255.255.252	62	2
Subred Clase C.			

2.10.2.1 Ventajas de las Subredes

Al subdividir las redes, se oculta la organización de la red interna a los ruteadores externos y esto simplifica el ruteo. Por ejemplo, una subred de clase B requerirá menos rutas que el número equivalente de direcciones clase C. Las tablas de ruteo mas cortas hacen que la transferencia sea más rápida.

Además de ventajas técnicas, subdividir una red permite la administración descentralizada de las direcciones. Esto puede proporcionar beneficios políticos a la organización. Por ejemplo, un administrador puede asignar una subred a un departamento, y responsabilizar de la administración de su propia subred al encargado, esto es, de la asignación de direcciones, y la vigilancia de la unicidad de las mismas.

El “subnetworking”, elimina las limitaciones de distancia entre redes distantes, ya que aunque se encuentren en localidades diferentes, forman una sola red lógica, interconectada mediante ruteadores.

2.10.2.2 Parámetros /Jara Realizar la División

Una de las principales tareas de un administrador de la red es determinar los requerimientos de la red. Lo más lógico es empezar por considerar cuántos “host” estarán conectados a la red.

Conectar el máximo número de “hosts” en un segmento Ethernet no es muy práctico debido a que esto crea problemas de desempeño ya que se congestiona la red. Sin embargo si solo se tiene asignada una red de clase C, aparentemente el “subnetworking” no tiene sentido, debido al escaso número de direcciones.

Aunque una clase C puede soportar hasta 254 “hosts”, en la práctica un segmento Ethernet clásico de una oficina en donde se usa herramientas de automatización, mantiene su eficiencia con 60 a 80 “hosts”. Dependiendo del tráfico, el máximo recomendable es 1 00 hosts por segmento. Por lo que también es recomendable particionar una clase C en varias subredes. Si se usa cableado estructurado, muchas tarjetas de HUB vienen con 12, 16 ó 24 puertos UTP, por lo que se recomienda adquirir concentradores (“hubs’j expandibles o con capacidad de realizar una pila (“snack’) para que las características de estos equipos no sean lo que determine el tamaño de las subredes.

El esquema de división puede ser definido por dos factores: Cuantas redes se desean tener; y el máximo número de “host” por red.

Usando el primer parámetro, se definiría inmediatamente el esquema de división, El procedimiento es el siguiente: el número de subredes+2, se redondea a la potencia de 2 inmediatamente superior, esto determina el número de bits que se usarán para la máscara de subred, el número de bits restantes de la porción de “host”, determinará el número de “hosts” por subred.

El segundo parámetro también definiría el esquema de división. El número máximo de “hosts” en alguna subred +2, se redondea a la potencia de dos inmediatamente superior, esto determina el número de bits utilizados por los “hosts” de cada subred, los bits restantes, determinan la cantidad de subredes con esa cantidad de “hostil, en las que se podrá partir la subred.

Una configuración posible será dividir la red clase C en 8 subredes, con 32 direcciones IP cada una, debido a que la primera y la última subred no se pueden utilizar y la primera y la última dirección de las subredes restantes tampoco se pueden utilizar, esta configuración permite 6 subredes de 30 “host” cada una.

Se puede ver el siguiente caso de estudio: La compañía ACME, posee la red clase C 192.100.180.0, el tráfico en el segmento único, hace que el desempeño de su red, sea poco

eficiente. La compañía cuenta con 5 departamentos, con un número de computadoras entre 5 y 14. Determinar el esquema de división y por lo tanto la máscara de subred a utilizar.

Recordamos que para una red clase C, se utilizan 8 bits para el número de “host”. Utilizando como parámetro la cantidad de subredes deseadas, se tienen 5+2=7, redondeando a la potencia de 2 más cercana que es 8, se determina que el número de bits utilizados por el número de subred es 3, para dar una máscara de subred de 27 bits que expresada en la notación punteada es: 255.255.255.224. Entonces los 5 bits restantes se usan para el número de “host”, lo que permite 32 direcciones por subred o hasta 30 “hosts”, lo que cumple con los requerimientos.

Utilizando como parámetro la máxima cantidad de “hosts” por subred, se tienen 14+2= 16, que es una potencia de 2, por lo que no hay que redondear, esto determina que se requieren 4 bits para identificar los “host” de cada subred, los 4 bits restantes se usarán para identificar las 16 subredes posibles. Este esquema permite 14 subredes de hasta 14 “hosts” cada una, lo que cumple con los requerimientos, la máscara de subred para este esquema es 255.255.255.240.

La siguiente tabla especifica las direcciones de las 8 posibles subredes bajo el esquema de la máscara 255.255.255.224, a partir de los tres bits utilizados por la subred.

8	7	6	5	4	3	2	1	Subred
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	0	0	0	96
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160
1	1	0	0	0	0	0	0	192
Direcciones de las 8 posibles Redes								

NÚMERO DE SUBRED	IP SUBRED	IP PRIMER HOST	IP ULTIMO HOST	DEC.MIN	DEC.MAX
1	X.X.X.32	X.X.X.33	X.X.X.62	33	62
2	X.x.X.64	X.X.X.65	X.X.X.94	65	94
3	X.X.X.96	X.X.X.97	X.X.X.126	97	126
4	X.X.X.128	X.x.X.129	X.X.X.158	129	158
5	X.X.X.160	X.x.X.161	X.X.X.190	161	190
6	X.X.X.192	X.X.X.193	X.X.X.222	193	222

En resumen podemos decir que la división de una red clase C debe ser cuidadosamente planeada y ejecutada. Se debe de instalar un ruteador para dividir la red en un determinado número de subredes, y entonces reenumerar los segmentos y homologar la máscara de subred en cada uno.

2.11 Ruteo de IP

Para poder manejar una red, en ocasiones es necesario dividirla en segmentos más sencillos de administrar. La forma de interconectar los segmentos es por medio de los ruteadores. Un ruteador pasará paquetes de datos de una red a otra y determinará la ruta óptima (ruteo) hacia la cual el tráfico de datos deberá ser dirigido de acuerdo con su destino final.

Para poder enviar datos se emplean lenguajes entre los ruteadores que se conocen como protocolos de ruteo, ya sea protocolo Interno de ruteo (IGP, “Internal Gateway Protocol’) o protocolo externo de ruteo (EGP, “External Gateway Protocol’).

2.11.1 Datos de Ruteo

Un paquete que es enviado a la red puede ser entregado a un elemento de la red dentro del segmento físico de red, a este tipo de servicio se le conoce como ruteo directo. Si se establece que el paquete debe ser enviado a un segmento diferente de red, distinto a su segmento de red, el paquete deberá ser enviado a través de un ruteador, a este tipo de ruteo se le conoce como ruteo indirecto.

El proceso de cuando utilizar un ruteo directo o indirecto es simple. Cuando un nodo (nodo origen) envía un paquete a otro nodo (nodo destino), el nodo origen verifica la dirección IP de red del nodo destino (recordando que los 4 primeros bits más significativos de la dirección IP son los que definen la clase de la dirección). Si el número de red del nodo destino pertenece al segmento de red local, los paquetes sean enviados de manera local, en caso contrario, el paquete será enviado a los dispositivos que tengan la capacidad de ruteo.

Una vez que se determinó que el paquete debe ser reenviado a otro segmento físico de red, el nodo origen deberá enviar la información necesaria al ruteador para que éste pueda dirigir el paquete hacia el segmento de red adecuado para alcanzar su destino final.

Cuando se alcanza el destino, el ruteador que se encuentra conectado a la red donde esta el nodo destino, manejará la información como si se tratara de un ruteo directo al realizar el proceso de establecer la comunicación local con su dirección MAC.

Cuando el paquete es enviado no se puede determinar cuantos ruteadores debe pasar para alcanzar su destino final, cada ruteador que sea atravesado irá decrementando el campo TTL (“Time To Live’) en la cabecera de IP, cuando el campo TTL sea cero, se enviará un mensaje ICMP, el destino no pudo ser alcanzado.

2.11.2 Información de Ruteo y Tablas de Ruteo

Una tabla de ruteo es necesaria para hacer más eficiente la decisión de que si el paquete de información que será enviado debe ser dirigido a un ruteador o debe ser manejado de manera local.

La tabla de ruteo es un conjunto de entradas (rutas), las cuales definen el camino por el cual un paquete de información puede ser enviado. La tabla de ruteo está formada por rutas previamente definidas (ruteo estático) o por intercambio de información de ruteo (protocolos de ruteo) entre los ruteadores (ruteo dinámico).

El método de ruteo estático siempre designa las mismas rutas para trayectos equivalentes en la red, siguiendo un esquema básico implementado por el administrador en la configuración del sistema. En el método de ruteo dinámico, los dispositivos ruteadores eligen las rutas para los paquetes de información, calculando en cada ocasión, las rutas más convenientes. El parámetro que se toma como referencia para obtener la mejor ruta se llama métrica.

Existen dos criterios de calcular la métrica, vector distancia (“Oistance Vector’) y estado del enlace (“Link State’).

Cuando el ruteador no cuenta con la información necesaria en su tabla de ruteo para enviar un paquete a su destino hace uso de una entrada en la tabla de ruteo conocida como Rutas por omisión (“Oefault Route’), configurada manualmente por el administrador del sistema como la ruta a tomar cuando no existe ruta hacia el destino. Una tabla de ruteo típica es la siguiente:

Número de Red	Conocida por algoritmo de ruteo	Métrica	Tiempo para mantener la ruta	Conocido por
134.4.0.0	Directamente conectado	0 hop		Puerto 1
134.3.0.0	Directamente conectado	0 hop		Puerto 2
200.34.234.0	Ruta estática	1	---------	Puerto 1
132.48.0.0	RIP	1 hop	270	134.4.3.56
148.4.0.0	RIP	1 hop	250	134.3.1.100
9.0.0.0	OSPF	Cost = 900	300	134.3. 1 . 1 01
192.1.1.0	OSPF	Cost = 64	350	134.4.3.90

En la tabla anterior se observan protocolos de ruteo, de los cuales se hablará mas adelante; también se puede ver el ruteo estático y ruteo dinámico.

2.11.3 Protocolos de Ruteo

En ocasiones se confunden los términos protocolo ruteable y protocolo de ruteo. Los protocolos ruteables son los protocolos que se rutean entre las redes. Ejemplos de estos protocolos son IP, IPX, DECnet, AppleTalk, NetWare, OSI, Banyan VINES, y Xerox Network. Los protocolos de ruteo son los que implementan los algoritmos de ruteo, en pocas palabras éstos rutean los protocolos ruteables entre las redes, y son los protocolos mediante los cuales se entienden los ruteadores.

Ejemplos de estos incluyen: Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Exterior Gateway Protocol (EGP), Border Gateway Protocol (BGP), OSI Routing, Advanced Peer-to-Peer Networking, Intermediate System to Intermediate System (IS-IS), y Routing Information Protocol (RIP). Los protocolos de ruteo se muestran en la figura 2.8.

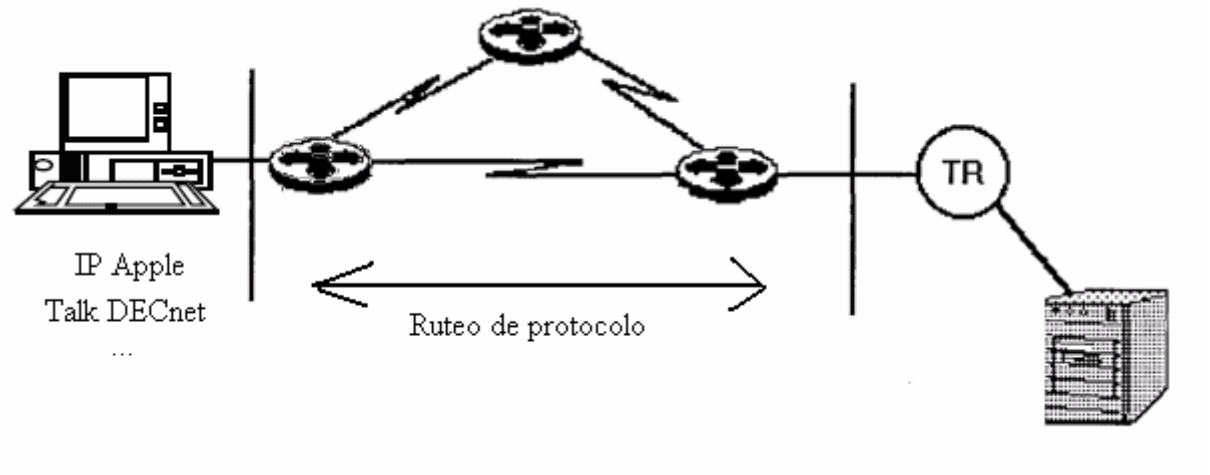


Figura 2.8 Protocolos de ruteo

2.11.4 Algoritmo de Ruteo

Los algoritmos de ruteo soportan a los protocolos de ruteo proporcionando las siguientes características:

- Construcción y mantenimiento de las tablas de ruteo.
- Escalar un protocolo ya existente a uno mejorado, por ejemplo RIP a IGRP.

La mayoría de los algoritmos de ruteo pueden ser clasificados conforme a cualquiera de dos algoritmos básicos, éstos son: Vector Distancia; y Estado de Enlace.

Los algoritmos de Vector Distancia hacen llamados a cada ruteador vecino (adyacente) para enviarles su tabla de ruteo completa. Las tablas de ruteo de vector distancia incluyen información correspondiente al costo total de transferencia por cada ruta (el costo queda definido por el tipo de métrica en uso).

Con el algoritmo de vector de distancia se tiene que las tablas de ruteo se envían de manera rutinaria y periódicamente o bien cuando se han incluido cambios a la topología.
El segundo algoritmo básico para el ruteo es el de Estado de Enlace. Este algoritmo realiza una captación total de la información relativa a la topología de la red y crea tablas de distancias mínimas y de caminos de tiempo mínimo de todo el sistema. Las tablas generadas con el uso de este algoritmo podrían compararse con mapas de carreteras, puesto que en éstos se puede localizar la ubicación de cada uno de los puntos de la red.

A diferencia del algoritmo de Vector de Distancia, el algoritmo de Estado de Enlace mantiene una información completa sobre todos los caminos disponibles a cada punto de la red. Los algoritmos de ruteo resultan procesos fundamentales en el método de ruteo dinámico y tienen cuatro características básicas:

- Exactitud
- Sencillez
- Confiabilidad
- Adaptabilidad

2.11.5 Métricas

Los ruteadores usan distintas métricas para determinar la mejor ruta, algunos algoritmos combinan varias de ellas para obtener una métrica híbrida. Algunas de estas son: Longitud de la trayectoria (número de saltos o ruteadores en el trayecto); confiabilidad; Retardos; Ancho de banda; Carga de Tráfico; Costo de la Comunicación.

2.11.6 Sistemas Autónomos (Autonomus System, AS)

En redes muy grandes que están conectadas a Internet, se tiene una administración local separada llamada Sistema Autónomo (AS-"Autonomous System') que tiene un número único asignado por la DDN del NIC ("Network Information Center'). Un Sistema Autónomo (SA) puede estar integrado por varias LAN interconectadas por medio de puertas ("Gateways') internas.

En un sistema autónomo, la estructura de la red no es visible para el resto de la Internet. Por lo general una compuerta lleva hacia la red por lo que todo el tráfico correspondiente a esa red debe pasar a través de la compuerta, que oculta la estructura interna de la red local a resto de la red.

2.11.7 Protocolos de Gateway Interno y Gateway Externo.

Si existe más de un "gateway" dentro de la red local y pueden comunicarse con otra, se consideran "gateways" vecinos interiores. Si los "gateways" pertenecen a diferentes sistemas autónomos, se trata de "gateways" exteriores.

2.11.8.-IGP ("Interior Gateway Protocol")

IGP es un protocolo cuya principal función es intercambiar información de tablas de ruteo entre "gate ways", "hosts" y ruteadores dentro de un esquema autónomo, es decir una red corporativa de redes independientes que desean intercambiar información entre ellas. El esquema de autonomía se define dentro del servicio de ruteo como Sistema Autónomo ("Autonomous System').

Los protocolos de mayor relevancia en IGP son "Routing Information Protocol" (RIP) y "Open Shortest Path First" (OSPF).

2.11.9.- EGP ("Exterior Gateway Protocol").

Este tipo de Protocolo es utilizado para intercambiar información de tablas de ruteo entre los Sistemas Autónomos, es utilizado principalmente por DON ("Defense Data Network'); la tabla de ruteo contiene una lista de los ruteadores con el costo asociado (métrica) para seleccionar la mejor ruta. Cada ruteador solicita actualización de sus tablas de ruteo a los vecinos cada 120 a 480 segundos, EGP-2 es la versión más nueva de EGP.

El administrador de la red decidirá el ruteador que funcionará como ruteador externo para poder anunciar a la red interna las rutas que están recibiendo de otros sistemas autónomos.
"Border Gateway Protocol" (8GP), es más reciente, proporcionando capacidades adicionales.

2.11.10.- RIP (“Routing Information Protocol”)

RIP es unos de los protocolos de ruteo más utilizados para manejar la información al interconectar redes de área local LAN, RIP está clasificado como un protocolo de ruteo interno (IGP) por el “Internet Engineering Task Force” (IETF). Su base es utilizar el algoritmo de ruteo 80.

Al utilizar RIP como protocolo de ruteo, los “gateways” envían toda la información de las rutas que él conoce hacia el vecino más cercano, a este proceso se le conoce como actualización de tablas de ruteo, el vecino que recibe la información pasara al otro vecino la información que le llegó por el vecino original, este procedimiento de enviar las tablas de ruteo se realiza cada 30 segundos. El algoritmo de vector distancia usa como medida (métrica) de decisión para la generación de su tabla de ruteo la cuenta en saltos (“Hop Count’).

En caso de ocurrir algún cambio en la red, será reflejado hasta que la actualización de la tabla de ruteo se lleve a cabo, (30 segundos si está directamente conectado al vecino inmediato ó 450 segundos si es que se encuentra en la distancia máxima soportada por RIP, 15 saltos) a este cambio y el reflejo del mismo se le llama tiempo de convergencia. Lo anterior se muestra en la figura 2.9

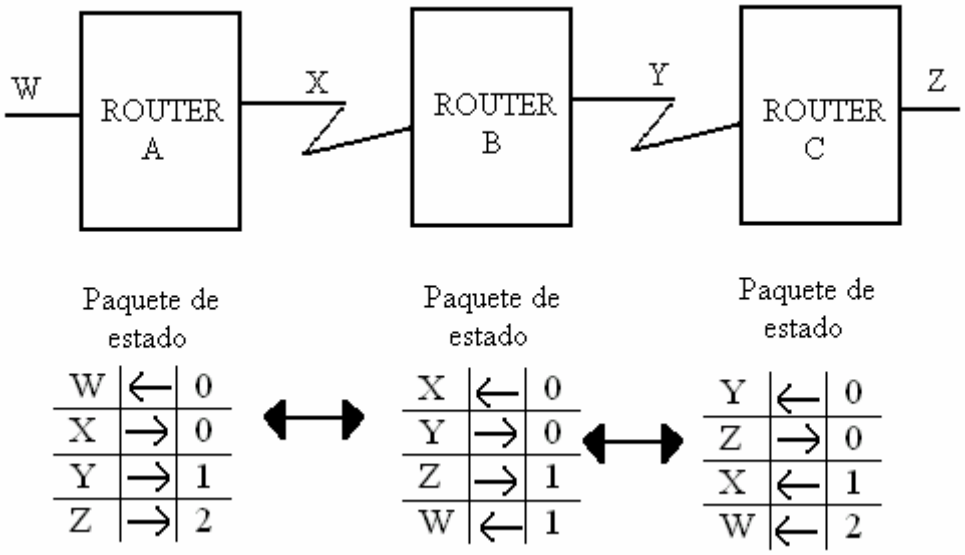


Figura 2.9 RIP

RIP es una buena solución para redes pequeñas. Sin embargo, para redes de mayor dimensión la transmisión de toda la tabla de ruteo cada 30 segundos sería una gran cantidad de tráfico innecesario en la red.

2.11.11 "Open Shortest Path First Protocol" (OSPF)

OSPF es un protocolo de ruteo utilizado para redes más complejas dentro de un sistema autónomo, OSPF es preferido sobre RIP. En OSPF, cuando se detecta un cambio en la tabla de ruteo o algún cambio en la topología de la red, es reflejado de manera inmediata por medio de "Multicast", enviando la información a todos los nodos de la red. A diferencia de RIP de enviar la actualización cada 30 segundos, OSPF reporta de manera inmediata la actualización sí y sólo sí, ha existido algún cambio.

A diferencia de RIP que utiliza un método simple (número de saltos) para calcular la métrica, OSPF toma la decisión de la ruta basado en el algoritmo de ruteo "link state" que usa información adicional de los parámetros del enlace de red para realizar el cálculo de la métrica de su red. OSPF además soporta el concepto de subredes de máscara variable (VLSM, "Variable Length Subnet Mask").

RIP no toma en cuenta la velocidad del enlace, para realizar el cómputo de decisión por donde debe de enviar el paquete de información, sino que se llega al mismo destino por dos rutas distintas, una línea es de 64kbps y las otras líneas son de 2.048Mbps, desde el punto de vista de RIP, la mejor ruta es por la línea de 64kbps (un salto), pero para OSPF la misma decisión es incorrecta, ya que la mejor ruta para OSPF es el enlace de 2.048 Mbps, por la capacidad de ancho de banda que tiene el enlace hacia el mismo destino.

Existe un concepto denominado sumarización, el cual surge con el objetivo de agrupar un rango de redes y reportar como si fuera una sola, este termino es mejor conocido como CIDR ("Classless Interdomain Routing').

Con OSPF debe existir una conectividad con los ruteadores vecinos, es decir se deben de reconocer para poder establecer el intercambio de información. La conectividad se lleva a cabo por medio de paquetes llamados "Hello", éstos; permiten que los vecinos establezcan el intercambio de comunicación para manejar una comunicación bidireccional.

No se puede decir que todo es mágico en OSPF, si una red es muy grande los "Multicasfs" mencionados con anterioridad pueden convertirse en un problema, para evitar este problema se generan áreas.

2.11.12 Áreas

La administración se puede hacer compleja por conveniencia, la frase de Julio Cesar "divide y vencerás", aplica perfectamente en este concepto, ya que nos permite dividir nuestra red en regiones que sean más sencillas de administrar. Un área es una administración de equipos que constantemente se están comunicando entre sí.

El nivel óptimo de ruteo es cuando esta porción de información requiere comunicarse con un área con la que nunca perderá comunicación, a esta área se le conoce como el área 0 o área 0.0.0.0 en algunas implementaciones de OSPF, recibe el nombre de "Backbone". Todas las áreas siempre están de manera contigua, todos los ruteadores tienen una ruta hacia otro ruteador.

2.11.13 Ruteadores de Área Frontera (“Area Border Routers”)

Los ruteadores que tienen comunicación con el área 0, (“backbone”) en alguna de sus interfazs, serán llamados “Area Border Routers”. Éstos tienen la capacidad de propagar la información de las redes que están contenidas dentro del área de manera sumarizada, es decir con una “subnet mask” diferente a la del sistema autónomo.

2.11.14 Enlaces Virtuales (“Virtual Links”)

Todas las áreas deben tener contacto con el área 0 para poder conservar comunicación con las diferentes áreas, debido a que esto puede ser impráctico o difícil, existe un tipo especial que es conocido como una enlace virtual, virtual porque simula que conecta el área cero sin tener una interfaces directamente conectada al “Backbone”.

2.11.15.- Interfaz OSPF (“OSPF Interfaz”).

Un ruteador tiene al menos dos interfaces de red, el “Area Border Router” es un ruteador que tiene como característica que una o más de las interfaces pertenecerá al área cero y el resto puede pertenecer a otra área. El decir que pertenece a un área es por que las interfaces del ruteador están en contacto con los vecinos del área, éste contiene un identificador y posiblemente si se tiene autenticación con el ruteador, se necesitara el envío de una contraseña (“Password’). La información de ruteadores mal configurados o funcionando inapropiadamente será descartada.

2.11.16 Comunicación entre Ruteadores con Protocolo OSPF (“OSPF Pockets”).

Como todos los protocolos de ruteo la manera de comunicar información entre los ruteadores es por medio de paquetes, pero a diferencia de RIP que usa un servicio UDP y a diferencia de BGP que utiliza TCP, en el campo de tipo de protocolo de IP, con el servicio 89 asignado, determina que el mismo es un servicio de OSPF. Eliminando la cabecera del Protocolo de Internet (“Internet Pro tocol’), el ruteador sabe que la porción de información de datos de IP es información de OSPF, como lo muestra la figura 2.10

In the Internet Protocol (IP) [DON], [RFC791] there is a field, called :
Protocol, to identify the next level protocol. This is an 8 bit field.
Assigned Internet Protocol Numbers

Decimal	Keyword	Protocol	References
Reserved			
1	ICMP	Internet	[RFC792,JBP]
4	IP	IP	In fRFC18531

Figura 2.10 Protocolo OSPF

2.11 .17 Mantenimiento y Descubrimiento de los Vecinos

Un ruteador con OSPF descubre a sus vecinos mediante paquetes de reconocimiento llamados paquetes de “Hello” en sus interfaces, estos mensajes son enviados cada 10 segundos, es un parámetro que se puede configurar.

La porción de información que se envía con el protocolo OSPF, es responsable de establecer la comunicación entre los vecinos y detectar una falla en uno de sus vecinos, en caso de existir alguna; el vecino al no detectar información de que es lo que está ocurriendo en el sistema y al no recibir respuesta, inundará (“f1ooding’) con LSA avisando que los ruteadores deberán de hacer el cálculo de la topología de la red. Este proceso se llama convergencia.

El paquete “Hello” es responsable de que cada vecino envíe y reciba paquetes en ambos sentidos. Además de manejar el intervalo de actualización, los intervalos sin envío de información y determinar cuando existe algún cambio.

Las redes se pueden clasificar en dos tipos de servicios, redes que manejan “Broadcast” y redes que no lo hacen.

2.11.18 Sincronización de la Base de Datos.

Cuando se realiza una conexión entre dos vecinos, el vecino que está arrancando debe esperar a que los “link state packets” para poder sincronizar su propia base de datos antes de empezar a utilizar el servicio de redireccionar tráfico en sus interfaces.

El intercambio de LSA (“Link State Adverlisement’), permite que la base de datos de información de las tablas de ruteo sea conocida y el LSA avisa solo cuando existe un cambio en la estructura de la red.

2.11.19 RIP vs OSPF

Si se decidiera hacer una comparación entre OSPF y RIP, se obtendría la siguiente tabla:

RIP	OSPF
La topología de la red se ve desde la perspectiva del vecino	La topología de red es desde el punto de vista del propio ruteador
La métrica utilizada para sus tablas de ruteo son saltos sin tomar en cuenta la cantidad de información que puede llevar el enlace	La métrica para el uso de servicio es un costo, en el cual se toma en cuenta el enlace
Se realizan actualizaciones para saber los cambios en la red	Se envían LSA para conocer de algún cambio en la red
Su convergencia es lenta	La convergencia es más rápida

2.11.20 “Border Gateway Protocol” (BGP)

BGP (“Border Gateway protocol”) es un protocolo que intercambia su propia tabla de ruteo entre puertas (“gateways’), cada una de ellas con su propio Sistema Autónomo; es el protocolo que se usa actualmente para intercambiar información en Internet, la información es enviada por parte de los ruteadores en su tabla de ruteo.

2.11.20.1 Figura de Sistemas Autónomos

Los nodos al comunicarse con BGP utilizan TCP ("Transmission Control protocol") al puerto 179 y envían la información cuando han detectado algún cambio de información. Una vez establecida la comunicación de TCP el propósito es intercambiar rutas entre los vecinos. BGP-4 es la última versión de BGP.

BGP-4 tiene la capacidad de manipular sumarización, mejor conocido como CIDR ("Classless Inter-Domain Routing'). Que es la manera de agrupar un número de redes con "subnet-mask" diferente al asignado a las redes internas.

BGP fue desarrollado para poder reemplazar a su predecesor EGP (ya un protocolo obsoleto), mientras la red en Internet empezó a crecer las actualizaciones por parte de EGP, empezaron a tener sus altibajos, BGP los ha ido resolviendo de manera más eficiente, BGP es el protocolo utilizado por los ISP's.

El RFC 1771 describe a BGP-4. El RFC 1654 describe la primera versión de BGP-4. BGP inicialmente intercambia toda la información posible, posteriormente, envía actualizaciones increméntales, en caso de no existir actualizaciones, se envían mensajes de "keepalive", para monitorear si el vecino está funcionando.

2.11.20.2 "Classless Inter-Domain Routing" (CIDR)

Las tablas de ruteo de Internet han ido creciendo de manera exponencial, en Diciembre de 1990 existían 2190 rutas, 2 años después, eran aproximadamente 8500 rutas. Para Julio de 1995 eran alrededor de 29,000 rutas que requieren aproximadamente 10MB de RAM por ruteador para mantenerlas. Los ruteadores con 64MB podrían mantener en RAM alrededor de 60,000 rutas.

IDR ("Class/ess Inter-Domain Routing') está generado por los RFC1517, RFC1518, RFC1519, RFC1520. CIDR es un método de evitar que la tabla de ruteo se pierda por falta de recursos en el equipo. Sin la implementación CIDR en 1994, Internet actualmente no podría seguir funcionando.

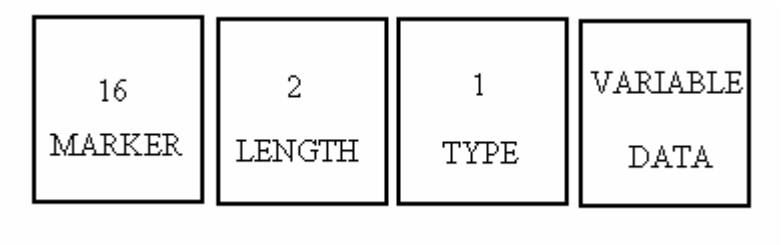
El principio de CIDR elimina el concepto de las redes Clase A, B Y C, y lo generaliza en un prefijo de IP, CIDR cubre un espacio de direcciones más amplio al agrupar una cantidad mayor de redes.

Cuando se habla de la dirección 192.1.0.0, es una red clase C, el número de red es 192.1.0.0 y el "Netmask" es 255.255.255.0, el formato que maneja CIDR es el siguiente: La red 192.1.0.0/16, es decir el rango de direcciones comprendida entre 192.1.0.0 a 192.255.0.0, este rango se reporta como una sola red, en lugar de guardar 255 redes en la tabla de ruteo solo se conserva una red que agrupa a todo el rango. Es como si el ruteador diera a conocer una dirección clase C 192.1.0.0 pero con máscara de red clase B.

2.11.20.3.- Información de las Cabeceras de BGP

Todos los mensajes de BGP están comprendidos en un solo paquete de información, pueden variar según sea el tipo de información que se está enviando.

Cada paquete de BGP tiene como principal propósito identificar qué servicio será el que se va a utilizar. Las cabeceras de BGP se ilustran en la figura 2.11



Marker: contiene información de autenticación del mensaje del receptor.

Lenght: longitud total del mensaje en bytes

Type: el tipo de mensaje: Open, Update, Notification, Keep-alive

Data: Información para las capas superiores. Este campo es opcional

Figura 2.10 Cabeceras de BGP

BGP-4 es considerado un protocolo de ruteo para comunicar sistemas autónomos. Existen dos clases de BGP, interno y externo, (IBGP y EBGP). BGP soporta CIDR.

2.12 Capa de Transporte

El Protocolo de Control de la Transmisión ("Transmission Control Pro to Gol", TCP), aunque aquí se presenta como parte de la familia de protocolos TCP/lP, en realidad es un protocolo independiente, de propósito general que se puede adaptar para usarse sobre otro sistema de entrega. Por ejemplo, debido a que TCP hace muy pocas asunciones acerca de la red subyacente, es posible usarlo sobre una sola red Ethernet o sobre la compleja Internet. De hecho, TCP es tan popular que uno de los protocolos de ISO, el TP-4 se ha derivado de él. El estándar TCP está definido en el RFC 793. [Postel, 1981]. La figura 2.12 muestra este protocolo.

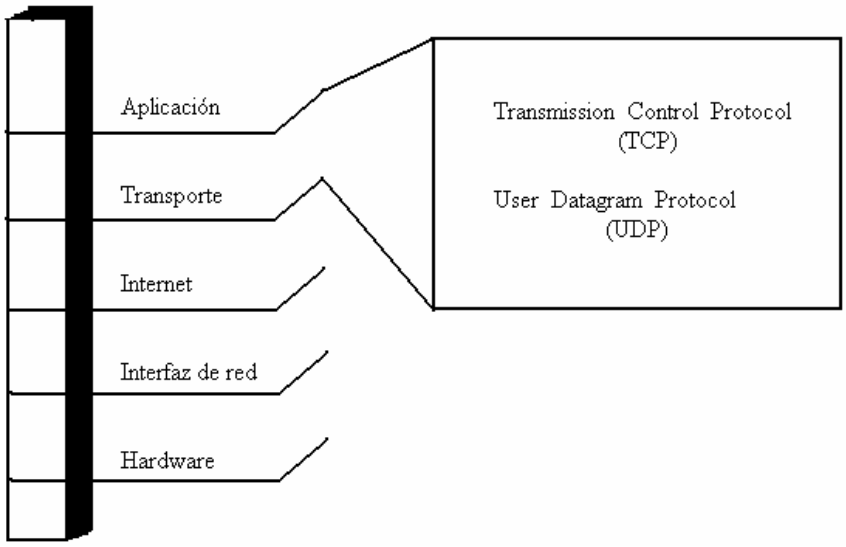


Figura 2.12 TCP

2.12.1 La Necesidad de una Entrega Garantizada.

En el nivel mas bajo, las redes de comunicaciones ofrecen una entrega no confiable de paquetes. Los paquetes pueden perderse o destruirse cuando ocurren errores en la transmisión de datos, cuando falla la red o cuando la red está demasiado saturada. Las redes que envían dinámicamente los paquetes, los podrían entregar en desorden, retardarlos o entregarlos duplicados. Más aún, las tecnologías de red subyacentes podrían dictar un tamaño óptimo de paquete u otras restricciones necesarias para lograr los niveles óptimos de transferencia.

En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de información de una computadora a otra. El uso de un sistema de entrega no orientado a la conexión, no confiable para la transferencia de grandes cantidades de datos es tedioso y problemático además de que requeriría que los programadores desarrollaran un método de detección y corrección de errores para cada programa de aplicación.

Debido a la dificultad que representa la elaboración de software que ofrezca confiabilidad en cuanto a los conocimientos técnicos que un programador necesitaría, sería difícil contar con tal software.

2.12.2.- Propiedades de un Servicio de Entrega Confiable.

La interfaz entre los programas de aplicación y el servicio de entrega de TCP/P debe contar con 5 características:

- Orientación a “Streams” o Flujos.
- Conexión de circuitos virtuales
- Transferencia con Buffer
- “Stream” no estructurado
- Conexión Full Dúplex

2.12.3 Proporcionando Confiabilidad

Para que un software de protocolo pueda ofrecer una transferencia confiable si el sistema de comunicación inferior sólo ofrece entrega no confiable de paquetes, se utiliza una técnica conocida como acuse de recibo positivo con retransmisión (positive aknowledgmet). La técnica requiere un recipiente para comunicarse con la fuente, mandando un mensaje de regreso llamado acuse de recibo o (“acknowledge’) a medida que va recibiendo los datos, el que envía manda un registro con cada paquete que envía y espera el acuse de recibo antes de enviar el siguiente paquete.

El que envía también activa un reloj cuando envía un paquete y lo retransmite si el tiempo de reloj expira antes de recibir el acuse de recibo. La figura 2.13 muestra cómo el protocolo más simple con acuse de recibo transfiere los datos, cada línea diagonal representa la transferencia de un mensaje a través de la red.

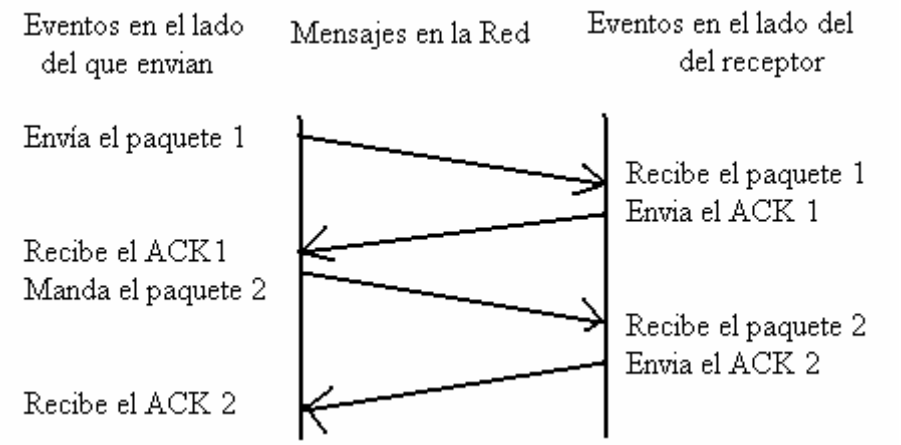


Figura 2.13 Transferencia de un mensaje

Un protocolo usando acuse de recibo con retransmisión que envía espera un acuse de recibo para cada paquete enviado. La distancia vertical hacia abajo representa el incremento del tiempo y las

líneas diagonales en medio representan la transmisión de paquetes en la red. La transferencia de paquetes se muestra en la figura 2.14

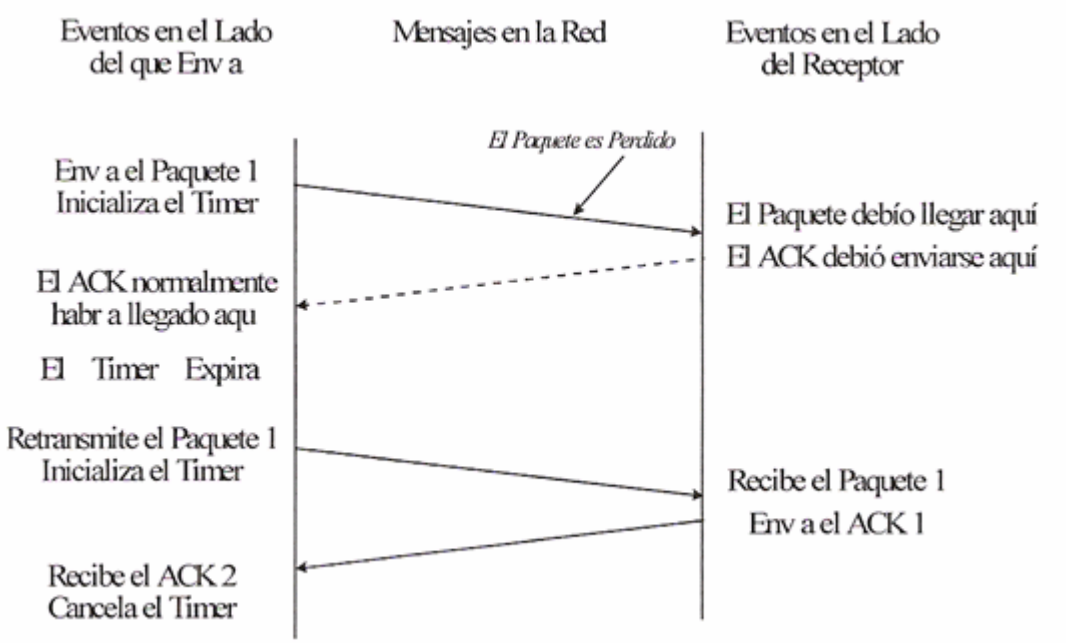


Figura 2.14 Transmisión de paquetes en red

El problema final de confiabilidad surge cuando el sistema de entrega de paquetes subyacente duplica los paquetes. Los duplicados también pueden originarse cuando las redes experimentan retardos largos que causan la retransmisión prematura.

Para resolver la duplicación se requiere especial cuidado porque tanto los paquetes como el acuse de recibo podrían estar duplicados. Usualmente, los protocolos confiables detectan los paquetes duplicados al asignarle a cada paquete un número de secuencia y exigiéndole al receptor que recuerde los números se secuencia que ha recibido.

En la figura 2.14, el “tímeout” y retransmisión ocurre cuando se pierde un paquete. Las líneas punteadas muestran el tiempo que tomaría la transmisión de un paquete y su acuse de recibo si el paquete no se hubiera perdido.

Para evitar confusiones causadas por los acuses de recibo duplicados o retardados, los protocolos con acuse de recibo mandan los números de secuencia de regreso en los acuses de recibo para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

2.12.4 Las Ventanas Deslizantes (“Sliding Windows”)

Antes de examinar el servicio de flujo de TCP, se debe explorar un concepto adicional sobre el que trabaja la transmisión de flujos. El concepto, conocido como Ventanas Deslizantes, se asegura que la transmisión de “streams” sea eficiente. Para lograr la confiabilidad, el que manda, transmite un paquete y luego espera su acuse de recibo antes de transmitir otro.

Los datos sólo fluyen entre las máquinas en una sola dirección a la vez, aún cuando la red sea capaz de realizar comunicaciones simultáneas en ambos sentidos. La red estará totalmente inactiva durante los momentos en que las máquinas retarden sus respuestas (ejemplo; mientras las máquinas calculan las sumas de controlo las rutas). Si se imagina una red con largos retrasos en la transmisión, el problema es claro: Un protocolo con acuse de recibo positivo desperdicia una parte

sustancial del ancho de banda porque debe retrasar el envío de un nuevo paquete hasta no recibir el acuse de recibo del paquete previo.

La técnica de la Ventana Deslizante es una forma más compleja que la del acuse de recibo y retransmisión que el sencillo método mostrado anteriormente. Los protocolos de la ventana deslizante usan mejor el ancho de banda de la red porque le permiten al que envía transmitir múltiples paquetes antes de esperar un acuse de recibo.

La manera más sencilla de conceptual izar la operación de las Ventanas Deslizantes es imaginándose la secuencia de paquetes a ser transmitidos como lo muestra la figura 2.15. El protocolo pone una pequeña ventana en la secuencia y transmite todos los paquetes que quepan dentro de ella.

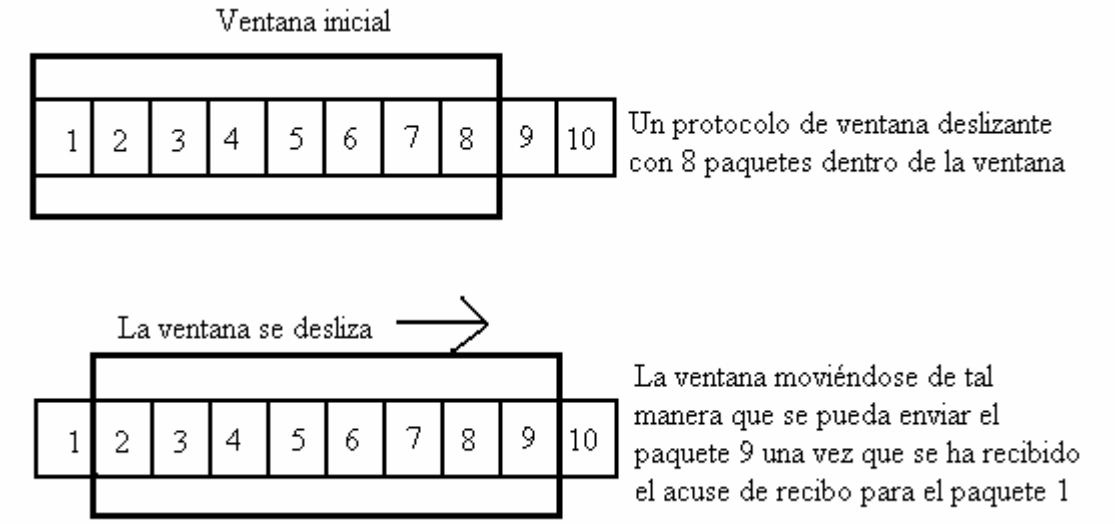


Figura 2.15 Ventanas deslizantes

Técnicamente, el número de paquetes sin acuse de recibo que pueden existir en un momento dado está limitado por el tamaño de la ventana a un número pequeño y fijo. Por ejemplo, en un protocolo de ventana deslizante con tamaño de ventana de 8, el que envía tiene permitido transmitir 8 paquetes antes de recibir un acuse de recibo.

Como la muestra la Figura 2.15, una vez que el que envía recibe un acuse de recibo del primer paquete dentro de la ventana, la “mueve” longitudinalmente y envía el siguiente paquete. La ventana continúa moviéndose mientras se estén recibiendo los acuses de recibo.

El desempeño de los protocolos de ventana deslizante depende del tamaño de la ventana y de la velocidad a la que la red acepte lo paquetes. La figura 2.16 muestra un ejemplo de la operación del protocolo de ventana deslizante cuando envía tres paquetes. Nótese que el que envía manda los tres primeros paquetes antes de recibir acuse de recibo alguno.

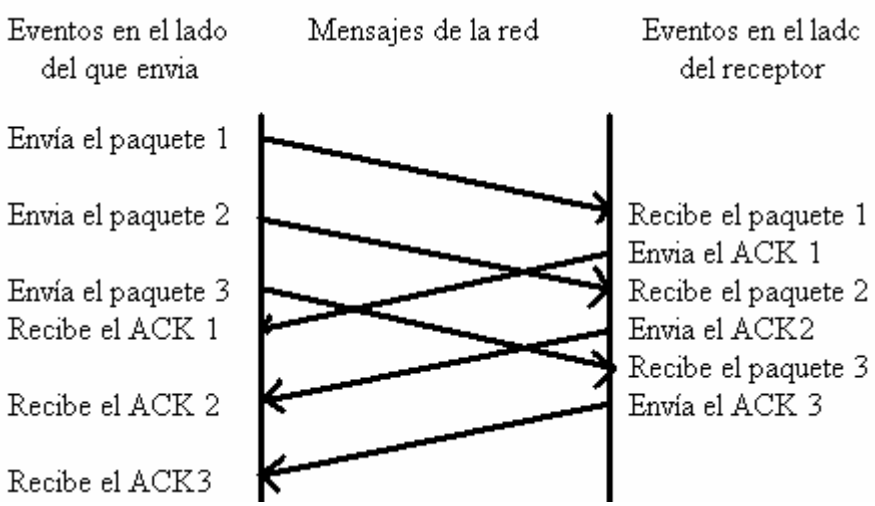


Figura 2.16 Ejemplo de transmisión de paquetes

Cuando el tamaño de la ventana es 1, el protocolo de la ventana deslizante es exactamente igual que el protocolo simple de acuse de recibo positivo. Al incrementar el tamaño de la ventana, es posible eliminar la inactividad de la red totalmente.

Esto es, en el caso continuo, el que envía podría transmitir paquetes tan rápido como la red pudiera transmitirlos. El punto principal es: debido a que un protocolo de ventana deslizante bien configurado mantiene a la red totalmente saturada de paquetes, obtiene un "throughput" sustancialmente mas alto que el del protocolo simple con acuse de recibo positivo.

El Concepto Clave es que el que Envía puede Transmitir todos los Paquetes de la Ventana sin Esperar Ningún Acuse de Recibo.

Conceptualmente, un protocolo de ventana deslizante siempre recuerda qué paquetes han sido notificados como recibidos y mantiene un "tímer" separado para cada paquete sin acuse de recibo. Si un paquete se pierde, el "tímer" expira y el que envía retransmite el paquete.

Cuando el que envía mueve su ventana, deja atrás a todos los paquetes con acuse de recibo. En el lado del receptor, el software del protocolo mantiene una ventana similar, aceptando y acusando de recibido los paquetes como van llegando.

Así, la ventana separa la secuencia de paquetes en tres conjuntos: los que están a la izquierda de la ventana son los que han sido transmitidos, recibidos y notificados exitosamente; los que están a la izquierda son los que todavía no son transmitidos y los que están dentro de la ventana son los que están siendo transmitidos. El paquete con el número mas bajo dentro de la ventana es el primer paquete de la secuencia que no ha sido notificado como recibido.

2.12.5 Protocolo de Control de la Transmisión (Transmission Control Protocol. TCP)

Ahora que se ha entendido el principio de la ventana deslizante, se examinará el servicio de "stream" confiable proporcionado por la familia de Protocolos TCP/IP. El servicio se define como "Transmission Control Protocol" o TCP. El servicio confiable de "stream" es tan importante que al protocolo a menudo se le llama TCP/IP. Es importante entender que: TCP es un protocolo de comunicación, no una pieza de software.

La diferencia entre un protocolo y el software que lo implanta es análoga a la diferencia entre la definición de un lenguaje de programación y un compilador, lo que ocurre es que frecuentemente se olvida la diferencia entre la definición y la implantación.

El Protocolo TCP especifica el formato de los datos y acuses de recibo que dos computadoras intercambian para lograr una transferencia confiable, al igual que los procedimientos usados por las computadoras para asegurarse de que los datos lleguen correctamente. Especifica cómo el software de TCP distingue entre los múltiples destinos en una máquina dada y cómo las máquinas que se comunican se recuperan de errores tales como paquetes perdidos o duplicados. El Protocolo también especifica cómo dos computadoras inician una transferencia de flujos y cómo se ponen de acuerdo cuando está completa.

Es importante también entender lo que el Protocolo no incluye. Aunque la especificación TCP describe cómo las aplicaciones usan el TCP en términos generales, no dicta los detalles de la interfaz entre una aplicación y TCP. Esto es, la documentación del Protocolo sólo discute las operaciones que TCP ofrece; no especifica los procedimientos exactos que los programas invocan para tener acceso a estas operaciones.

La razón para no especificar la interfaz para la programación de aplicaciones es flexibilidad. En particular, porque los programadores usualmente lo implantan sobre el sistema operativo de las computadoras y deben utilizar la interfaz que cada sistema operativo ofrezca. Ésta le da al programador la flexibilidad que hace posible tener una sola especificación para TCP que se puede usar para implantarlo en una gran variedad de máquinas.

Debido a que TCP asume muy poco acerca del sistema de comunicaciones subyacente, se puede usar con una gran variedad de sistemas de entrega de paquetes, incluyendo IP. Por ejemplo, TCP se puede implantar sobre líneas telefónicas, redes locales, redes de fibra óptica de alta velocidad o redes lentas. De hecho, la gran variedad de sistemas de entrega que TCP puede usar es una de sus fuerzas principales.

2.12.5.1 Puertos. Conexiones y Puntos de Conexión.

TCP, al igual que el “User Datagram Protocol”, (UDP) (que se verá en la siguiente sección), reside arriba de IP en el esquema de protocolos por capas. TCP permite que las múltiples aplicaciones de una máquina dada se comuniquen de manera concurrente y demultiplexa el tráfico TCP entrante entre las aplicaciones. TCP usa los números de puerto para identificar el destino final dentro de la máquina. Cada puerto tiene asignado un número entero pequeño que lo identifica.

Una conexión consiste de un circuito virtual entre dos aplicaciones, así que es natural asumir que una aplicación sirve como el punto de conexión. TCP define un punto de conexión como un par de enteros; (nodo, puerto), donde nodo es la dirección IP de un nodo y puerto es un puerto TCP en dicho “host”. Por ejemplo, el punto de conexión (128.10.2.3,25) especifica el puerto TCP 25 en la máquina con dirección IP 128.10.2.3.

Recuérdese que una conexión se define por sus dos puntos de conexión. Así, si hay una conexión de la máquina (18.26.0.36) a la máquina (128.10.2.3), podría definirse por los puntos de conexión: (18.26.0.36,1069) y (128.10.2.3,25).

Mientras tanto, otra conexión podría estar en progreso desde la máquina (128.9.0.32) a la misma máquina de (128.10.2.3), identificada por sus puntos de conexión: (128.9.0.32, 1184) y (128.10.2.3,53).

Hasta aquí el ejemplo ha sido muy sencillo porque los puertos usados en todos los puntos de conexión han sido únicos. Sin embargo, la abstracción de conexión permite múltiples conexiones compartiendo un punto de conexión. Por ejemplo, se podría agregar otra conexión a las dos de arriba desde la máquina (192.100.202.5.139): (192.100.202.5,1184) y (128.10.2.3,53).

Podría parecer extraño que dos conexiones puedan usar el puerto TCP 53 de la máquina 128.10.2.3 de forma simultánea, pero no existe ninguna ambiguedad porque TCP asocia los mensajes entrantes con una conexión en lugar de un puerto, usa ambos puntos de conexión para identificar la conexión apropiada. Debido a que TCP identifica una conexión por un par de puntos de conexión, un puerto TCP dado puede compartirse por múltiples conexiones en la misma máquina.

2.12.5.2 Aperturas Pasivas y Activas.

A diferencia de UDP, TCP es un protocolo orientado a la conexión que requiere que ambos puntos estén de acuerdo a participar. Esto es, antes de que el tráfico TCP pueda pasar por una Internet, las aplicaciones de ambos lados deben ponerse de acuerdo en que se desea la conexión. Para hacer esto, la aplicación de un lado realiza una función de apertura pasiva al contactar a su sistema operativo e indicarle que aceptará una conexión entrante.

En ese momento, el sistema operativo asigna un número de puerto TCP para su lado de la conexión. La aplicación en el otro lado entonces contacta a su sistema operativo usando la petición de apertura activa para establecer la conexión. Los dos módulos de software TCP se comunican para establecer y verificar una conexión. Una vez que se ha creado la conexión, las aplicaciones pueden empezar a transferir datos; los módulos de software de TCP en cada extremo intercambian mensajes que garantizan la entrega confiable. Posteriormente se explicarán los detalles de esta comunicación después de examinar el formato de un mensaje TCP.

2.12.5.3.- Segmentos, “Streams” y Números de Secuencia.

TCP ve el flujo de datos como una secuencia de octetos o bytes que divide en segmentos para su transmisión. Normalmente, cada segmento viaja a través de la red en un solo datagrama IP.

TCP usa un mecanismo especializado de ventana deslizante para resolver dos importantes problemas: transmisión eficiente y control de flujo. El mecanismo de la ventana deslizante hace posible enviar múltiples segmentos antes de que llegue un acuse de recibo.

Este mecanismo también resuelve el problema de control de flujo extremo a extremo al permitir que el receptor restrinja la transmisión hasta que tenga suficiente espacio en el buffer para meter más datos.

El mecanismo de la ventana deslizante de TCP opera a nivel de octetos, no a nivel de segmentos o paquetes. Los octetos en el flujo de datos se numeran secuencialmente y el que envía mantiene tres apuntadores asociados con cada conexión.

Los apuntadores definen una ventana deslizante tal como la ilustra la figura 2.17. El primer apuntador marca la izquierda de la ventana deslizante, separando los octetos que han sido enviados y con acuse de recibo de los que todavía no se envían.

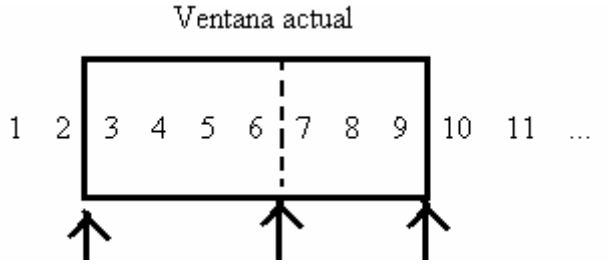


Figura 2.17 Ventana actual

Un segundo apuntador marca la derecha de la ventana deslizante y defina el último octeto de la secuencia que se puede enviar antes de que se reciban mas acuses de recibo. El tercer apuntador marca la frontera dentro de la ventana que separa aquellos octetos que ya se enviaron de los que todavía no se envían.

El software del protocolo manada todos los octetos de la ventana sin retraso, por lo que la frontera dentro de la ventana generalmente se mueve muy rápido de izquierda a derecha.

2.12.5.4 Un Ejemplo de una Ventana Deslizante de TCP.

Los octetos 1 y 2 ya fueron enviados y se recibió el acuse de recibo, los octetos 3 a 6 ya fueron enviados pero no ha llegado su acuse de recibo, los octetos 7 a 9 todavía no han sido mandados pero serían enviados sin demora alguna y los octetos 10 en adelante no se pueden enviar hasta que la ventana se mueva.

Se ha descrito cómo la ventana TCP del que envía se mueve y se ha mencionado que el receptor debe mantener una ventana similar para armar el “stream”. Es importante entender que debido a que las conexiones TCP son full dúplex, dos transferencias proceden inmediatamente sobre cada conexión, una en cada dirección.

Las transferencias son totalmente independientes porque en cualquier momento los datos pueden fluir a través de la conexión en una dirección o en ambas. Así, el software de TCP en cada extremo mantiene dos ventanas por conexión (para un total de cuatro), una se desplaza a lo largo de los datos del “stream” que se están enviando, mientras las otras se desplazan a lo largo de los datos recibidos.

2.12.5.5.- Tamaño de Ventana Variable y Control de Flujo.

Una diferencia entre el protocolo de la ventana deslizante de TCP y el protocolo simplificado de ventana deslizante presentado al principio, es que TCP permite que el tamaño de la ventana cambie con el tiempo. Cada acuse de recibo, el cual especifica cuántos octetos se han recibido, contiene un aviso de la ventana que especifica cuántos octetos adicionales de datos el receptor está preparador para aceptar.

Este anuncio de ventana se puede ver como el tamaño actual del buffer del receptor. En respuesta a un aviso de la ventana incrementado, el que envía incrementa el tamaño de su ventana deslizante y procede a enviar octetos sin acuse de recibo. En respuesta a un decremento en el aviso de la ventana el que envía decrementaría el tamaño de su ventana y dejaría de enviar los octetos a la derecha de la frontera de la ventana. El software de TCP no debe contradecir los avisos previos al encoger la ventana después de que recibe la aceptación de los octetos del “stream”.

En vez de eso, si los avisos acompañan los acuses de recibo son cada vez más pequeños, el tamaño de la ventana cambiará en el momento en que se mueva. La ventaja de usar una ventana de tamaño variable es que ofrece tanto control de flujo así como también una transferencia confiable.

Si los “buffers” del receptor se comienzan a llenar, ya no podrá tolerar más paquetes, así que enviará un aviso de la ventana. En un caso extremo el receptor manda un aviso de la ventana de cero para detener todas las transmisiones. Posteriormente, cuando haya espacio disponible en el buffer el receptor mandará un aviso de la ventana distinto a cero para activar nuevamente el flujo de datos.

El tener un mecanismo para el control del flujo es esencial en un ambiente de Internet, donde las máquinas de diferentes velocidades y tamaños se comunican a través de Redes y Puertas (“gateways’) de diferentes capacidades y velocidades.

En realidad hay 2 problemas independientes de flujo. Primero, los protocolos de Internet necesitan un control de flujo de extremo a extremo, entre las máquinas fuente y destino. Por ejemplo, cuando una minicomputadora se comunica con un gran “mainframe”, la minicomputadora necesita regular la entrada de datos o el software del protocolo se saturará muy rápido.

Así, TCP debe implantar control de flujo de extremo a extremo para garantizar una entrega confiable. Segundo, los protocolos de Internet necesitan un mecanismo de control de flujo que les permita a los sistemas intermedios (como los “gateways’) controlar una fuente que mande más tráfico del que la máquina pueda tolerar.

Cuando las máquinas intermedias se saturan, esta condición se llama congestión, todos los mecanismos que resuelven este problema se llaman mecanismos de control de congestión. TCP usa el esquema de la ventana deslizante para resolver el problema del control de flujo de extremo a extremo; no tiene un mecanismo explícito para el control de la congestión.

Una implantación cuidadosamente programada puede detectar y recuperarse de la congestión mientras que una mala implantación la puede empeorar. En particular, un

esquema de retransmisión cuidadosamente seleccionado puede ayudar a evitar la congestión mientras que un esquema pobre puede complicarlo.

2.12.5.6 Formato del Segmento de TCP.

La unidad de transferencia entre el software TCP de dos máquinas se llama segmento. Los segmentos son intercambiados para establecer conexiones, transferir datos, mandar acuses de recibo, anunciar el tamaño de la ventana y cerrar las conexiones. Debido a que TCP usa “piggybacking”, un acuse de recibo que viaja de la máquina A hacia la B puede viajar en el mismo segmento en que viajan los datos de A hacia B aún cuando el acuse de recibo se refiere a los datos enviados de B hacia A. La figura 2.18 muestra el formato del segmento TCP.

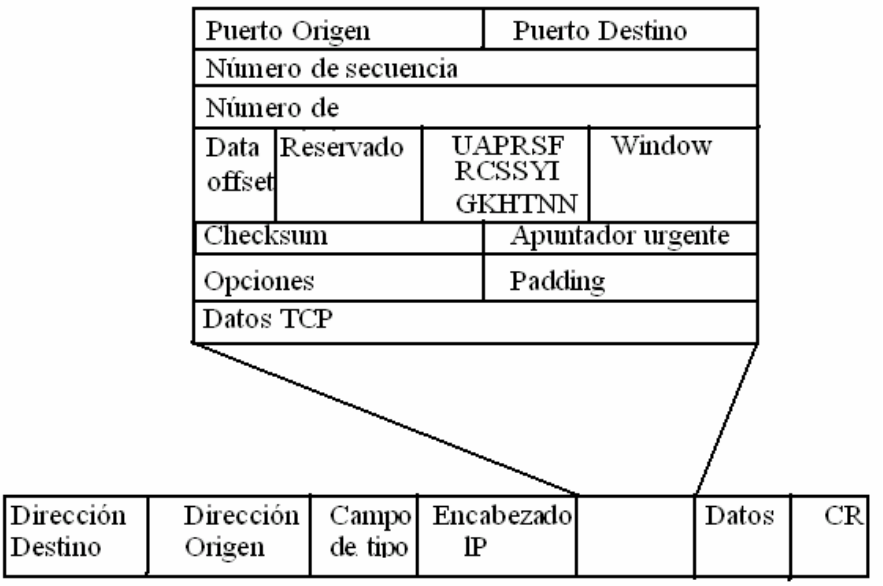


Figura 2.18 El formato de un segmento TCP con cabecera TCP

Cada segmento se divide en dos partes; encabezado y datos. El encabezado, conocido como encabezado TCP, lleva la identificación esperada e información de control. Los campos “Puerto Fuente” y “Puerto Destino” contienen los números de puerto TCP que identifican las aplicaciones en los extremos de la conexión.

El campo “Número de Secuencia” identifica la posición de los datos del segmento en el flujo de que envía. El campo “Número de Acuse de Recibo” identifica el número de octeto del que la fuente espera recibir notificación. Debe notarse que el número de secuencia se refiere al flujo que viaja en la misma dirección del segmento, mientras que el “Número de Acuse de Recibo” se refiere al “stream” que viaja en la dirección opuesta al segmento.

El campo “HLEN” contiene un entero que especifica la longitud del encabezado del segmento medido en múltiplos de 32 bits. Es necesario porque la longitud del campo “Opciones” varía dependiendo de las opciones que se hayan incluido. Así, el tamaño del encabezado TCP varía dependiendo de las opciones seleccionadas. El campo de 6 bits marcado como “Reservado” es necesario para usos futuros.

Algunos segmentos llevan sólo un acuse de recibo mientras que otros llevan datos. Otros más, llevan peticiones para establecer o cerrar una conexión. El software de TCP usa el campo de 6 bits etiquetado como “Bits de Código” para determinar el propósito y contenido del segmento. Los seis bits dicen cómo interpretar los otros campos del encabezado (“Header’) de acuerdo a la tabla.

Bit (de izquierda a derecha)	Significado si el bit está encendido
URG	El campo del apuntador Urgente es válido
ACK	El campo del Acuse de Recibo es válido
PSH	Este segmento solicita un push
RST	Reinicializa la comunicación
SYN	Sincroniza los números de secuencia
FIN	El que envía ha llegado al fin de su flujo de bytes

El software de TCP avisa cuántos datos espera recibir cada vez que manda un segmento al especificar el tamaño del buffer en el campo “WINDOW”, El campo contiene un entero sin signo de 32 bits en el orden de bytes estándar de la red. Los anuncios de la ventana ofrecen otro ejemplo de piggybacking porque acompañan a todos los segmentos, lo mismo los que llevan datos que los que sólo llevan un acuse de recibo.

2.12.5.7 Datos Fuera de Banda.

Aunque TCP es un protocolo orientado a la conexión, algunas veces es importante para el programa al final de una conexión enviar datos fuera de banda, esto es, sin esperar a que el programa al otro lado de la conexión consuma los octetos del “stream”. Por ejemplo, cuando TCP se usa para dar “Iogin” a una sesión remota, el usuario puede decidir enviar una secuencia de teclas que interrumpan o aborten el programa. Tales señales son más útiles cuando un programa de la máquina remota deja de funcionar correctamente. Estas señales se deben enviar sin esperar a que el programa lea los octetos del “stream” TCP (o un usuario no sería capaz de abortar los programas que dejan de leer la entrada).

Para utilizar el señalamiento fuera de banda, TCP permite que el que envía especifique los datos como urgentes, lo que significa que el programa receptor deberá ser notificado de su llegada tan pronto como sea posible sin importar su posición actual en el “stream”. El protocolo especifica que cuando se encuentren datos urgentes, el receptor deberá notificar a cualquier aplicación que esté asociada con la conexión que cambie a “Modo Urgente”. Después de que todos los datos urgentes se han consumido, TCP le dice a la aplicación que regrese a la operación normal.

Los detalles exactos de cómo TCP le informa a la aplicación dependen del sistema operativo de la computadora en cuestión. El mecanismo usado para marcar los datos como urgentes cuando se transmiten en un segmento consiste en el bit URG del campo “Apuntador Urgente”. Cuando el bit URG se enciende, el apuntador urgente especifica la posición en la ventana donde los datos urgentes terminan.

2.12.5.8 Opción de Tamaño Máximo del Segmento

No todos los segmentos enviados en una conexión son del mismo tamaño. Sin embargo, ambos extremos necesitan ponerse de acuerdo en el tamaño máximo de segmento que transferirán. El software de TCP usa el campo “Opciones” para negociar con el software de TCP al otro lado de la conexión; una de las opciones permite que el software TCP especifique el tamaño máximo de segmento (MSS) que está esperando recibir.

Por ejemplo, cuando una pequeña computadora personal que sólo tiene unos cuantos cientos de bytes de buffer se conecta a una supercomputadora, puede negociar un MSS que restrinja los segmentos de tal manera que quepan en el buffer. Es especialmente importante para las computadoras conectadas a las redes locales de alta velocidad escoger un tamaño máximo de segmento que llene los paquetes o no harán un buen uso del ancho de banda.

2.12.5.9.- Cálculo de la Suma de Control (“Checksum”)

El campo “Checksum” del Encabezado TCP contiene una suma de control de 16 bits usada para verificar la integridad de los datos así como también del Encabezado TCP. Para calcular la Suma de Control, el software de TCP en la máquina que envía realiza el siguiente procedimiento: antepone un pseudo encabezado al segmento, le pospone suficientes bytes con valor “0” para que su longitud sea un múltiplo de 16 bits y calcula la suma de control sobre todo el segmento resultante. TCP no cuenta los ceros agregados como “Pad” en la longitud del segmento ni los transmite.

También, asume que el campo de suma de control en sí mismo tiene puros ceros para los propósitos de la suma de control.

Al igual que otros “checksums”, TCP usa aritmética de 16 bits y toma el complemento a uno de la suma con complemento a uno. En el “site” receptor, el software de TCP realiza los mismos cálculos para verificar que el segmento ha llegado intacto. El propósito de usar un pseudo encabezado al igual que en UDP, es permitir que el receptor verifique que el segmento ha llegado a su destino correcto. Este Encabezado incluye tanto la dirección IP del destino así como el número de puerto. Tanto la dirección IP destino como la fuente son importantes para TCP porque debe usarlas para identificar la conexión a la que pertenece un segmento dado. Por lo tanto, siempre que llega un datagrama con un segmento TCP, IP debe pasar a las direcciones IP fuente y destino al igual que el segmento en sí. La figura 2.19 muestra el formato del pseudo encabezado usando en el cálculo de la suma de control.

Figura 2.19 Formato de Checksum

En el lado del receptor, la información es extraída del datagrama IP que llevó el segmento. TCP le asigna al campo “Protocolo” el valor que el sistema de entrega subyacente usará en su campo “tipo de protocolo”. Para los datagramas IP que llevan TCP, el valor es 6. El campo “Longitud TCP” especifica la longitud total del segmento TCP incluyendo el Encabezado TCP. En el lado del receptor, la información del pseudo encabezado es extraída e incluida en la suma de control para verificar que el segmento llegó al destino correcto intacto.

2.12.5.10 Acuses de Recibo y Retransmisiones.

Debido a que TCP manda datos en segmentos de longitud variable, y porque los segmentos retransmitidos pueden incluir más datos que el original, los acuses de recibo no se pueden referir fácilmente a los datagramas o a los segmentos. En su lugar, se refieren a una posición en el “stream” usando los números de secuencia. El receptor colecta los datos de los segmentos que van llegando y reconstruye una copia exacta del “stream” que se está enviando.

Debido a que los segmentos viajan en datagramas IP, se pueden perder o entregarse en desorden; el receptor usa los números de secuencia para reordenar los segmentos. En cualquier momento, el receptor habrá reconstruido cero o mas octetos contiguamente desde el principio del “stream”, pero puede haber piezas adicionales de datagramas que llegaron en desorden.

El receptor siempre manda el aviso del “stream” que se ha recibido correctamente. Cada aviso especifica un valor de secuencia que es el número adicionando un uno en la última posición de octeto en el que ha recibido. Así, el que envía recibe constante retroalimentación del receptor a medida que va avanzando a lo largo del “stream”. Esta idea se puede resumir así: Los Acuses de Recibo siempre especifican el número de secuencia del siguiente octeto que el receptor espera recibir.

Para entender porqué la carencia de información acerca de todas las transmisiones exitosas hace al protocolo menos eficiente, su póngase una ventana de 500 octetos que comienza en la posición 101 del “stream” y su póngase que el que envía ha transmitido todos los datos de la ventana mandando 5 segmentos. Supóngase que el primer segmento se perdió pero todos los demás llegaron intactos.

El receptor continúa enviando acuses de recibo, pero todos ellos especifican el octeto 101, el siguiente octeto contiguo que espera recibir. No hay manera de que el receptor le diga al que envía que la mayor parte de los datos de la ventana actual ya llegaron.

Cuando ocurre un “timeout” en el lado del que envía, éste deberá escoger entre dos esquemas potencialmente ineficientes. Podría escoger retransmitir los 5 segmentos en lugar de mandar solo el que falta. Por supuesto, cuando el segmento retransmitido llegue, el receptor habrá recibido correctamente todos los datos de la ventana y habrá mandado un acuse de recibo indicando que espera el octeto 5101 a continuación.

Sin embargo, ése acuse de recibo podría no lIegarle al que envía lo suficientemente rápido como para prevenir la retransmisión innecesaria de los otros de la ventana.

Si el que envía siguiera la política retransmitir sólo el primer segmento sin acuse de recibo, deberá espera el acuse de recibo antes de poder decidir qué y cuánto enviar. Así, se convertiría en un protocolo sencillo con acuse de recibo positivo y podría perder las ventajas de tener una ventana grande.

2.12.5.11 Establecimiento de una Conexión Orientada

Para establecer una conexión, TCP usa el mecanismo llamado “Three Way Handshake” o “Apretón de Manos en Tres Sentidos”. En el caso más simple, el “handshake” o “Apretón de Manos” procede como se muestra en la Figura 2.20

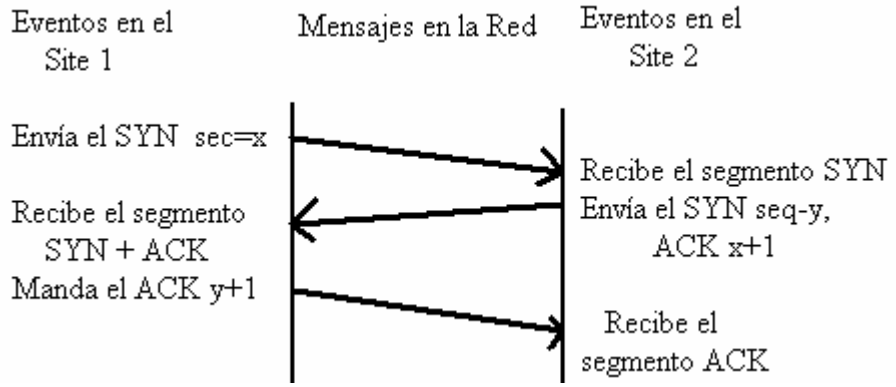


Figura 2.20 Conexión Orientada

El “Three Way Handshake” realiza dos importantes funciones: Garantiza que ambos lados están listos para transferir datos (y que ambos saben que el otro está listo), y permite que ambos estén de acuerdo en los números iniciales de secuencia. Los números de secuencia se envían y se notifican de recibido durante el “Handshake”.

Cada máquina debe escoger un número de secuencia inicial aleatorio que usará para identificar los bytes del flujo que está enviando. Los números de secuencia no pueden comenzar siempre en el mismo valor. En particular, TCP no puede escoger meramente la secuencia 1 cada vez que abra una conexión. Por supuesto, es importante que ambos lados estén de acuerdo en un número inicial, para que números de los octetos usados en los acuses de recibo concuerden con los usados en los segmentos de datos.

2.12.5.12 Números Iniciales de Secuencia

Para ver cómo las máquinas pueden estar de acuerdo en los números de secuencia para dos “streams” después de sólo tres mensajes, recuérdese que cada segmento contiene tanto un campo de número de secuencia como un campo de acuse de recibo. La máquina que inicia el “handshake”, llamada A, pasa su número de secuencia, x, en el campo de secuencia del primer segmento SYN del “handshake”.

La segunda máquina, llamada B, recibe el SYN, graba el número de secuencia y contesta enviando su número de secuencia inicial en el campo de secuencia al igual que un acuse de recibo que especifica que B está esperando el octeto x+1. En el mensaje

final, A “notifica de recibido” de B todos los octetos hasta el y. En todos los casos, los acuses de recibo siguen la convención de usar el número del siguiente octeto esperado.

Se ha descrito cómo TCP usualmente realiza el “three way handshake” intercambiando segmentos que contienen una mínima cantidad de información. Debido al diseño del protocolo, es posible enviar datos junto con los números de secuencia iniciales en los segmentos del “handshake”. En tales casos, el software de TCP debe retener los datos hasta que el “handshake” termine. Una vez que se ha establecido una conexión, el software de TCP puede liberar los datos retenidos y entregárselos rápidamente a una aplicación.

2.12.5.13 Cerrando una Conexión TCP

Dos programas que usan TCP para comunicarse pueden terminar la conversación de una manera agradable usando la operación “clase”. Internamente, TCP usa un “handshake” modificado para cerrar las conexiones. Debe recordarse que las conexiones TCP son full dúplex y que tienen dos “streams” independientes, uno en cada dirección. Cuando una aplicación le dice a TCP que no tiene mas datos para enviar, TCP cerrará la conexión en una dirección.

Para cerrar su mitad de la conexión, el TCP que envía termina de transmitir los datos restantes, espera a que el receptor mande el acuse de recibo y envía entonces un segmento con el bit FIN encendido. El TCP receptor manda su acuse de recibo del segmento FIN y le informa a la aplicación de su lado que no hay mas datos disponibles (ejemplo: usando el mecanismo end of file del sistema operativo).

Una vez que se ha cerrado la conexión en una dirección, TCP se rehusa a aceptar mas datos de esa dirección. Mientras tanto, los datos pueden continuar viajando en la dirección opuesta hasta que el que envía los rechaza. Por supuesto que, los acuses de recibo siguen llegando al que envía aún cuando la conexión se haya cerrado. Cuando ambas direcciones se han cerrado, el software de TCP de cada punto borra su registro de la conexión.

Los detalles del cierre de una conexión son un poco mas ingeniosos que lo que se acaba de explicar porque TCP usa un “three way handshake” modificado para cerrar una conexión. La figura 2.21 ilustra el procedimiento.

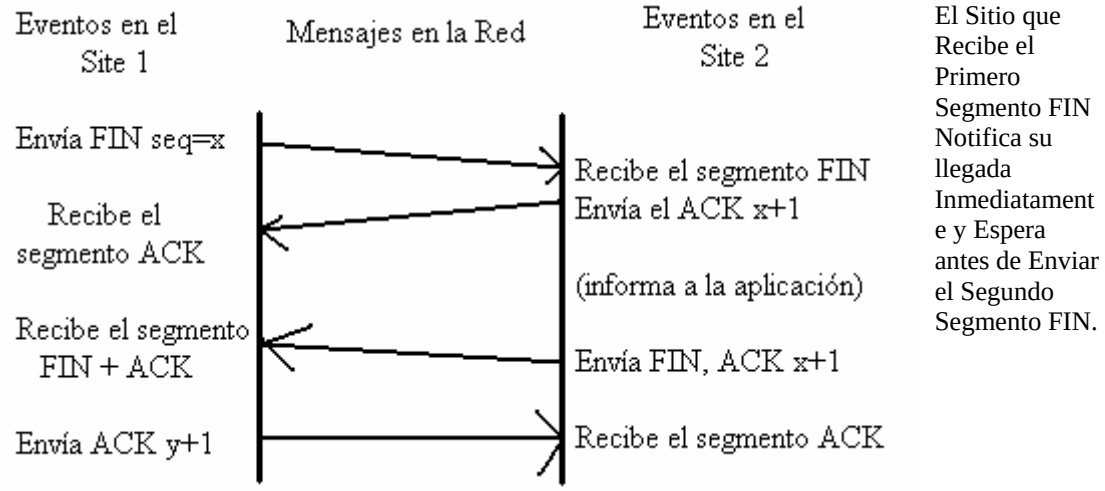


Figura 2.21 Three Way Handshake modificado

La diferencia entre el "handshake" usado para establecer una conexión del usado para terminarla ocurre después de que una máquina recibe el segmento FIN inicial. En lugar de generar un segundo segmento FIN inmediatamente, TCP manda un acuse de recibo y entonces le informa a la aplicación acerca de la petición de terminar la conexión. lnformarle a la aplicación acerca de esta petición y obtener una respuesta puede tomar una considerable cantidad de tiempo (ejemplo: puede involucrar interacción humana). El acuse de recibo evita la retransmisión del segmento FIN inicial durante la espera. Finalmente, cuando la aplicación le indica al TCP que cierre la conexión, TCP manda el segundo segmento FIN y el sitio original contesta con el tercer mensaje, un ACK.

2.12.5.14.- Reinicialización de una Conexión TCP.

Normalmente, una aplicación usará la operación "close" para terminar una conexión cuando termine de usarla, de esta manera el cierre de las conexiones se considera una parte normal del uso, análogo a cerrar un archivo. Algunas veces surgen condiciones anormales que obligan a una aplicación o al software de la red a romper una conexión. TCP ofrece un mecanismo de Reinicialización para tales desconexiones anormales.

Para reinicializar una conexión, un lado inicia la terminación enviando un segmento con el bit RST del campo de "Códigos" encendido. El otro lado responde a un segmento "Reset" inmediatamente abortando la conexión. TCP también le informa a la aplicación que ha ocurrido una Reinicialización, lo que implica que las transferencias en ambas direcciones cesan inmediatamente y que los recursos tales como el buffer se liberan.

2.13.- Números de Puertos Reservados.

Al igual que UDP, TCP combina el enlace estático y dinámico de los puertos, usando un conjunto de asignaciones de puertos bien conocidos para los programas comúnmente invocados (ejemplo: el correo electrónico), pero dejando disponibles la mayor parte de los números de puertos para que el sistema operativo los asigne a los programas que los necesiten. La especificación establece que sólo los números de puerto menores a 1024

serán usados para los puertos bien conocidos; los restantes hasta el 65535 para las diferentes aplicaciones.

La siguiente tabla muestra algunos de los puertos TCP actualmente asignados. Se debe resaltar que aunque los números de puerto de TCP y de UDP son independientes, los diseñadores han escogido usar los mismos números de puerto para cualquier servicio que se pueda acceder por TCP o por UDP. Por ejemplo, un servidor de nombre de dominios se puede acceder por ambos transportes.

Decimal	Nombre	Nombre en UNIX	Descripción
0			Reservado
1	TCPMUX	-	Multiplexor TCP
5	RJE	Echo	Echo
9	DISCARD	discard	Descartar
11	USERS	systat	Usuarios activos
13	DAYTIME	daytime	Hora el día
15	-	netstat	Programa para ver estado de la red
17	QUOTE	qotd	Cita del día
19	CHARGEN	chargen	Generador de caracteres
20	FTP-DATA	ftp-data	File Transfer Protocol (datos)
21	FTP	ftp	File Transfer Protocol
23	TELNET	telnet	Conexión de terminal virtual
25	SMTP	smtp	Simple Mail Transport Protocol
37	TIME	time	Hora
42	NAMESERVER	name	Nombre del host servidor
43	NICNAME	whois	Programa que identifica a usuarios
53	DOMAIN	nameserver	Servidor de nombres de dominios
77	-	rje	Cualquier servicio RJE privado
79	FINGER	finger	Programa que da información de usuarios en un sistema
93	DCP	-	Device Control Protocol
95	SUPDUP	supdup	Protocolo SUPDUP
101	HOSTNAME	hostnames	Nombre NIC del host name servidor
102	ISO-TSAP	iso-tsap	ISO-TSAP
103	X400	x400	Servicio de Mail X.400
104	X400-SND	x400-snd	Envío de Mail X.400
111	SUNRPC	sunrpc	Llamadas a procedimientos remotos de SUN
113	AUTH	auth	Servicio de autenticación
117	UUCP-PATH	uucp-path	Servicio de rutas UUCP
119	NNTP	nntp	USENET New Transfer Protocol
129	PWDGEN	-	Protocolo generador de Passwords
139	NETBIOS-SSN	-	Servicio de sesiones NETBIOS
160-223	Reservados		

En cualquier protocolo, el número de puerto 53 está reservado para los servidores del sistema de nombre de dominios.

2.14.- Protocolo de Datagrama de Usuario ("User Dataqram Protocol. UDP).

Además de TCP, existe otro protocolo en la capa de transporte, el "User Datagram Protocol", especificado en el RFC 768. [Postel, 1980].

El UDP ofrece un servicio de conexión para los procesos de la capa de aplicación. Le permite a un proceso enviar mensajes a otros procesos con un mínimo de mecanismos involucrados. Un ejemplo del uso de este protocolo es en la administración centralizada de redes con SNMP.

UDP trabaja sobre IP, al igual que TCP. Debido a que es un protocolo no confiable (al igual que el protocolo subyacente IP), y que no está orientado a la conexión, UDP tiene muy poco que hacer. Esencialmente sólo le agrega la capacidad de direccionamiento de puertos a IP y realiza la Suma de Control. Esto se entenderá mejor al examinar el formato de su encabezado, mostrado en la siguiente tabla.

Puerto Origen	Puerto Destino
Longitud del mensaje	Checksum
Datos	
Datos	
Datos	

El encabezado incluye los puertos origen y destino. Como en el caso de TCP, se debe hacer uso de los puertos al realizar una transmisión. El campo "Longitud" contiene la longitud de todo el segmento UDP, incluyendo el encabezado. La suma de control al igual al que se usa en TCP e IP sirve para verificar la integridad de esta porción de información.

2.15 Protocolos de Aplicación y Servicios.

No es posible apreciar los detalles técnicos de Internet sin conocer los servicios que proporciona. Mucha de la discusión acerca de los servicios se enfoca a los llamados protocolos, los cuales dan la fórmula para enviar mensajes, especificar los detalles de los formatos de dichos mensajes y describir cómo controlar las condiciones de error. Más importante aún, es que nos permiten definir los estándares de comunicación.

De alguna forma, los protocolos son a la comunicación lo que los programas a la computación. Un lenguaje de programación nos permite especificar o comprender la computación sin necesidad de conocer los detalles de cualquier conjunto de instrucciones del CPU. Similarmente un protocolo permite entender la comunicación de datos sin la necesidad de conocer los detalles del hardware de algún fabricante en particular.

Al hacer referencia a que TCP/lP no era una pieza de software independiente y es en realidad un servicio de comunicación de las diferentes aplicaciones a las que otorga la capacidad de transportar la misma para simular que sé esta llevando información de un sitio a otro de manera transparente para el usuario.

De los servicios más relevantes y usados de manera conocida, está el correo electrónico, el navegador de Internet, ("Netscape" o "Mosaic"), el servicio de Información a distancia, el World Wide Web, el servicio de nombres de dominio (DNS), entre otros.

2.15.1 Protocolo de Transferencia de Archivos ("File Transfer Protocol", FTP).

La transferencia de archivos, es una de las actividades de mayor frecuencia en una red, el Protocolo FTP provee de un mecanismo confiable y eficiente para llevar a cabo esta tarea.

Dado un protocolo de transporte confiable de extremo a extremo como el TCP, la transferencia de archivos podría parecer trivial. Sin embargo, los detalles de autorización, el nombre y la representación entre máquinas heterogéneas hacen que el protocolo sea complejo. Además, el FTP ofrece muchas facilidades que van más allá de la función de transferencia misma.

Este protocolo proporciona una interfaz interactiva que permite a las personas interactuar fácilmente con los servidores remotos. Por ejemplo, un usuario puede pedir una lista de todos los archivos de un directorio en una máquina remota. Incorpora ayuda en línea, mostrando información al usuario acerca de los comandos posibles que se puedan invocar.

El FTP permite al cliente especificar el tipo y formato de datos almacenados. Por ejemplo, el usuario puede especificar si un archivo contiene datos de texto o binarios, así como, si los archivos de texto utilizan los conjuntos de caracteres ASC2 o EBCDIC. Asimismo, el FTP requiere que los clientes se identifiquen, mediante el envío de un nombre de conexión y una clave de acceso al servidor antes de pedir la transferencia de archivos.

2.15.1.1.- FTP y el Modelo Cliente-Servidor.

Como en otros servidores, el protocolo FTP trabaja bajo el procesamiento c1iente-servidor. Los clientes se valen del TCP para conectarse a un servidor. Un proceso servidor maestro espera las conexiones y crea un proceso esclavo para manejar cada conexión. Igual que otros servicios, el proceso servidor se denomina "ftpd", mientras que el cliente se llama "ftp".

Sin embargo, a diferencia de casi todos los servidores el proceso esclavo no ejecuta todos los cómputos necesarios. Por el contrario, el esclavo acepta y maneja la conexión de control de cliente, pero utiliza un tercer proceso para manejar una conexión de transferencia de datos separada. La conexión de control transporta comandos que indican al servidor qué archivo transferir. La conexión de transferencia de datos, que también usa el TCP como protocolo de transporte, transporta todas las transferencias de datos. Por lo general, el cliente y el servidor crean un proceso separado para manejar la transferencia de datos.

El proceso de control del cliente se conecta al proceso de control del servidor mediante una conexión TCP, mientras que los procesos de transferencia de datos asociados utilizan su propia conexión TCP. En general, los procesos de conexión y la conexión de control permanecen activos mientras el usuario continúa con la sesión de FTP.

Sin embargo, - el FTP establece una nueva conexión de transferencia de datos para cada transferencia de archivos. De hecho, muchas de las implantaciones crean un nuevo par de procesos de transferencia de datos, así como también una nueva conexión TCP cada vez que el servidor necesite enviar información al cliente. Así, las conexiones de transferencia de datos y los procesos de transferencia de datos que los emplean pueden crearse de manera dinámica cuando se necesitan, pero la conexión de control continúa a través de una sesión. Una vez que la conexión de control desaparece, la sesión se termina y el software en ambos extremos termina todos los procesos de transferencia de datos.

Por supuesto, las implantaciones de cliente, que se ejecuten en una computadora sin el soporte de sistema operativo para diversos procesos, pueden tener una estructura menos compleja. Tales Implantaciones a menudo sacrifican la generalidad utilizando un solo programa de aplicación para ejecutar la transferencia de datos y las funciones de control. Sin embargo, el protocolo requiere incluso que tales clientes utilicen diversas conexiones TCP, una para el control y otras para la transferencia de datos.

Cuando un cliente establece una conexión inicial con un servidor, el cliente utiliza un número de puerto de protocolo aleatorio asignado localmente, pero se pone en contacto con el servidor en un puerto bien conocido (21). A pesar de que un servidor utilice sólo un puerto de protocolo puede aceptar las conexiones de muchos clientes, puesto que el TCP se vale de ambos puntos extremos para identificar una conexión.

Cuando los procesos de transferencia crean una nueva conexión TCP para un enlace FTP, no pueden usar el mismo par de números de puerto utilizados en la conexión de control. Por el contrario, el cliente obtiene un puerto no utilizado en su máquina y se vale del puerto para ponerse en contacto con el proceso de transferencia de datos en la máquina del servidor. Este proceso de transferencia de datos puede usar el puerto bien conocido (20), reservado para la transferencia de datos FTP.

Sin embargo, debido a que desde un mismo cliente se pueden manejar varias conexiones a un mismo servidor, para que el proceso de transferencia en el servidor acepte solo conexiones del proceso de transferencia apropiado, y gracias a que el protocolo utiliza dos conexiones, el proceso de control de cliente se encarga de obtener un puerto local aleatorio para la conexión de transferencia y comunicar este número de puerto al servidor a través de la conexión de control.
Posteriormente, el servidor crea el proceso de transferencia, que espera a que el proceso de transferencia en el cliente solicite desde el número de puerto informado a través de la conexión de control, una conexión y así iniciar la transferencia de datos.

Además de enviar comandos del usuario al servidor, el FTP utiliza la conexión de control para permitir los procesos de control cliente y servidor, y así, coordinar el uso de puertos de protocolo TCP asignados dinámicamente y la creación de procesos de transferencia de datos que utilicen tales puertos.

Los diseñadores del FTP, lo crearon de tal forma que FTP utiliza el protocolo de terminal virtual de red TELNET. Aunque FTP no permite la negociación de opciones, emplea sólo la definición básica NVT. De este modo, la administración de una conexión de control FTP es mucho más sencilla que la administración de una conexión estándar de TELNET. Sin importar las limitaciones, usar la definición de TELNET, en lugar de intentar una, ayuda a simplificar considerablemente al FTP.

2.15.1.2 Operación de FTP

Para iniciar FTP, se debe proporcionar el nombre o dirección IP de la máquina a la cual desea conectarse. Solamente se puede utilizar el nombre, si el sistema tiene algún método para convertir el nombre a su dirección IP, como en el caso del Servicio de Nombre de Dominio. También se puede especificar un número de puerto si el servidor "ftpd" no escucha en el puerto estándar.

Cuando se establezca la conexión, se solicitará identificación de usuario y contraseña. Una vez que se establezca con éxito la conexión, se ingresará al modo de comandos de "ftp". Bajo ambientes UNIX, si no se especifica nombre o dirección, se ingresa directamente al modo de comando de "ftp".

Los usuarios ven al FTP como un sistema interactivo. Una vez que se invoca, el cliente ejecuta repetidamente las siguientes operaciones: leer una línea de entrada, analizar la línea para extraer un comando y sus argumentos, así como ejecutar el comando con los argumentos especificados. Por ejemplo, para iniciar la versión del FTP disponible UNIX, el usuario invoca el programa ftp: % ftp. El cliente FTP despliega un indicador para el usuario. Después del indicador, el usuario puede teclear cualquiera de los comandos aceptados. Para obtener información acerca de un comando, el usuario teclea el comando de ayuda ("Help Command').

2.15.1.3 FTP Anónimo.

Para proporcionar acceso a los archivos públicos, muchas de las localidades TCP/lP permiten el FTP anónimo. El acceso al FTP anónimo significa que el cliente no necesita una cuenta o clave de acceso, sino especificar un nombre de conexión anónimo y una clave de acceso de invitado. El servidor permite que el usuario anónimo se conecte pero restringe su acceso únicamente a los archivos públicos disponibles.
El usuario invoca al FTP anónimo especificando "anonymous" en el nombre del usuario y cualquier cosa (su "e-mail" completo en algunos sistemas) como contraseña ("password').

2.15.1.4 TELNET ("Telecommunications Network Protocol").

TELNET ofrece el servicio de "Iogin" remoto. Permite a un usuario desde un sistema cliente, iniciar una sesión en un sistema remoto y por lo que respecta al usuario, aparecerá como si estuviera sentado frente al "host" remoto. Una vez que la conexión se ha establecido, el proceso cliente emula una terminal conectada al proceso servidor. Al

igual que FTP; TELNET usa TCP como transporte. El estándar de TELNET se encuentra en el RFC 854.

Esto es un poco más complicado de lo que parece a primera vista, por la amplia variedad de terminales y computadoras existentes, cada una con sus propios códigos de control y características de terminal. Cuando se está conectado directamente a un servidor, la unidad central de procesamiento (CPU) de éste debe administrar la conversión de los códigos de terminal, lo que impone una severa carga en la CPU del servidor. Con varias conexiones remotas activas, la CPU del servidor puede gastar mucho tiempo administrando las conversiones.

TELNET aligera este problema manejando las secuencias características de terminal dentro del protocolo TELNET. Cuando dos máquinas se comunican mediante TELNET, durante la fase de conexión TELNET mismo determina y establece los parámetros de comunicación y de terminal para la sesión, e incluye capacidad de no aceptar un servicio que uno de los extremos de la conexión no pueda administrar. Cuando se establece una conexión mediante TELNET, ambos extremos acuerdan un método para el intercambio de información entre las dos máquinas, descargando la CPU del servidor de un porcentaje considerable de este trabajo.

El Protocolo TELNET utiliza el concepto de terminal virtual de red (NVT) para definir ambos extremos de una conexión TELNET. Cada extremo de la conexión tiene un teclado y una impresora lógicos. La impresora lógica puede desplegar caracteres, y el teclado lógico puede generar caracteres.

Por lo general, la impresora de red es una pantalla de terminal; en tanto que el teclado lógico es el teclado de usuario, aunque puede ser algún archivo o cualquier otro flujo de entrada.

2.15.1.5 Protocolos de Terminal Virtual.

El término “virtual” se usa por que NVT no existe físicamente, es un dispositivo imaginario que presenta las características de una terminal. La idea es liberar a los “hosts” de la carga de tener que mantener las características de todas las terminales con las que se tiene que comunicar. Con TELNET, tanto el dispositivo del usuario como el del servidor tienen que mapear las características de sus terminales a la descripción de una NVT.

El Protocolo de Terminal Virtual ofrece un lenguaje común, mediante la definición de una terminal virtual y un protocolo para transferir información y controlarla a través de la red. La implantación del protocolo de terminal virtual traduce a lenguaje NVT para realizar la transmisión al otro lado de la conexión. La implantación receptora del protocolo NVT traduce entonces de lenguaje NVT a lenguaje nativo.

EL NVT define:

- La forma en la que la información será enviada, por ejemplo, en conjuntos de bytes o en mensajes con algún formato previo.

- Cómo serán enviadas las señales de control de terminal virtual y cómo distinguirlas de la información
- El modo de transferencia de la información que se usará: half dúplex o fuI! dúplex, sincronía o asíncrona y cómo se controla dicha transferencia
- Cómo se transfieren las interrupciones especiales de prioridad y cómo deberán interpretarse.
- La manera en que se le entrega la información al usuario.

2.15.1.6 El Servicio TELNET y el Modelo Cliente-Servidor.

La especificación de TELNET, define un protocolo entre un cliente y un Servidor TELNET, esta especificación dice muy poco acerca de cómo el proceso TELNET se relaciona con las capas inferiores, específicamente con la de transporte, o sea la interfaz con TCP, varias implantaciones comerciales de TCP para computadoras personales incorporan TCP como parte del "kernel", mientras que TELNET corre como una aplicación del sistema operativo.

TELNET es un protocolo de las capas de presentación y de aplicación que corre sobre TCP. TCP y los protocolos de las capas de abajo proporción la conexión confiable entre los procesos cliente y el servidor TELNET. Como todas las aplicaciones de las capas superiores, el servidor usa un puerto conocido de TCP, es decir, escucha por el puerto 23 para aceptar las solicitudes de clientes TELNET.Mientras que cuando un cliente establece una conexión inicial con un servidor, el cliente utiliza un número de puerto de aleatorio asignado localmente.

En sistemas UNIX, el proceso servidor se conoce como "telnetd". El cliente (el extremo que está llamando) es un programa, llamado por lo general TELNET, que intenta la conexión con el servidor. Un pariente de TELNET es el programa "rlogin", común en máquinas UNIX
Cuando se establece una conexión, "telnetd" inicia un proceso en el servidor que usualmente es un proceso de "Iogin" y posteriormente un "shell".

Si el anfitrión y la máquina remota utilizan una interfaz gráfica como X o "Motif", los sistemas se deberán instruir para permitir el paso de información en ventanas de un lado al otro, de lo contrario, la máquina remota intentará abrir las ventanas en el servidor. Cuando el usuario sale de una sesión de red, TELNET cierra la conexión TCP.

En la mayoría de las implantaciones, el servidor de TELNET es un servidor concurrente; es decir, acepta múltiples conexiones a la vez. El hecho de que estas aplicaciones trabajen de manera cooperativa, permite que un cliente TELNET se pueda conectar con otros servidores que operan en otros puertos bien conocidos, como SMTP o HTTP.

TELNET debe ser capaz de solicitar aquélla información que tenga que ser enviada como información urgente de TCP y recibir notificaciones TCP urgentes de TELNET.

Opcionalmente, TELNET puede usar las capacidades de PUSH de TCP para indicar cuándo una información debe enviarse a su destino. Esto es útil si TCP intenta enviar segmentos de tamaño fijo y retarda la transmisión hasta que recibe suficiente

información para llenar un segmento. Debido a que las entradas de los usuarios son de diferente longitud y generalmente pequeñas, el PUSH de TCP se puede usar después de un <CR LF> para asegurarse de que la información del usuario se envíe inmediatamente.

2.15.1.7.- Negociación de Opciones de TELNET.

El Protocolo TELNET trata ambos extremos de la conexión como si fueran terminales virtuales de red. Los dos programas en cada extremo (TELNET y Telnetd) administran la conversión de la terminal virtual a los dispositivos físicos reales.

El concepto de terminales virtuales permite a TELNET interconectarse con cualquier tipo de dispositivo, siempre y cuando haya mapeo disponible de los códigos virtuales al dispositivo físico.

En TELNET las opciones son negociables, permitiéndosele al cliente y al servidor reconfigurar sus conexiones. Por ejemplo, en una conexión se mandan 7 bits de datos y utiliza bytes con el octavo bit activo para pasar la información de control, como el comando de interrupción de un proceso.

Sin embargo, TELNET tiene una opción que permite al cliente y al servidor pasar 8 bits de datos. El cliente y el servidor deben negociar y acordar el paso de datos de 8 bits antes de transferirlos.

Este proceso es sencillo: un extremo pregunta si se acepta una función y el otro extremo contesta positiva o negativamente. Si se acepta, se envían los códigos necesarios. De esta forma queda rápidamente cubierta la lista de funciones aceptadas por ambos extremos.

La cantidad de opciones de TELNET es grande: algunas son críticas mientras que otras negocian detalles pequeños. Por ejemplo, el protocolo original fue diseñado en un ambiente half-duplex en donde era necesario decirle al otro extremo “go ahead” antes de que enviara más datos. Una de las opciones controla la manera de operar de TELNET (Half dúplex o Full Dúplex). Otra opción le permite al servidor de la máquina remota determinar el tipo de terminal del usuario. Esto es importante para el software que genera las secuencias de control.

2.15.1.8 Operación de TELNET.

El programa TELNET es útil cuando usted está frente a una máquina de poca potencia o frente a una terminal y desea utilizar las capacidades de procesamiento de otra máquina, o si otra máquina tiene alguna herramienta en particular que usted no desea cargar en su máquina local.

Para iniciar TELNET, se debe proporcionar el nombre o dirección IP de la máquina a la cual desea conectarse. Solamente se puede utilizar el nombre, si el sistema tiene algún método para convertir el nombre a su dirección IP, como en el caso del Servicio de

Nombre de Dominio, DNS. También se puede especificar un número de puerto si el servidor “telnetd” no escucha en el puerto estándar.

Cuando se establezca la conexión, se solicitará identificación de usuario y contraseña. Una vez que se establezca con éxito la conexión, su sesión se comportará como si usted estuviera en la máquina remota, con todos los comandos válidos de dicho sistema operativo. Todas las instrucciones serán relativas al servidor, por lo que un comando de directorio mostrará el directorio de trabajo del servidor, no el del cliente. Para ver el directorio del cliente, tendrá que entrar en modo de comando. Para terminar la sesión remota, simplemente emita el comando de salida, y regresará a su máquina local.

2.15.1.9.- Comandos del Protocolo TELNET.

Cuando se establece una sesión TELNET se dispone de varias opciones de servicio. Durante el curso de una sesión TELNET sus valores se pueden modificar, siempre que ambos extremos estén de acuerdo (un extremo puede estar impedido para habilitar o deshabilitar un servicio por decisión del administrador o de ajuste de recursos).

El Protocolo TELNET utiliza cuatro verbos para ofrecer, rehusar, solicitar o evitar servicios: will, won’t, do, y don’t, respectivamente. Estos verbos se diseñaron para funcionar por pares. La siguiente sesión TELNET, tiene activo el despliegue de estos verbos mediante el uso del comando “Toggle Options” de TELNET:

```
tpci_server-1> telnet                (Se entra a modo de comando)
telnet toggle options                (Se habilita el despliegue de opciones)
Will show option processing.
telnet> open tpci_hpws4              (Se intenta una conexión)
Trying...
Connected to tpci_hpws4.
Escape character is '^ ]'.
SENT do SUPPRESS GO AHEAD       (Se negocian condiciones de trabajo)
SENT will TERMINAL TYPE (don't reply)
SEND will NAWS (don't reply)
RCVD do 36 (reply)
sent wont 36 (don't reply)
RECD do TERMINAL TYPE (don't reply)
RCVD will SUPPRESS GO AHEAD (don't reply)
RCVD do NAWS (don't reply)
Sent suboption NAWS 0 80 (80) 0 37 (37)
Received suboption Terminal type - request to send.
RCVD will ECHO (reply)
SEND do ECHO (reply)
RCVD do ECHO (reply)
SENT wont ECHO (don't reply)
HP-UX tpci_hpws4 A.09.01 A 9000/720 (ttys2)          (inicia sesión)
login:
```

La siguiente tabla muestra un conjunto parcial de códigos de comandos TELNET. Hay otros códigos adicionales para funciones de impresión, como tabuladores horizontales y verticales alimentaciones de forma, pero por razones de brevedad, estos se omitieron de la tabla.

Códigos	Valor	Descripción
Abortar salida (AO)	245	Ejecuta el proceso hasta su terminación pero no envía salida
Está usted ahí (AYT)	246	Consulta el otro extremo para asegurarse de que una aplicación esté funcionando
Ruptura (BRK)	243	Envía la instrucción de la ruptura
Marca datos	242	Porción de datos de un Sync
Do	453	Solicita al otro extremo que ejecute o acuse recibo de lo que el otro extremo ejecute
Don´t	254	Demanda al otro extremo que deje de ejecutar o que confirme que el otro extremo ya no está ejecutando
Borrar carácter (EC)	247	Borra un carácter de flujo de salida
Borra línea (EL)	248	Borra una línea de flujo de salida
Adelante (GA)	249	Indica permiso para seguir adelante al utilizar comunicaciones de medio dúplex (sin eco)
Interpretar como comando (IAC)	255	Interpretar lo que sigue como si fuera un comando
Interrumpir proceso (IP)	244	Interrumpe, suspende, aborta o da por terminado el proceso
NOP	241	No operación
SB	250	Subnegociación de una opción
SE	240	Fin de la subnegociación
Hill	251	Instruye al otro extremo para que empiece a ejecutar o confirme que este extremo está ejecutando ahora
Won´t	252	Se rehúsa a ejecutar o rechazar la ejecución del otro extremo

Parte del conjunto de comandos TELNET incluye seis funciones terminales (IP, AO, AYT, EC, EL y GA) que son comunes en la mayor parte de las definiciones de terminal; y por tanto, están definidas formalmente en el estándar de TELNET.

Los comandos TELNET se envían en un paquete conocido como comando. Típicamente, el comando contendrá dos o tres bytes.

2.15.1.10 TN3270

Muchas macrocomputadoras utilizan EBCDIC, en tanto que la mayor parte de máquinas más pequeñas se apoyan en ASC2. Esto puede causar un problema al tratar de usar TELNET desde máquinas basadas en EBCDIC hacia máquinas basadas en ASC2, porque los códigos que se estén transfiriendo no serán precisos. A fin de corregir lo anterior, se creó una aplicación TELNET conocida como TN3270, que proporciona la conversión entre ambos formatos.

Cuando se utiliza TN3270 para conectarse entre dos máquinas, TELNET mismo establece la conexión inicial, y a continuación uno de los extremos se ajusta para la conversión. Si una máquina ASC2 está llamando a una máquina EBCDIC, la conversión entre ambos formatos se realiza en el extremo EBCDIC (servidor), a menos que entre ambos exista una compuerta, en cuyo caso dicha compuerta puede llevar a cabo la conversión. TELNET ofrece el servicio de "Iogin" remoto. Permite que un usuario interactivo de un sistema cliente inicie una sesión en un sistema remoto. Una vez que la conexión se ha establecido, el proceso cliente pasa los golpes del teclado del usuario al proceso servidor. Al igual que FTP, TELNET usa TCP. El estándar de TELNET se encuentra en el RFC 854. [Postel y Reynolds, 1983].

2.15.1.11 Protocolos de Terminal Virtual.

El estándar TELNET se basa en la idea de una terminal de red virtual NVT ("Network Virlual Termina/'). El término "virtual" se usa por que NVT no existe físicamente, es un dispositivo imaginario que representa las características de una terminal. La idea es liberar a los "hosts" de la carga de tener que mantener las características de todas las terminales con las que se tiene que comunicar. Con TELNET, tanto el dispositivo del usuario como el del servidor tienen que mapear las características de sus terminales a la descripción de lo que es una NVT.

Un Protocolo de Terminal Virtual ofrece un lenguaje común para ser usado en una conexión mediante la definición de una terminal virtual y un protocolo para transferir información y controlaria a través de la red. La implantación del protocolo de terminal virtual de lenguaje nativo hace la traducción a lenguaje NVT para realizar la transmisión al otro lado de la conexión. La implantación receptora del protocolo NVT traduce entonces de lenguaje NVT a lenguaje nativo.

2.16.- Sistemas de Nombres de Dominios ("Domain Name System", DNS).

Los primeros sistemas de computadoras forzaban a los usuarios a utilizar direcciones numéricas que identificaban cada "hostil en una red. Actualmente el servicio de nombres de dominio permite que los usuarios manejen nombres simbólicos y significativos.

Este es sólo un servicio para hacer la utilización de la red más amigable. Las computadoras funcionan perfectamente usando direcciones IP, sin embargo, la gente prefiere estos nombres simbólicos ya que son fáciles de recordar. Inicialmente el conjunto de nombres simbólicos era plano, pero conforme las redes crecieron se tuvo la necesidad de implementar otro tipo de esquemas, como el servidor SINO de Internet.

El servidor SINO ("Berkeley Internet Name Domain", permite crear y mantener una base de datos distribuida de nombres de "hosts" y direcciones de computadoras en una red. Por "default" un sistema UNIX se configura para usar el archivo /etc/hosts. Sin embargo, si se tiene una red muy grande, actualizar este archivo en cada computadora puede consumir mucho tiempo. Usando BIND, el administrador del sistema no tendrá que actualizar el archivo de "host" en cada máquina.

2.16.1.- El Servidor de Nombres.

La función básica del servidor de nombres es atender las consultas de clientes relativas a nombres y direcciones de “hostil. Con el servidor de nombres, la red es dividida en jerarquías de dominios. El espacio de nombres es organizado como un árbol, de acuerdo con las características de las organizaciones o administrativas. Cada nodo, llamado un dominio, tiene una etiqueta. El nombre de un dominio esta dado por la concatenación de todas las etiquetas de los dominios desde la raíz hasta el dominio referido, listados de derecha a izquierda, separados por puntos. Cada etiqueta es única en el dominio. Todo el espacio es dividido en áreas llamadas zonas, cada zona generalmente se asocia con un área administrativa. Un ejemplo de nombre de un “hosts” en la empresa ACME, es: servidor. acme. com

El dominio superior para organizaciones comerciales es COM; Acme es un subdominio de COM y servidor es el nombre del “host”. Los dominios superiores para otros tipos de organizaciones establecidos por el NIC de Internet son: EDU (organizaciones educacionales), GOB (organizaciones gubernamentales), MIL (departamentos militares), ORG (organizaciones misceláneas).

2.16.1.1.- Tipos de Servidores.

Existen varios tipos de servidores. Estos son:

- Servidores maestros.
- Servidores de almacenamiento temporal.
- Servidores remotos.
- Servidores esclavos.

Un Servidor Maestro de un Dominio es la autoridad en ese dominio. Este servidor mantiene todos los datos correspondientes a este dominio. Cada dominio deberá tener por lo menos dos servidores maestros: un maestro primario, y uno o más secundarios para respaldar el servicio si el primero no esta disponible o esta sobrecargado. Un servidor puede ser un maestro para múltiples dominios, siendo primario para algunos y secundario para otros.

Un Servidor Maestro Primario es aquel que carga la base de datos desde un archivo en disco. Este servidor puede delegar autoridad a otros servidores de su dominio.

Un Servidor Maestro Secundario es un servidor al que le es delegada autoridad y recibe datos para un dominio desde un servidor maestro primario. Durante el arranque, el servidor secundario solicita todos los datos de la zona al servidor maestro primario. Este servidor verifica periódicamente con el servidor primario para verificar si se requiere actualizar los datos.

Todas las solicitudes son redirigidas en su totalidad hacia un servidor de nombres de otra maquina. Un servidor remoto es una opción para quienes les gustaría tener el servicio de nombres en su sistema pero no tienen los recursos para hacerlo, por lo que se apoyan en el servidor de nombres de otro equipo, por ejemplo una computadora

personal corriendo MS-DOS o Windows 95, este tipo de servicio también se conoce como resolvedor.

Un servidor esclavo es un servidor que siempre envía las consultas que no puede resolver localmente hacia una lista de servidores que si lo pueden hacer, denominados "forwarders", en lugar de interactuar con los servidores de nombres maestros, para el dominio raíz y otros. Las consultas hacia los servidores "forwarders" son recursivas. Es decir se intentan en el orden especificado hasta que la lista es agotada.

Bajo este esquema varios "hosts" podrían correr un servidor esclavo de otro servidor de nombres en un "host" más poderoso con acceso total a Internet, ese "host" desarrollaría un caché mucho mas completo, agilizando las consultas mas frecuentes de toda el área.

2.16.1.2.- Resolución de Nombres.

Los servidores de nombres obtienen información acerca del espacio de nombres de un dominio. Debido a la limitada inteligencia de algunos resolvedores, los servidores de nombres no solo pueden brindar información acerca de la zona para la que son autoridad, sino también para otros dominios, este proceso se conoce como resolución.

Debido a que el espacio de nombres esta estructurado como un árbol invertido, un servidor de nombres necesita un solo dato para determinar el punto de entrada dentro de este árbol hacia su objetivo: los nombres y direcciones de los servidores de nombres del dominio raíz. Un servidor de nombres puede consultar a un servidor raíz acerca de cualquier dominio dentro del árbol y el servidor raíz lo conducirá en su búsqueda.

2.16.1.3 Servidores del Dominio Raíz.

Los servidores del dominio raíz saben que servidores son la autoridad para todos los dominios del nivel más alto. (De hecho los servidores del dominio raíz son autoridades para el dominio de nivel más alto en los Estados Unidos).

Dada una consulta acerca de cualquier nombre de dominio, los servidores raíz pueden cuando menos proveer los nombres y direcciones de los servidores autoridades para el dominio de nivel más alto al que pertenece el dominio consultado. Yesos servidores de nombres de nivel más alto pueden proveer la lista de los servidores autoridades para el dominio del segundo nivel al que pertenece el dominio consultado. Cada servidor de nombre consultado proporciona al cliente que inicio la consulta información de como llegar cada vez mas cerca hacia el dominio que esta buscando o le provee esta respuesta en caso de conocerla.

Los servidores de nombres raíz son muy importantes para la resolución, por esto el DNS provee mecanismos como el "caché" para reducir la carga de estos servidores raíz. Pero en ausencia de otra información la resolución tiene que empezar con los servidores raíz esto hace que estos servidores sean cruciales para el DNS, ya que si todos ellos estuvieran ocupados por un periodo prolongado el proceso de resolución en toda la Internet fallaría.

Para proteger contra esto Internet tiene varios servidores raíz diseminados en distintas partes de la red. Algunos pertenecen a MILNET, uno en la NASA, uno en Europa y otros en el “Backbone” de NSFNET. Al ser el punto focal para muchas consultas estos servidores raíz se mantienen muy ocupados recibiendo 20 000 consultas por hora. Si embargo el proceso de resolución funciona muy bien en la Internet, en este proceso de resolución para la dirección de un “host” real en un dominio real se hace a través del árbol del espacio de dominio de nombres.

2.16.1.4 Iteración y Recursión

Existen dos tipos de consultas: recursivas e iterativas. En el proceso recursivo mucho del trabajo recae en un solo servidor, inicialmente el resolvedor envía una consulta recursiva a un servidor de nombres acerca de un dominio particular. El servidor de nombres consultado esta entonces obligado a responder esta consulta o a enviar un mensaje de error si el dominio no existe.

Este servidor de nombres no puede transferir al cliente hacia otro servidor ya que la consulta es recursiva. Si el servidor consultado no es la autoridad para los datos solicitados tendrá que consultar a otros servidores de nivel mas bajo, por lo tanto los obliga a encontrar la respuesta y regresársela (es decir les pasa “la bolita”). Este proceso se repite hasta encontrar la respuesta o hasta que sea imposible continuar la búsqueda recursiva.

En una consulta iterativa un cliente que consulta a un servidor de nombres, es transferido hacia otro servidor más cercano (dentro del árbol) al dominio buscado, si este no conoce la respuesta a la solicitud del cliente, el servidor dará su mejor respuesta, apoyado únicamente en la base de datos local (incluyendo su “caché’), ya que este no realizará ninguna consulta adicional.

Este proceso se repite, ayudando al cliente a redirigirlo hacia otros servidores de nombres más cercanos hacia los datos buscados. Usualmente en un sistema UNIX, el resolvedor consulta al servidor de nombres local mediante una consulta recursiva, este a su vez consulta a otros servidores de nombres en búsqueda de la respuesta para el resolvedor, mediante una consulta iterativa. Cada servidor de nombres que consulta lo redirige hacia otros de nivel inferior en el espacio de nombres y por lo tanto más cercanos hacia el objetivo.

Finalmente, el servidor de nombres local consulta al servidor de nombres autoridad del dominio buscado, el cual regresa la respuesta. Este a su vez responde al resolvedor.

2.16.1.5 El Caché DNS.

Un servidor de nombres que procesa una consulta recursiva puede requerir realizar otras consultas para encontrar la respuesta. Sin embargo este descubre que mucha de la información acerca del espacio de nombres de dominio se repite continuamente. Cada vez que es transferido hacia otros servidores, aprende que estos servidores de nombres son autoridades para una zona específica y también aprende su dirección.

Al final del proceso de resolución puede almacenar toda esta información para agilizar una futura referencia a esta los servidores de nombres guardan en un archivo de caché todos los datos para agilizar las consultas sucesivas, la próxima vez que un resolvedor consulta al servidor de nombres acerca de algún dominio el proceso es agilizado al consultar primero el caché local, si esta información se encuentra ahí no se tiene que realizar ninguna consulta posterior y por lo tanto no se es tan dependiente de otros servidores como los del dominio raíz.

2.17.- Protocolo de Transferencia de Correo Simple ("Simple Mail Transfer protocol, SMTP).

SMTP proporciona un protocolo para el intercambio de correo entre dos sistemas usando una conexión TCP. La definición de SMTP se encuentra en el RFC 821. [Postel, 1982]. El estándar para el formato de los mensajes de correo se encuentra en el RFC 822. [Crocker, 1982], el RFC 974. [Patridge, 1986] especifica la manera de enrutar el e-mail.

El correo electrónico, además se conoce como un sistema de mensajes basado en una computadora ("Computer Based Message System", CBMS), es un mecanismo que les permite a los usuarios de las terminales crear e intercambiar mensajes. A menos que el usuario (receptor o transmisor) desee una copia impresa del mensaje, todo se realiza de manera electrónica. Algunos sistemas de correo electrónico sólo sirven para los usuarios de una sola computadora, la mayoría permiten el intercambio de mensajes en una red de computadoras.

2.17.1 Funcionamiento.

Aunque los mensajes transferidos por SMTP usualmente siguen el formato definido en el RFC 822, a SMTP no le importa el formato o contenido del mensaje. Esta idea se expresa con frecuencia diciendo que SMTP usa la información escrita sobre el "sobre" del correo, no mira adentro.

Solo hay dos excepciones: SMTP estandariza el conjunto de caracteres del mensaje como ASC2 de 7 bits y le antepone a los mensajes entregados la información de registro que contiene la ruta que el mensaje siguió.

El correo es creado por el programa del usuario y se coloca en una cola de correo listo para salir junto con los otros mensajes de este usuario y del "host" local. La cola se atiende por un transmisor.

SMTP, el cual es típicamente un proceso presente del servidor en el "host".
El transmisor SMTP toma los mensajes de la cola y les transmite al "host" destino apropiado, vía transacciones SMTP sobre una o varias conexiones de TCP en el puerto 25.

Un "host" debe tener múltiples transmisores SMTP activos simultáneamente cuando tiene un volumen grande de correo listo para salir, además, debe tener la capacidad de

crear receptores SMTP, dependiendo del tamaño de la demanda, con la finalidad de no retardar el correo de los demás usuarios.

La entrada que requiere un transmisor SMTP se encuentra en la cola del correo lista para salir. Aunque la estructura de esta cola varía dependiendo del sistema operativo del “host”, cada mensaje de la cola conceptualmente tiene dos partes: El texto del mensaje y Una lista de destinatarios.

El texto del mensaje incluye el encabezado especificado por el RFC 822 y el cuerpo del mensaje creado por el usuario. El transmisor SMTP busca la información en la cola y abre una conexión TCP para entregar el correo. Siempre que el transmisor SMTP esté listo para completar la entrega de un mensaje en particular a uno o varios usuarios de un “host”, borra los destinatarios correspondientes de la lista de mensajes. Cuando todos los destinatarios de un mensaje son procesados, el texto del mensaje y la lista de destinatarios de ese mensaje se borra de la cola. El transmisor SMTP puede realizar diversas optimizaciones. Si un mensaje es enviado a usuarios múltiples de un “host”, el texto del mensaje se envía una sola vez. El transmisor SMTP puede además transferir múltiples mensajes sobre una sola conexión TCP.

El transmisor SMTP debe ser capaz de responder a varios errores. El “host” destino puede estar fuera de su alcance, apagado, o la conexión TCP puede fallar mientras que el correo se está transfiriendo. El transmisor debe volver a poner el mensaje en la cola para entregarlo mas tarde. Esta es una política a criterio del administrador del sistema, pero generalmente el transmisor seguirá intentando entregarlo por varios días.

Otra serie de errores ocurren con las direcciones destino erróneas o cuando el destinatario se ha mudado a otro sistema. El transmisor SMTP debe enfrentarse a estos problemas y enviar el mensaje o regresar un mensaje de error al remitente del mensaje.

El protocolo SMTP ofrece una operación confiable, pero no garantiza la recuperación de los archivos que el “host” pierda. Cuando un mensaje se entrega exitosamente no se le entrega ningún acuse de recibo al destinatario y no se garantiza la entrega. Sin embargo, el sistema de correo es lo suficientemente confiable como para que esto no sea un motivo de alarma.

El receptor SMTP acepta los mensajes recién llegados y los coloca en los buzones apropiados de los usuarios o los opia a la ola locas de correo. Para hacer este trabajo, el receptor SMTP verifica los destinos del correo local relacionados con los problemas de transmisión, la escasez de espacio en disco, etcétera. La estrategia general es que el transmisor indiqué cuándo ha finalizado la transferencia. Así, el transmisor es que mayor responsabilidad tiene sobre la recuperación de errores o los errores ocurridos durante la transmisión cuando éstos causan duplicación y no la pérdida de mensajes. Los mecanismos de recuperación de errores del receptor están sujetos a los de las conexiones TCP.

En la mayoría de los casos, los mensajes viajan directamente del remitente al destinatario. Ocasionalmente el correo pasa primero por sistemas intermedios. Una forma de que esto suceda, es cuando el transmisor especifica una ruta destino en la que existe una serie de servidores.

2.17.2 Protocolo de Oficina Postal (“Postal Office Protocol”, POP3)

En ciertos tipos de nodos pequeños en Internet es impráctico mantener un Sistema de Transporte de Mensajes (MTS). Por ejemplo, una “Workstation” puede no tener suficientes recursos para permitir un servidor SMTP y un sistema asociado de entrega de correo local, residente y que este corriendo en forma continua. Similarmente, puede ser caro (o incosteable) mantener una computadora personal interconectada a una red con arquitectura TCP/P durante un periodo largo (esto es que el nodo carece de conectividad).

A pesar de estas restricciones, algunas estaciones si pueden recibir correo, ya que algunas de estas soportan un agente de usuario (UA) que puede interaccionar con un servidor de correo.

Bajo este esquema, un nodo que puede soportar un sistema MTS, ofrece el servicio de “Oficina Postal” a los otros nodos. El Protocolo POP (“Postal Office Protocol”) Versión 3, conocido como POP3, fue diseñado para permitir a una estación de trabajo acceder dinámicamente un buzón en un “host” servidor.

Usualmente, esto significa que el POP3 permite a una estación de trabajo leer correo desde un buzón que el servidor de correo administra. Este servidor recibe el correo dirigido a cierto usuario y lo deposita en su buzón, en espera de que este sea leído. Haciendo uso de la terminología de la arquitectura c1ienteservidor, el término “cliente” se refiere a una estación que hace uso del servicio POP3, mientras que el término “servidor” se refiere a un “host” que ofrece el servicio de POP3 a esa estación. En este documento no se especifica como un cliente deposita correo en el sistema MTS. Cuando el agente usuario en un cliente desea introducir un mensaje en el sistema de transporte, establece una conexión SMTP con un “host” capaz de inviar correo. Este “host” podría ser, pero no necesariamente, el “host” que correo1 servidor POP3.

2.17.2.1. Operación Básica.

Inicialmente, el “host” servidor inicia el servicio POP3 que utiliza el puerto TCP 110 oara esperar solicitudes de conexión. Cuando un cliente desea hacer uso del servicio, establece una conexión TCP con el “host” servidor. Una vez que la conexión se ha establecido, el servidor POP3 envía un saludo. A continuación, el cliente y el servidor POP3 intercambian comandos y respuestas respectivamente hasta que la conexión es cerrada o abortada.

Los comandos de POP3 consisten de una palabra clave, posiblemente seguida de uno o más argumentos. Todos los comandos son terminados por el par CRLF. Las palabras clave y los argumentos consisten de caracteres ASC2 imprimibles y están separados por un solo carácter de espacio. Las palabras clave constan de tres o cuatro caracteres y cada argumento puede tener hasta 40 caracteres de longitud.

Las respuestas de POP3 consisten de un indicador de status y una palabra clave posiblemente seguida de información adicional. Todas las respuestas son terminodos por un el par CRLF. Actualmente existen dos indicadores de estatus: positivo (“+OK”) y negativo (“-ERR”).

Las respuestas a ciertos comandos son multilínea. En estos casos, que son mencionados posteriormente, después de enviar la primera línea de la respuesta y un CRLF, se envía cualquier línea adicional, cada una terminada por un par CRLF. Cuando todas las líneas de la respuesta han sido enviadas, se envía una línea final, que consiste de un byte de terminación (código decimal 046, u.") y un par CRLF. Por lo tanto una respuesta multilínea es terminada con 5 bytes ("CRLF.CRLF").

Cuando se examina una respuesta multilínea, el cliente checa cada línea para determinar si empieza con el byte de terminación. Si es así y si este es seguido por otros caracteres diferentes al par CRLF, entonces el primer byte de la línea (el punto) es ignorado. Si el par CRLF sigue inmediatamente al punto, entonces la respuesta del servidor POP3 ha terminado y la línea que contiene u. CRLF" no es considerada como parte de la respuesta multilínea.

Una sesión POP3 se lleva acabo a través de diferentes estados durante su tiempo de vida. Una vez que la conexión TCP ha sido abierta y el servidor POP3 ha enviado el saludo, la sesión entra al estado de AUTORIZACIÓN. En este estado, el cliente debe identificarse con el servidor POP3.

Una vez que el servidor ha validado su identificación, el servidor adquiere recursos asociados con el buzón del cliente y la sesión pasa al estado de TRANSACCIÓN. En este estado, el cliente solicita diversas acciones al servidor POP3.

Cuando el cliente emite el comando QUIT, la sesión entra al estado de ACTUALIZACIÓN (UPDATE). En este estado, el servidor POP3 libera cualquier recurso adquirido durante el estado de TRANSACCIÓN y envía un mensaje de despedida al cliente. Por último se cierra la conexión TCP.

Un servidor POP3 puede tener un "timer" para terminar automáticamente después de cierto tiempo de inactividad. Este "timer" debe ser de por lo menos de 10 minutos de duración. La recepción de cualquier comando del cliente durante este intervalo, es suficiente para reinicializar el "timer". Cuando el "timer" expira, la sesión no entra en el estado de UPDATE, el servidor cerrará la conexión TCP sin borrar los mensajes o mandar respuestas al cliente.

2.17.2.2.- El Estado de Autorización.

Una vez que la conexión TCP ha sido abierta por un cliente POP3, el servidor POP3 manda una línea de saludo. Esta puede ser cualquier cadena terminada con un CRLF. Un ejemplo podría ser:

S: +OK POP3 server ready

Este saludo es una respuesta del POP3 que siempre ira precedido de un estatus positivo.

La sesión POP3 esta ahora en el estado de AUTORIZACiÓN. El cliente debe entonces identificarse con el servidor POP3, mediante la combinación de los comandos USER y PASS.

El cliente debe primero emitir el comando USER seguido de un “Iogin-id” válido en el servidor. Si el servidor POP3 responde con un indicador de estatus positivo (“+OK’), entonces el cliente debe emitir el comando PASS seguido de la contraseña (“Password’) del usuario para completar la autenticación o el comando QUIT para terminar la sesión POP3.

Si el servidor POP3 responde con un indicador de estado negativo (“-ERR’) al comando USER, entonces el cliente debe emitir un nuevo comando de autenticación o puede emitir el comando QUIT. Cuando el cliente emite el comando PASS, el servidor POP3 usa el par de argumentos de los comandos USER y PASS para determinar si al cliente se le dará acceso al buzón apropiado.

Una vez que el servidor POP3 ha determinado que el cliente puede tener acceso al buzón apropiado, el servidor POP3 adquiere acceso exclusivo (“lock’) al buzón, esto es necesario para prevenir que los mensajes sean modificados o borrados (por otra sesión) antes de que la sesión entre en el estado UPDA TE. Si el acceso exclusivo es adquirido con éxito, el servidor POP3 responde con un indicador de estado positivo.

La sesión POP3 entra ahora en el estado de TRANSACCIÓN, sin mensajes marcados como borrados. Si el buzón no puede ser abierto por alguna razón (por ejemplo, un acceso exclusivo no puede ser adquirido, se le niega el acceso al cliente al buzón apropiado, o el contenido del buzón no puede ser interpretado), el servidor POP3 responde con un indicador de estatus negativo.

Después de regresar un indicador de estatus negativo, el servidor puede cerrar la conexión. Si el servidor no cierra la conexión, el cliente puede emitir un nuevo comando de autenticación y volver a empezar o el cliente puede emitir el comando QUIT.

Después de que el servidor ha abierto el buzón, este asigna un número a cada mensaje, y anota el tamaño en bytes de cada mensaje. Al primer mensaje en el buzón se le asigna el número 1, al segundo se le asigna 2, así hasta el n-esimo mensaje. En los comandos y respuestas de POP3, todos los números de mensajes y tamaños de mensajes son expresados en base 10 (es decir en decimal).

2.17.2.3 El Estado de Transacción.

Una vez que el cliente se ha identificado con éxito con el servidor POP3 y el servido POP3 ha abierto el buzón apropiado mediante un acceso exclusivo, la sesión POP3 esta ahora en el estado de TRANSACCIÓN.

El cliente puede ahora usar cualquiera de los comandos POP3 repetidamente. Después de cada comando, el servidor POP3 emite una respuesta. Eventualmente, el cliente emite el comando QUIT y la sesión POP3 entra en el estado UPDATE.

2.17.2.4.- Formato de los Mensajes.

Se asume que todos los mensajes transmitidos durante una sesión POP3 se ajustan al estándar de mensajes de texto Internet (RFC822).

Es importante notar que el tamaño en bytes de un mensaje en el “host” servidor puede diferir del contador de bytes asignado al mensaje debido a convenciones locales en la designación del fin de línea. Usualmente, durante el estado de AUTORIZACiÓN de la sesión POP3, el servidor POP3 puede calcular el tamaño de cada mensaje en bytes cuando este abre el buzón. Por ejemplo, si el “host” representa internamente el fin de línea como un solo carácter, entonces el servidor POP3 simplemente cuenta cada ocurrencia de este carácter en un mensaje como dos bytes. Notése que líneas en el mensaje que empiezan con el byte de terminación no son tomadas en cuenta, ya que el cliente POP3 eliminará todos los bytes de terminación cuando se reciba una respuesta multilínea.

2.17.2.5.- Consideraciones de Seguridad.

En algunos servidores POP3 el comando APOP sirve para autenticar la identificación y el origen del usuario en el cliente y da protección a una sesión POP3, mediante el mecanismo de cifrado de llave pública.

Esta característica es deseable ya que la contraseña de una sesión POP3 viaja como texto claro por la red, y puede ser interceptada mediante un “sniffer’. Un servidor POP3 que implementa tanto el comando APOP como el PASS, no debe permitir el uso de ambos métodos en el acceso de un usuario dado; esto es, para un nombre de usuario (USER Name) se puede permitir el PASS o el APOP pero no ambos.

2.18 Administración de Redes TCP/IP.

Los protocolos de administración de redes fueron desarrollados para permitir a los administradores manejar los dispositivos, dar seguimiento a los eventos críticos de la red y colectar información relacionada con las tendencias de crecimiento de las rutas de comunicación así como del desarrollo de la red y todo desde una estación de administración centralizada.

El primer protocolo de administración de redes no propietario que ha sido ampliamente aceptado fue desarrollado por la comunidad Internet para el uso del conjunto de protocolos TCP/lP. Inicialmente, se crearon para satisfacer necesidades básicas. Por ejemplo, para realizar el manejo centralizado del crecimiento local de direcciones IP asociadas a ruteadores en una red global Internet.

El grupo de estudio conocido como IETF (Internet Engieneering Task Force) fue asignado al problema del manejo de ruteadores Internet. Este grupo diseñó una plataforma de trabajo que vino a constituir la fundación del conjunto de protocolos de manejo Protocolo de Administración de Red Simple (Simple Network Management Protocol, SNMP).

Dos de los criterios más importantes, que son utilizados en los protocolos de manejo de red, y que son parte del diseño de la plataforma de trabajo SNMP, son:

- El protocolo no debe aumentar significativamente el tráfico en la red para satisfacer las necesidades de administración.

- El agente de protocolo, en el dispositivo de manejo, no debe disminuir las capacidades de operación básicas o primarias que deba satisfacer el dispositivo en el trabajo que tenga asignado. Un mínimo de ciclos de CPU y de memoria deben ser utilizados para propósitos de manejo o administración.

Lo anterior se observa en la figura 2.22

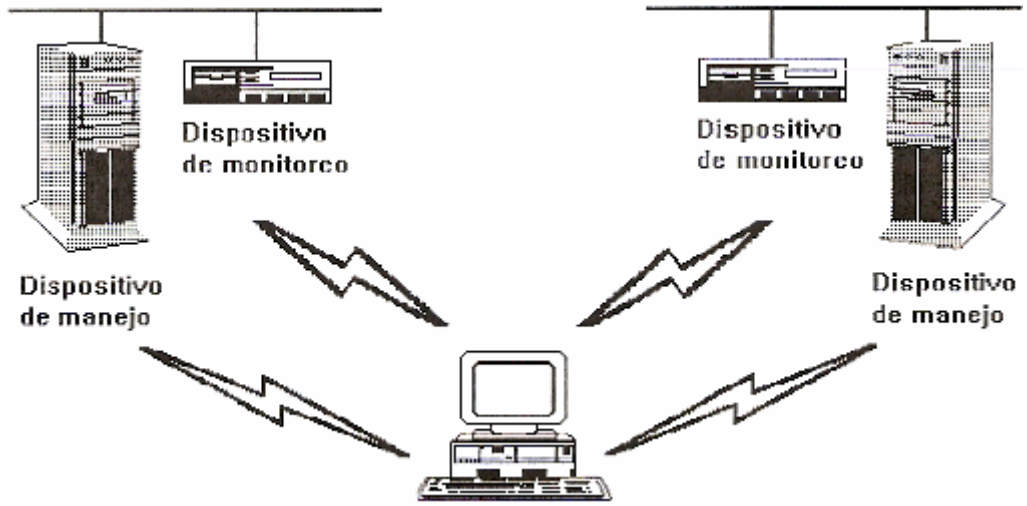


Figura 2.22 Organización y Administración

2.18.1 Agentes de Manejo

Un agente de manejo es una Base de Datos de información relacionada con un dispositivo y su ambiente de trabajo; estando este dispositivo instalado en el dispositivo de manejo o en el de monitoreo. Los datos contenidos en la base de datos del agente dependerán de las funciones del dispositivo. Por ejemplo, un ruteador puede contener información relacionada con su propia tabla de ruteo, el total de paquetes transmitidos y recibidos por el protocolo de capa de red, el número de los paquetes no validados e información variada, como lo muestra la figura 2.23.

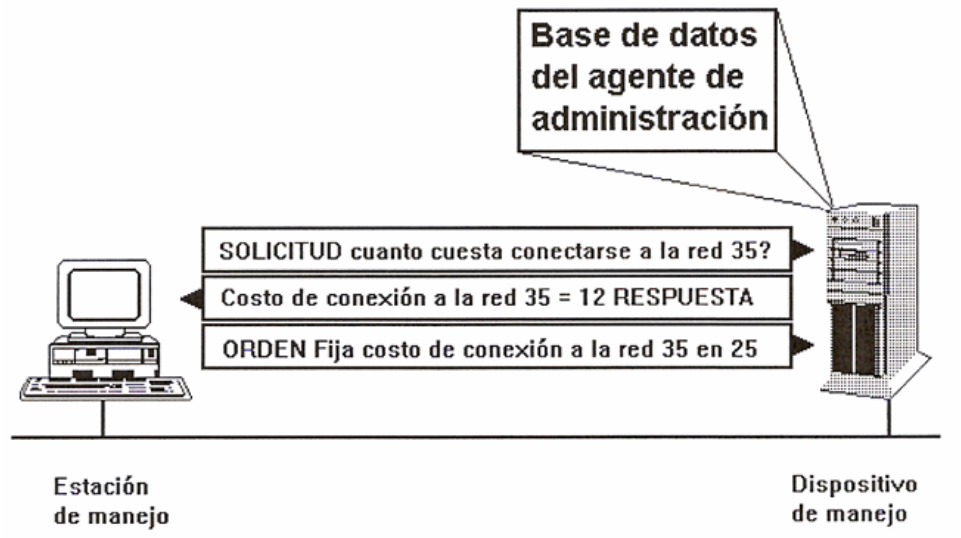


Figura 2.23 Agentes de Manejo

La estación de manejo realiza las siguientes solicitudes al agente en el dispositivo de manejo; estas solicitudes pueden ser de recuperación de información relacionada con el dispositivo, actualización o anexión de entradas en la base de datos o fijar un valor máximo a una variable crítica.

El agente en el dispositivo de manejo no ofrece información, porque lo podría alejar de su tarea específica y primaria. La única excepción a esta regla es que el agente podrá enviar una señal de alarma a la estación de manejo en el caso de que se sobrepase un valor de condición crítica.

2.19 Protocolo de Administración de Red Simple ("Simple Network Management Protocol". SNMP).

El Protocolo SNMP ("Simple Network Management Protocol') es actualmente una familia de especificaciones que provee un significado a la colecta de información de la red para el caso de la administración desde los mismos dispositivos de la red.
Este protocolo también provee un método, para los dispositivos, que les permite reportar problemas que se estén experimentando en el manejo de la estación.

Una estación de manejo SNMP realiza solicitudes - de poleo - al software para obtener datos de dispositivos en la red. La estación de manejo presenta los datos a la administración para que sean utilizados en el diagnóstico y el manejo del dispositivo.

Los protocolos de la familia de protocolos SNMP son: SMI (Structure and Identification of Management Information), MIB (Management Information Base), y SNMP (Simple Network Management Protocol)

2.19.1 Estructuración e Identificación.

La especificación SMI define la estructura de la base de datos del agente SNMP. Cuando se construye la base de datos, lo primero que debe hacerse es decidir la

estructura que deberá tener. La estructura define el número de campos de cada entrada así como su tamaño y el tipo de datos que podrá contener cada uno.

Por ejemplo, la estructura de la base de datos de unos libros de direcciones puede contener los campos:

Nombre	Dirección (Estado, C.P.)	Teléfono

Cada registro tendrá entonces seis campos, que son Nombre, Dirección, Estado, Código Postal y Teléfono. El último campo contendrá sólo números. Estos campos podrán visualizarse con una ficha de registro o en formato de tabla. SMI define la estructura de la base de datos del agente SNMP exactamente de la misma manera.

2.20.- Información de Manejo.

El Protocolo MIB describe los objetos, o las entradas, que deben ser incluidas en la base de datos del agente SNMP. Por esta razón, los agentes SNMP son referidos algunas veces como MIBs. Los objetos en un MIS deben estar definidos de la manera en que los desarrolladores del software de la estación conocen a disposición (los nombres de los objetos y sus valores correspondientes). Esta información se incluye en la especificación MIB.

Existen tres categorías de la especificación MIS: estándar, experimental, privado o de empresa.

- Estándar. Esta especificación incluye in conjunto común de objetos aceptados y ratificados por el grupo de estándares Internet. El primer estándar MIS que se dio a conocer constaba de 114 objetos, este fue mejorado posteriormente y presentando como MIS 11, conteniendo 172 objetos. La información que proveen estas especificaciones MIS está dirigida a ruteadores de manejo IP.

RMON (“Remote Monitoring’) MIS es actualmente en proceso de ratificación por la comunidad Internet para que constituya un estándar MIS. RMON posee funciones diferentes a MIS 11. Puede contener objetos para el monitoreo de los medios de transmisión de la red, como pueden ser los relacionados con la utilización de medio, el número total de paquetes transmitidos sin errores e información variada sobre este respecto.

RMON también puede utilizarse para realizar el monitoreo de dispositivos que no tienen un agente SNMP. Un dispositivo de monitoreo RMON es identificado como un cuasi agente del dispositivo sin agente.

- Experimental. Esta categoría incluye información específica relacionada con otros aspectos de la red y de los dispositivos de manejo considerada como de gran valía y que no existe en otros estándares MIB. Una vez que la especificación experimental de MIB sea refinada y llevada a niveles competitivos de eficiencia, será reclasificada como estándar.

- Privado (o de Empresa). Ésta se ha diseñado para uso individual de compañías que requieren colectar datos particulares de sus propios dispositivos de red. Permite que se definan objetos propios, que pueden ser específicos y no estar definidos en la categoría estándar.

2.21.- Protocolo SNMP.

El Protocolo SNMP ("Simple Network Management Protocol') fue diseñado para permitir la administración y manejo de la red a través del uso de una aplicación consola para realizar las solicitudes MIB de SNMP.

La estructura de manejo declara a un protocolo de manejo capaz (con un mínimo de sobrecarga en el nodo de manejo) de hacer la toma de datos de la estación y de la propia red, como lo muestra la figura 2.24

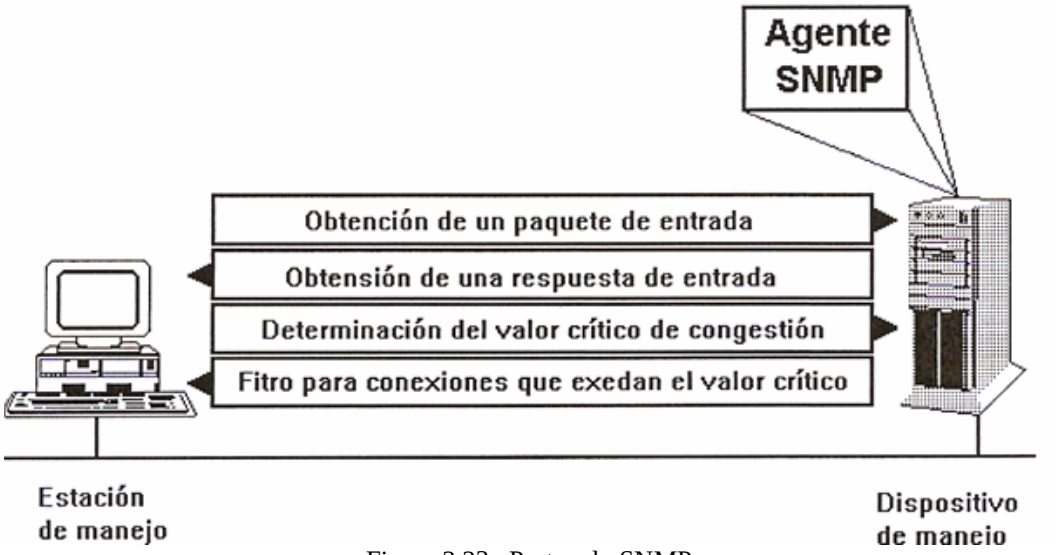


Figura 2.23 Protocolo SNMP

Lo anterior se completado constituyendo a SNMP como un protocolo cliente-servidor con únicamente cuatro operaciones:

- GET. Utilizado para recuperar un objeto simple en el MIB.
- GET-NEXT. Usado en tablas de transferencia (tablas transversas).
- SET. Se aplica para manipular información de administración.
- TRAP. Sirven para realizar reportes - alarmas - de eventos críticos.

SNMP fue diseñado específicamente para se un protocolo de transporte independiente. Lo que significa que las solicitudes de SNMP sobre los agentes pueden hacerse utilizando cualquier protocolo de transporte como TCP/IP, IPX/SPX, AppleTalk y cualquier otro.

2.22 SNMP II

El cuerpo de estándares de Internet ha ratificado a SNMP II. Este añade las siguientes características a la funcionalidad del protocolo SNMP:

- Seguridad mejorada
- Estación de comunicaciones con manejo interno (no sólo el manejo del agente).
- Operación GET-BULK. Actualmente, una base de datos como una tabla de ruteo debe ser recuperada entrada por entrada (registro a registro) utilizando el operador GET-NEXT. El operador GET-BULK permite hacer la solicitud de la tabla completa en un sólo tiempo.

CAPÍTULO 3:
FUNDAMENTOS DE LA TRANSMISIÓN DE VOZ SOBRE TECNOLOGÍA IP, (VoIP).

3.1 Voz sobre IP y Telefonía IP: Definición y Conceptos.

La Telefonía IP ("Internet Protocol Telephony") es un término general para designar las tecnologías que utilizan las conexiones "packet-switches" para intercambio de voz" fax y otras formas de información que tradicionalmente han sido llevadas sobre conexiones de circuitos de switcheo de la Red Telefónica Pública (PSTN).

Voz sobre IP (VoIP) especifica la transmisión de tráfico de voz en "paquetes IP", usando una red de transmisión de datos para telecomunicaciones.

En suma, el TCP/IP, la Telefonía sobre IP y VoIP usan el Protocolo de Tiempo Real (RTP o alguno similar) para asegurar que los "paquetes" de información son liberados en los tiempos adecuados.

Hay bastantes términos describiendo este proceso de comunicaciones; entre ellos está el Protocolo de Internet de Telefonía (IT Telephony) y Protocolo de Voz sobre IP. Usualmente estos términos son usados como sinónimos.

Los términos Voz sobre IP e IP para telefonía son usados para describir los diferentes servicios en tiempo real, tales como Voz, Video y Fax. Especialmente la Voz, la cual es manejada sobre Redes TCP/IP. Los Acrónimos más utilizados son:

- VoIP: Voz sobre IP.
- IPtel: Telefonía sobre IP.
- FoIP: Fax sobre IP.

3.1.1 Circuito de Datos.

El Circuito de datos es la transferencia de datos en un tipo de red en la cual una ruta física es obtenida para una simple conexión entre dos puntos finales en la red. Esta trayectoria se mantiene durante la conexión. Por ejemplo; el servicio de Voz en un teléfono. La Compañía Telefónica reserva una trayectoria física específica para el número al que se desea marcar por el periodo que dura la llamada. Durante ese tiempo nadie puede usar esa línea física.

Algunas redes semejante a la X.25 y ATM son capaces de direccionar circuitos virtuales. Una conexión de direccionamiento de circuito virtual es una conexión lógica dedicada que permite compartir la trayectoria física entre múltiples conexiones virtuales de circuitos, de tal forma que los datos son transmitidos en paquetes. Un circuito permanente virtual es una conexión lógica dedicada pero sus recursos físicos pueden ser compartidos por múltiples conexiones lógicas o por muchos usuarios. Esto se puede ver en la figura 3.1

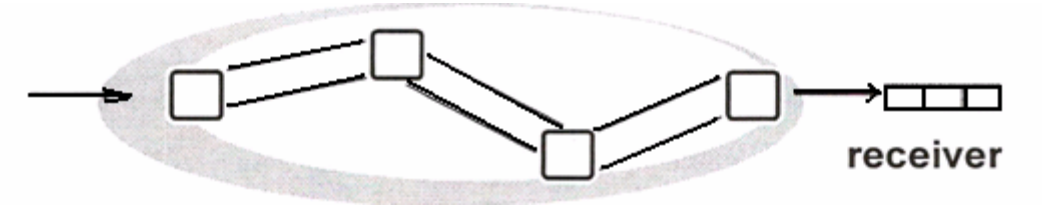


Figura 3.1 Circuito de datos

3.1.2 Datos Llevados por Paquetes.

La transferencia de datos en paquetes sobre una red describe el tipo de red en la cual se transmiten los datos, la llamada de paquetes son llevados hacia una red basada sobre direcciones destino, y en cada una esta contenida la dirección de cada paquete. Si hay una caída en la comunicación de los paquetes, la red permite establecer una trayectoria compartida por los usuarios en la red. Este tipo de comunicación entre quien envía y quien recibe, es conocida como conexión inalámbrica. Mucho tráfico (y no todo necesariamente) sobre Internet usa este proceso de direccionamiento de paquetes y en este caso, el Internet es básicamente una conexión de la red sin cables.

Cuando las llamadas de Voz usan la red de paquetes direccionados de Internet, cada final de la conversación es dividida en paquetes que son reacomodados en el otro extremo. Uno de los mayores problemas con esto es que el flujo de paquetes en el extremo de la recepción puede estar defasado.

Algunos paquetes se pueden perder, otros se pueden retrasar debido a las diferentes rutas o pueden llegar en un orden incorrecto.

Otro tipo común de red digital es la que usa el protocolo X.25, definida sobre una red de área amplia comercial. Los paquetes de IP pueden ser transportados sobre la red X.25. Ésta también puede soportar circuitos virtuales en la cual una conexión lógica se establece para dos partes sobre una base de comunicación dedicada con cierta duración. Un Circuito Permanente Virtual (PVC) reserva la ruta base y a la vez, es una alternativa para corporaciones con líneas arrendadas o contratadas. Un PVC es una conexión lógica dedicada, pero los recursos físicos actuales pueden ser dirigidos hacia múltiples conexiones lógicas de diferentes usuarios; esto se observa en la figura 3.2.

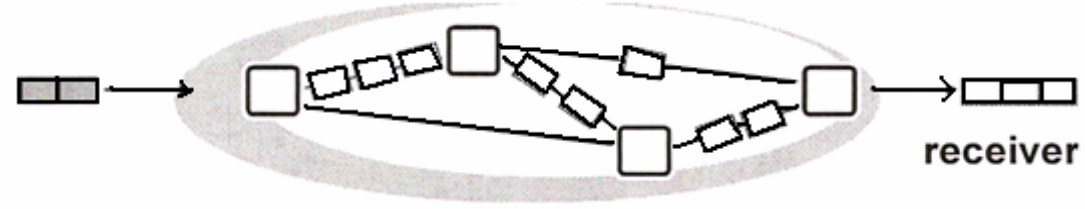


Figura 3.2 Envío de paquetes

3.1.3 Requerimientos de la telefonía IP

El uso de escenarios es lo que mantienen a los usuarios en el Internet Público, utilizando programas basados en telefonía IP en ordenadores personales comunicándose con terminales de telefonía ordinaria utilizando PSTN.

La Conectividad se ofrece por la Nueva Generación Telco ("Next Generation Telco'), Como en la nueva clase de telefonía basada en IP preferida para hacer llamadas telefónicas.

Interfaces y transductores entre dos redes permiten las comunicaciones.
Una interfaz de puertas ("Gateway') con direccionamiento y tareas administrativas también es requerida.

Cuando se usa telefonía IP o VoIP, se requieren terminales. Éstas pueden ser "Hardware" o "Software", normalmente conectadas a redes telefónicas públicas o privadas, y en algunos casos las puertas ("Gateways') son requeridas, o bien las terminales pueden ser conectadas directamente hacia la red IP. En este caso las terminales ya traen implementado un codificador y un decodificador con condiciones de direccionamiento.

En terminales basadas en sistemas de telefonía clásica, los datos son direccionados a través de circuitos con el VoIP y los datos son acomodados en pequeños paquetes, cada uno con su propia etiqueta de dirección asegurando una correcta entrega.

La telefonía IP tiene la capacidad de acomodar todas las posibles terminales con líneas existentes a través de puertas ("Gateways') tanto en telefonía tradicional como en telefonía inalámbrica (a través de la Norma IEEE 802.11, a través de tecnología para redes inalámbricas); o a través de programas de aplicación instalados en ordenadores personales.

La aplicación basada en computadoras personales (introducida por Vocaltec en 1995) a tenido un largo proceso de aceptación, pero ahora con las nuevas posibilidades para el manejo de multimedia, le ha permitido instalarse y resolver problemáticas diversas. Los paquetes y programas que actualmente se utilizan en la telefonía IP contiene funciones para codificar y decodificar información, direccionar rutas adecuadas y realizar funciones de multimedia, que permitan la optimización de los recursos. Por ejemplo se tiene el protocolo H.323 orientado al cliente; el cual esta soportado por el protocolo LDAP, ("Light Weight Directory Access Protocol"). La figura 3.3 muestra lo anterior.

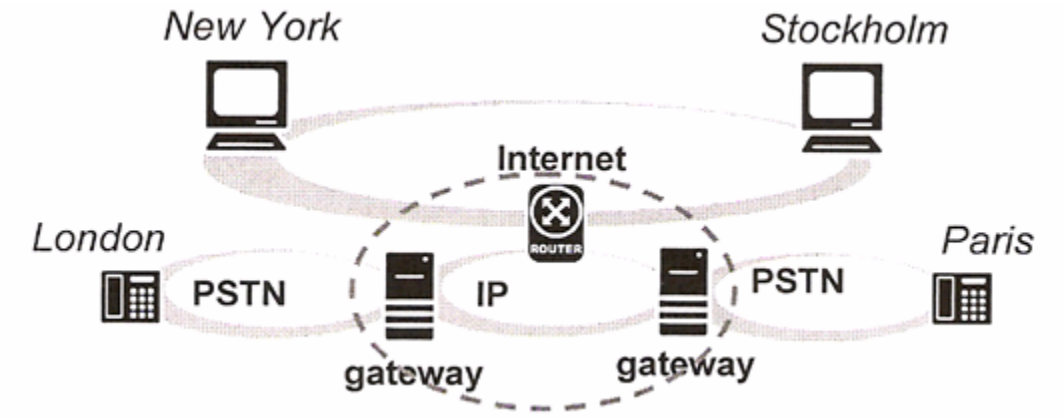


Figura 3.3 Requerimientos de Telefonía IP

3.1.4 Internet y TCP/IP.

Internet es pública, de cooperación, autodidácta y accesible a millones de personas en todo el mundo. Físicamente, Internet usa sólo una parte del total de recursos que existen en las redes de telecomunicación públicas. Técnicamente, lo que distingue a Internet es el uso de un juego de protocolos llamado TCP/IP ("Transmisión Control Protocol/Internet Protocol"). Uno de los mayores beneficios de Internet es la capacidad para tratar cualquier red como una simple "Nube" la cual esta compuesta a su vez por muchas redes. Hay muchas restricciones en esta simple aproximación, pero básicamente lo siguiente es cierto: una aplicación puede ignorar la complejidad de la red y concentrarse sólo en los negocios.

Internet tiene diversas aplicaciones disponibles como www y el correo electrónico. Usualmente el protocolo TCP/IP incluye otros protocolos como UDP, el cual es parte vital cuando se transmite VoIP.

TCP/IP toma a su cargo la complejidad de la aplicación y es capaz de operar aplicaciones en diferentes redes; por ejemplo, tanto en redes de área amplia como en redes de área local, utilizando una larga lista de diferentes medios de comunicación.

TCP ofrece un canal de transmisiones libre de errores para sus aplicaciones, teniendo un corrector de errores, un verificador de secuencia y retransmitiendo los paquetes perdidos; por lo tanto, TCP es uno de los más completos componentes de TCP/IP.

USD ("User Datagram Protocol'), es un método de comunicación que ofrece servicios cuando los mensajes son intercambiados entre ordenadores en una red que usa IP. UDP es una alternativa para el TCP. A diferencia de TCP, UDP no proporciona la posibilidad de dividir un mensaje en paquetes (Datagramas) y rehacer el paquete en el otro extremo. Específicamente, UDP no proporciona la posibilidad de que los paquetes de datos lleguen en secuencia, este servicio esta lejos de esta aplicación.

IP se concentra en el direccionamiento y selección de ruta a nivel de red. La red IP simplemente libera paquetes entre servidores de la red. Abajo la capa IP, está la capa física. VoIP usa ambos (TCP y UDP) en conexiones abiertas cuando la velocidad no es importante, mientras que cuando el flujo de datos se incrementa, éste utiliza UDP, como se muestra en la figura 3.4.

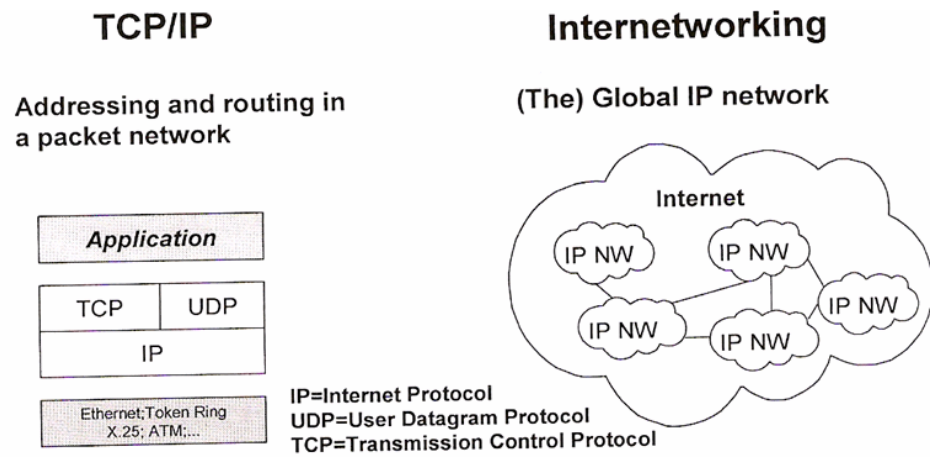


Figura 3.4 Internet y TCP/IP

3.1.5 Desarrollo de Internet y de PSTN.

Originalmente, Internet fue desarrollado para direccionar los recursos de los ordenadores. La aplicación que rápidamente se generalizó fue el correo electrónico. Hasta el arribo del servicio de www en 1993, el tráfico de información en Internet era relativamente bajo y los requerimientos de ancho de banda eran limitados. Pero, con la llegada de www los requerimientos de ancho de banda se incrementaron drásticamente. Imágenes, páginas Web Avanzadas, grandes archivos adjuntos y una gran cantidad de nuevos usuarios han dado como resultado una mayor expansión de Internet.

Pero tomará algunos años más poder transmitir voz, video y datos en redes con ancho de banda amplias, lo cual permitirá trabajar en tiempo real, con aplicaciones todavía inimaginables. Con el rápido desarrollo y uso de la telefonía móvil, los servicios de telecomunicaciones arrojan los siguientes datos:

- Más de 1,100 millones de líneas sobre PSTN
- Más de 200 millones de usuarios de Internet
- Más de 500 millones de suscriptores en telefonía móvil

Las nuevas comunicaciones requieren servicios de convergencia, y éstos son:

- Expandirse a la población de escasos recursos.
- Comunicar nuevas comunidades.
- Impactar el estilo y calidad de vida.
- Etcétera

3.1.6 Internet contra PSTN.

PSTN (“Public Switched Telephone Network”) se diseñó para trabajar los servicios de Voz en tiempo real y tiempos de espera bajos; mientras que Internet está diseñada para liberar servicio de transmisión de datos sobre redes, usando redundancia como el mejor recurso en ese formato.

La Telefonía IP es barata por muchas razones: es esencial en la comunicación de datos y esta ventaja la hace muy competitiva en el mercado, además:

- Los costos son bajos.
- No hay regulación de mercados formal.
- Gran competencia para ofrecer el servicio.

Técnicamente, la compresión en el proceso de decodificación hace que la eficiencia sea mayor al transmitir VoIP en comparación de Voz sobre redes de circuitos tradicionales. Entre esas ventajas se puede considerar:

- Red común para transmitir Voz y Datos.
- Asignación Dinámica.
- Compresión.

La figura 3.5 muestra una comparación entre el funcionamiento de PSTN y la Internet.

Internet vs. Public Switched Telephone Networks (PSTN)

	Internet	*PSTN*
Transport	packet	circuit
Voice service	developing	excellent
Data service	excellent	acceptable
Price model	bandwidth	time & distance
Cost model	fixed	regulated
User interface	GUI	black phone

Figura 3.5 Internet vs PSTN

3.1.7 Ventajas con Telefonía IP y Sistemas Abiertos.

Con Telefonía IP, la distancia usuario a usuario y entre usuarios y los operadores no es relevante. La red IP está expandiendo el planeta como la tecnología ha logrado expandir las oficinas; sin embargo, hay restricciones en ciertas políticas, accesos y capacidad.

El ordenador personal es generalmente mucho más versátil que un simple teléfono y generalmente, ofrece interfaces "amigables" para una gama de aplicaciones complejas. Sin embargo, es posible poder hablar con personas al igual que con las máquinas. Hasta ahora, una interfaz de servicio que permita "hablar" con el ordenador está restringido a cierta cantidad de palabras de uso frecuente.

La integración de aplicaciones que involucren comunicación de datos y telefonía se está simplificando al usar IP como una plataforma común en oposición al uso de CTI ("Computer Telephony Integration") el cual involucra protocolos y plataformas de los propietarios.

La red TCP/IP es verdaderamente un estándar o sistema abierto que alberga diversos protocolos. Usando protocolos y plataformas estándar se tiene un desarrollo rápido de aplicaciones y de fácil acceso a todos los niveles, ofreciendo soluciones competitivas.

Comparando el mercado de los ordenadores antes y después de que se instaurará el concepto de "estándar" o "abierto" en los sistemas operativos de los ordenadores personales respecto con la industria telefónica se tiene:

- La industria telefónica suministra todavía a sus clientes los productos en tiendas de formato tradicional y de mercado cautivo
- La industria de la computación ha abandonado el rol de venta tradicional "vertical" y se ha transformado en un nicho de venta horizontal, lo cual ha incrementado tanto la línea de productos como su propio mercado de ventas.

La industria de la telefonía IP ha adoptado un acercamiento en alto grado con los proveedores tanto con los que suministran los programas, como con los que comercializan los componentes de arquitectura y los que venden los sistemas.

3.1.8 Breve Historia de la Telefonía IP.

El llamado escenario de transmisión de voz en gran escala utilizando Internet como medio de transmisión entre ordenadores personales, fue desarrollado por la Compañía Israelí Vocaltec quien, en 1995, utilizó un programa de telefonía IP.

Recientes intentos con VoIP han podido demostrar en Laboratorios que la transmisión de VoIP es factible, tal como lo demostro la Compañía Vocaltec. Ahora se ha convertido en un producto comercial.

La introducción de compuertas ("Gateways") entre el PSTN e Internet fue siguiendo la idea de usar ordenadores como un teléfono y reactivar la suscripción de uso de la red de telefonía pública posteriormente.

La idea de usar una compuerta en ambos extremos de la conexión creo una nueva clase de operadores (conocido como Nueva Generación Telco u Operadores de Telefonía IP), estos operadores ofrecen servicios de telefonía utilizando una infraestructura de comunicación de datos que no utiliza la infraestructura de circuitos selectivos para su operación.

El paso para utilizar la red IP fue tomado con la introducción de los teléfonos basados en IP en 1998. Esos teléfonos IP llamados comercialmente PBX fue introducido por Ericsson y Nokia durante 1998 y 1999. Esta evolución se muestra en la figura 3.6.

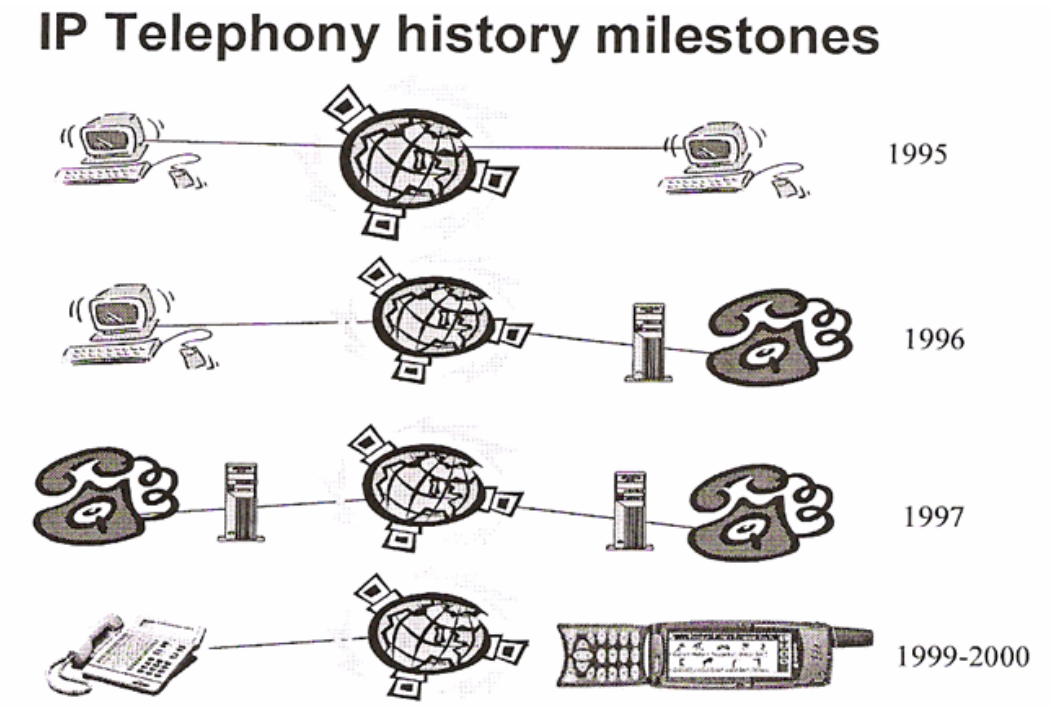


Figura 3.6 Historia de la telefonía

3.1.9 Perspectivas de la Industria.

La siguiente perspectiva está tomada de las presentaciones de dos magnates de las telecomunicaciones: Harry Newton y Bill Gates.

Para Harry Newton: "La telefonía IP en 1997 es a las telecomunicaciones lo que en 1981 significó para la industria de la computación, la introducción de la primer IBM PC".

Para Bill Gates: "La Voz y los Datos han estado siempre separados. Esto es limitan te. Los datos pueden agregar riqueza a la transmisión de voz y la voz puede dar riqueza a los datos. Brindando ambos enormes beneficios a la telefonía basada en la computación. En algunos años se podrá distinguir voz y datos por dispositivos de entrada y salida en redes que utilicen tecnologías más abiertas y transparentes".

3.1.10 Cómo Crecer en el Mercado.

La renta y los pronósticos para equipo de telefonía IP y sus servicios son modestos comparados con el mercado de comunicación de datos. En 1998 el mercado para los servicios y equipo utilizado en VoIP fue menor a un Billón de Dólares mientras que el servicio y equipo para la transmisión de datos fue 200 veces mayor a la anterior.

La Compañía IDC ("Internacional Data Corporation") pronostica que el mercado de telefonía IP llegará a 480 millones de dólares en renta para el año 1999 y 24 billones en el 2002, esto permitirá una tasa de crecimiento del 110%.

El pronóstico de la Empresa IDC en 5 años en el uso de voz de IP alrededor del mundo muestra incrementos sustanciales en la renta de equipos de la siguiente manera: el 1999 el mercado recibió ingresos de 290 millones de dólares, contra los 130 millones en 1998.

3.1.11 PSTN-by-Pass.

El PSTN-by pass, tambien conocido como "TolI by.pass" es hoy explotado por mas de 100 Companías telefónicas alrededor del mundo, complementando los servicios de teléfono a teléfono y los servicios de ordenador a teléfono, ofreciendo condiciones de operación óptimas. Continúan ofreciendo como campaña publicitaria el concepto "El minuto más barato" ofrecido a los consumidores por parte de las Compañías telefónicas. Las razones para comprar telefonía IP son:

- Funcionalidad.
- Infraestructura Simplificada.
- Soluciones de Red Virtual.
- Convergencia de Medios.

3.1.12 Desafíos para la Telefonía IP.

Un número de desafíos son inminentes para VoIP/Telefonía IP: el direccionamiento en un mundo de interoperatividad de redes en difícil. Existen normas, pero incompletas y todavía no bien establecidas, la Norma H.323 es la más utilizada en el mundo como el mejor protocolo.

La breve historia de la telefonía IP es una limitante cuando' quiere comparársele con la ya bien establecida tecnología utilizada en la telefonía tradicional. Las redes basadas en TCP/IP y las que incorporan "intranets" fueron originalmente diseñadas para optimizar la transmisión de datos de tal manera que garantizaran los requerimientos de calidad de servicio y prestaciones en tiempo real como Voz y Video durante las transmisiones.

3.1.13 Panorama de la Red.

Diferentes Compañías han acercado soluciones IP en diferentes formas. Algunas de ellas han decidido no invertir en tecnología obsoleta, ya que esas Compañías han decidido evitar problemas al utilizar ciertas plataformas operativas. Mientras que otras Compañías han hecho importantes inversiones en redes basadas en IP manteniendo la infraestructura existente. Sin embargo, incorporar tecnología existente con nueva tecnología puede ofrecer mayores dificultades, que los problemas que solucionará.

Muchas redes con costos de mantenimiento altos pueden ser un inconveniente en el proceso. Sin embargo, la obligación de invertir en infraestructura que pueda soportar los servicios basados en IP, permitirá crear servicios que puedan utilizar una mayor cantidad de opciones de comunicación sobre la red.

Sin embargo en la transmisión de voz, la principal obligación es resolver la problemática de comunicar PC-to-PC e IP con su centro de operación; ya que usan diferentes redes. La migración en las redes basadas en IP deben considerar los siguientes puntos:

- Incremento en los costos de mantenimiento.
- Problemas con la transparencia del servicio.
- Integración de resultados.

Los usuarios de IP pueden basar sus negocios sobre una red IP que proporcionan una gran capacidad de ancho de banda. La red es el núcleo de sus negocios y dentro de los servicios ofrecidos por las empresa prestadoras de servicio están: El acceso a Internet, los servidores de Internet, IP-VPN y por supuesto la telefonía IP.

3.1.14 VoIP y el Modelo OSI.

El Modelo de Referencia llamado Interconexión de Sistemas Abiertos (OSI) describe cómo se mueve la información en un ordenador desde cierta aplicación hasta otra aplicación en un ordenador diferente. El Modelo de Referencia OSI es un modelo conceptual compuesto de siete capas, cada una con una con una función específica y particular dentro de la Red.

El Modelo fue desarrollado por la Organización Internacional de Normas (ISO) en 1984 y se considera como el modelo primario de arquitectura para la comunicación entre ordenadores. El Modelo OSI divide las tareas involucradas con la información que se esta moviendo entre las máquinas a partir de sus siete capas.

Cada capa es autónoma, pero sus funciones pueden ser compartidas. La siguiente lista detalla las siete capas del Modelo OSI:

- Capa 7.- Capa de Aplicación.
- Capa 6.- Capa de Presentación.
- Capa 5.- Capa de Sesión.
- Capa 4.- Capa de Transporte.
- Capa 3.- Capa de Red.
- Capa 2.- Capa de Enlace.
- Capa 1.- Capa Física.

3.2 Calidad de Servicio en Redes de Telefonía IP, (QoS).

Tradicionalmente, el tráfico IP ha sido considerado como un "Gran Esfuerzo". La calidad de servicio de refiere a la capacidad de una red para proporcionar el mejor servicio que permita seleccionar el tráfico dentro de la red sobre diversas tecnologías incluyendo "Frame Relay", ATM Ethernet y Redes de Ruteo para IP. En particular QoS proporciona más y mejores servicios de red para:

- Soporte dedicado para gran ancho de banda.
- Incrementar las características de transmisión.
- Evitar congestiones en la red.
- Redireccionar el tráfico en la red.
- Poner prioridades durante el tráfico de información hacia la red.

La tendencia actual es la posibilidad de definir políticas de QoS sobre las diferentes capas desde la uno hasta la siete, que le permita operar en condiciones de gran flujo de información. Las diferentes funciones para QoS están implementadas en diferentes elementos de la red y QoS requerirá que todos los componentes estén enterados de dichas funciones.

El cliente debe ser capaz para decidir la clasificación de QoS según el tipo de desarrollo que se tenga para manejar el tráfico de información. El responsable de la Red debe ser capaz de definir las políticas utilizadas para diferentes tipos de tráfico, pero se debe diferenciar a los diferentes grupos de usuarios y dar prioridad a la Red de Área Local (LAN).

En el núcleo de la red, el tráfico debe ser manejado de la misma forma que en una LAN, la política de calidad necesita ser distribuida a todos los ruteadores y los ruteadores deben tener funciones de QoS integradas. Cada nivel de QoS tiene gran cantidad de soluciones y de protocolos los cuales está bien definidos por IETF ("Internet Engineering Task Force') y algunas otras organizaciones.

El RSVP ("Resource Reservation Protocol') es el Protocolo de Señalización para abanderar los requerimientos QoS de los diversos ruteadores en la Red. Dentro de cada ruteador, hacen fila mecanismos que toman la prioridad entre los diversos paquetes. RSVP permite aplicaciones con tráfico en tiempo real y reserva además, recursos de red necesarios para encontrar los requerimientos específicos de QoS.

La etiqueta de flujo y los campos de prioridad en el encabezado de IPv6 puede ser utilizado por los ruteadores de IPv6 para identificar paquetes que requieren un manejo especial por el ruteador. Un flujo es definido como los paquetes enviados desde una fuente a un destino particular. Un flujo puede por lo tanto, estar dado con una prioridad especial, semejante a las garantías de QoS.

3.2.1 Servicios diferenciados y MPLS.

Diffserv ("Differentiated Services') y MPLS ("Multiprotocol Label Switching') son dos estándares separados los cuales pretenden ayudar a resolver el problema de calidad de IP. Cuando se discute sobre los niveles de calidad es importante diferenciar entre QoS ("Quality of Service') y CoS ("Class of Service'). El concepto de CoS es absoluto y define niveles de calidad. El concepto CoS proporciona niveles relativos de calidad dependiendo de la red utilizada y de algunos otros parámetros.

DS ("Differentiated Services') es un Protocolo para especificar y controlar el tráfico de la red por "clase" en el entendido de que existe cierto tipo de tráfico, por ejemplo; el tráfico de voz.

"Diffserv" toma el campo del IP TOS ("Type of Service'); renombra éste con el byte DS y lo usa para acarrear información usando los requerimientos de servicio de los paquetes enviados por IP. Esto sucede en la capa 3, que se encarga de los servicios de la Red.

El DS acerca dos parámetros: Cualitativo y cuantitativo. El referente cualitativo especifica por ejemplo; prioridad relativa, mientras que el aspecto cuantitativo especifica por ejemplo, el ancho de banda. DS es el más avanzado método para manejar tráfico en términos, lo que es llamado Clase de Servicio.

A diferencia de mecanismos de la Norma 802.1 p que etiqueta el tipo de servicio (ToS), DS evita la simple etiquetación y depende de políticas que determinan cómo enviar hacia delante los paquetes de la red. Una vez clasificados los ruteadores, los paquetes pasan directamente hacia la ruta adecuada dependiendo de la información de prioridad que existe sobre el DS.

MPLS especifica caminos que la capa 3 puede "Mapear" para hacer una conexión orientada en la capa 2 semejante a lo que hace ATM y Frame Relayg. MPLS adiciona una etiqueta que contiene información de la ruta para cada paquete IP y permite a los ruteadores asignar rutas específicas entre varias clases de tráfico.

La tecnología MPLS también integra IP y ATM Y además proporciona soluciones para incrementar la velocidad y la prioridad de tráfico en el cable de la red. Esto requiere

inversión en nuevos ruteadores capaces de leer la información que tiene los encabezados de cada paquete y asignar rutas específicas para distribuir los datagramas.

3.3 Protocolo H.323

3.3.1 Las series ITU-T H.32x

La Unión Internacional de Telecomunicaciones (ITU) tiene un número de recomendaciones para las Series H como se muestra en la figura 3.7. La recomendación particular de la serie H para VoIP es: H.323.

La especificación H.323 fue aprobada el 1996 por la ITU (Grupo de Estudio No. 16). La versión dos fue aprobada en Enero de 1998; el estándar es extenso e incluye tanto equipos de cómputo personales como equipos multiusuario. H.323 también tiene un control de dirección de llamadas, manejo de multimedia y ancho de banda con interfaces que permiten conectar Redes de Área Local con Redes de otro tipo.

H.323 ha sido el estándar para la interoperabilidad entre diferentes productos en tiempo real para la comunicación sobre IP. La comunicación en tiempo real puede ser voz, vídeo, etcétera. Organizaciones como IBMTM, Intel™, Microsoft™, Netscape™ y Cisco™, forman parte del Comité H.323.

H.323 es un estándar que especifica los componentes, protocolos y procedimientos que proporcionan servicios de comunicación multimedia (audio en tiempo real, video y comunicación de datos), sobre paquetes en red, incluyendo IP basado en redes. H.323 es parte de las recomendaciones para la familia de ITU-T llamadas H.32x que proporciona servicios de comunicación multimedia en una gran variedad de redes. El estándar incluye componentes para activar, mantener y terminar una conexión de voz, video conferencia, etcétera. Nuevos componentes pueden ser fácilmente agregados a H.323; como algoritmos de compresión, etcétera.

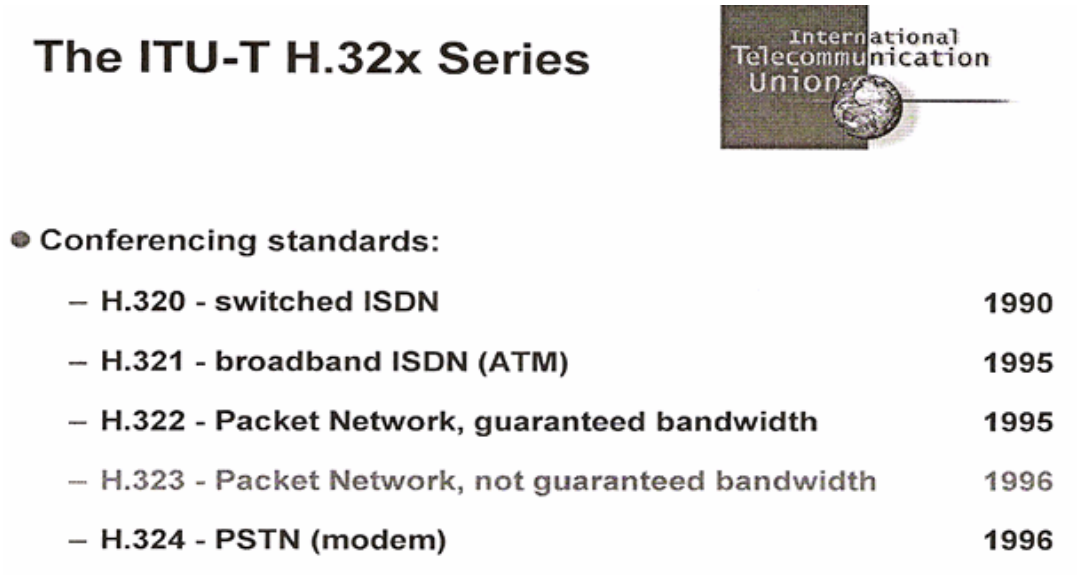


Figura 3.7 La serie IYU-T H.32x

3.3.2 Estructura Funcional del H.323.

Esta es una revisión de la estructura funcional del H.323 en una terminal del cliente. Los componentes para la interfaz de los medios son:

- Audio Codec para el micrófono/bocina .
- Video Codec para la cámara/unidad de video .
- Interfaz de datos para el equipo de datos.

Los componentes para el sistema y el control de interfaz son:

- H.245 (media channel signallin).
- Q.931 (call set-up and call release).
- Gatekeeper interfaz, RAS (Registration, Admission, Status).

H.323 proporciona un juego de códigos de audio y video. Algunos son obligatorios y otros no lo son.

El Protocolo de Tiempo Real (RTP) desde IETF es usado para llevar tráfico en tiempo real.

RTP suministra funciones de transporte en la red en ambos puntos de la conexión en tiempo real para transmitir datos como audio, video o simulación de datos sobre servicios de red para multiusuarios o usuarios únicos. RTP no es una fuente para reservar direcciones y no es garantía de calidad de servicio para aplicaciones en tiempo real. El transporte de datos es incrementado por un protocolo de control (RTCP) que permite verificar que la llegada de datos se realice de forma escalable en redes con distancias grandes, y tambien proporciona funciones de identificación y control. RTP y RTCP estan diseñados para ser independientes tanto de la capa de transporte como de la capa de red. La estructura funcional del H.323 se muestra en la figura 3.8

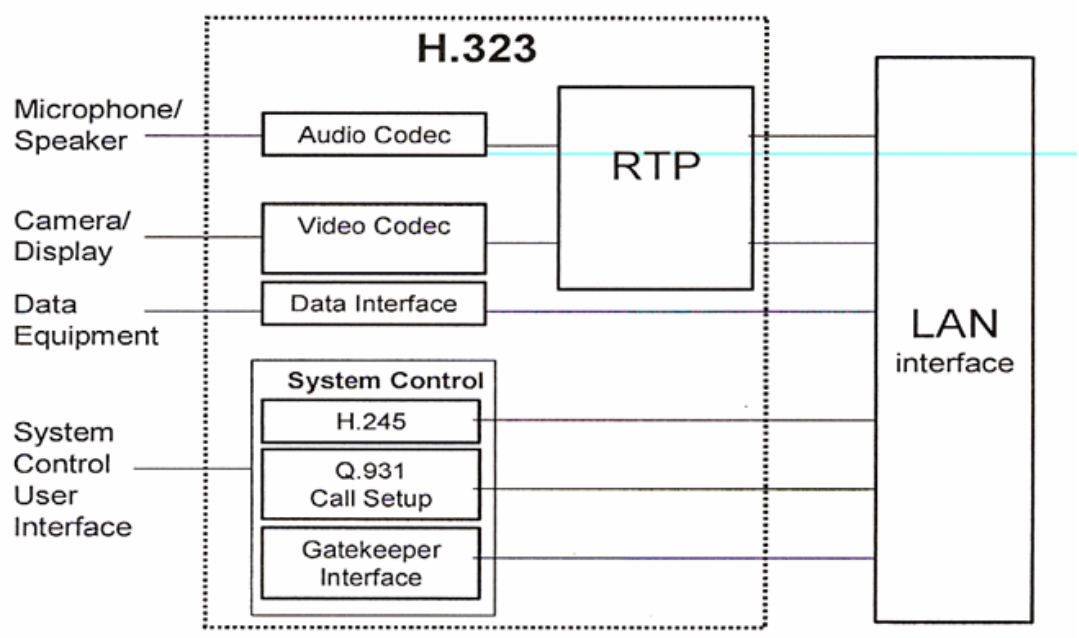


Figura 3.8 Estructura funcional del H.323

3.3.3 H.323 Diversos Estándares.

La comunicación manejada por H.323 es una mezcla de datos, voz y video que son controlados en una ruta específica. El control y señalización es el núcleo de la comunicación basada en H.323. Esas funciones proporcionan mecanismos para establecer, mantener y concluir la trayectoria de comunicación.

El control y señalización también decide cual es sub-norma de la comunicación deberá usarse.
De conformidad con el estándar H.323, un sistema puede implementar una llamada de control íntegra de señalización a través de G.711 (PCM) y el RTP y RTCP como protocolo de transporte. Sin embargo, algunas partes del H.323 no son obligatorias para todos los vendedores de productos y por lo tanto en estándar H.323 no se puede implementar completo y el vendedor podrá especificar sólo aquellas partes de esta norma que sí se cumplirán. Diferentes implementaciones del H.323 tienen dificultades en la comunicación con otros sistemas. Sin embargo existe un Foro de Iteroperatividad llamado TIPHON.

Los siguientes puntos son opcionales en H.323:

- Los estándares de audio G.723 y G.729 tienen una alta velocidad de compresión y pueden suministrar buena calidad sobre bajas velocidades de transmisión de bits.
- El estándar de video en H.323.
- El formato de transporte de datos en H.323.

El estándar T.120 contiene una serie de protocolos de comunicación y aplicación, además de servicios que proporcionan un soporte para tiempo real y comunicaciones de datos multipunto. Esas prestaciones multipunto están construyendo bloques para aplicaciones incluyendo el escritorio para conferencia de datos, aplicaciones y juegos para multiusuarios. Establecido por la ITU, T.120 es una familia de estándares abierto que fue definido para adelantar comunicación de datos en la industria. Dichos estándares son:

- T.122: Servicio de Comunicaciones Multipunto.
- T.123: Protocolos de Transporte para Diferentes Redes.
- T.124: Control de Conferencias Numérico.
- T.125: Servicio de Comunicaciones Multipunto.
- T.126: Imagen Inmóvil en Conexión Multipunto y Protocolo de Anotación.
- T.127: Multipoint Binary File Transfer Protocol

La figura 3.9 muestra estos estándares.

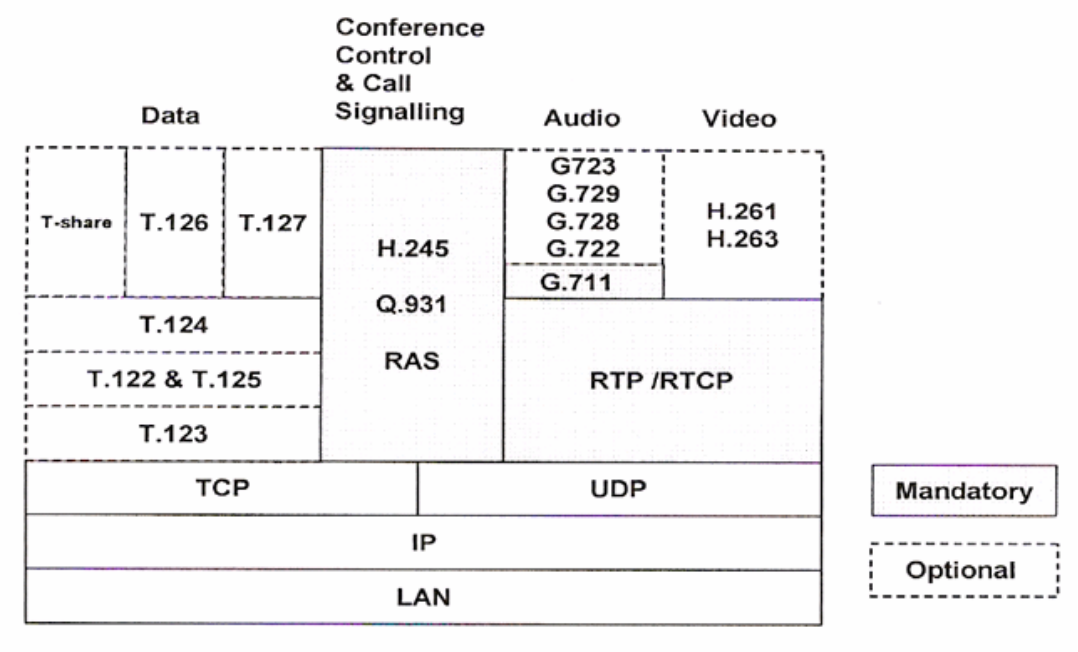


Figura 3.9 Pila de estándares

3.3.4 Transporte en H.323 (RTP y RTCP).

H.323 especifica el IETF protocolo en tiempo real (RTP) como el mecanismo de transporte para tráfico en tiempo real. RTP suministra servicios de entrega de datos en los extremos de la red en tiempo real, semejante al audio y video interactivo. Esos servicios incluyen tipo de identificación, número de secuencia, tiempo de reconocimiento y verificación de entrega. Las aplicaciones corren en RTP o en UDP para ser uso de un multiplexado y otros servicios; ambos protocolos contribuyen en parte al transporte de la información. RTP soporta transferencia de datos hacia múltiples destinos utilizando un control distribuido definido por la red.

RTP no suministra ningún mecanismo para asegurar una entrega a tiempo o proporciona cualquier otra garantía de calidad de servicio, pero tiene otros beneficios. La secuencia de números incluidos en RTP permite la recepción para reconstruir el paquete enviado, pero los números de secuencia podrían también ser usados para determinar la ubicación propia de un paquete; por ejemplo en la decodificación de video, sin que necesariamente los paquetes se decodifiquen en secuencia.

Mientras que RTP esta diseñado para satisfacer las necesidades de participantes que utilizan conferencias en multimedia, esto no ha limitado su uso en aplicaciones particulares. Por ejemplo el almacenamiento continuo de datos, simulación interactiva, y control, pueden ser usadas a partir de RTP, como lo muestra la figura 3.10

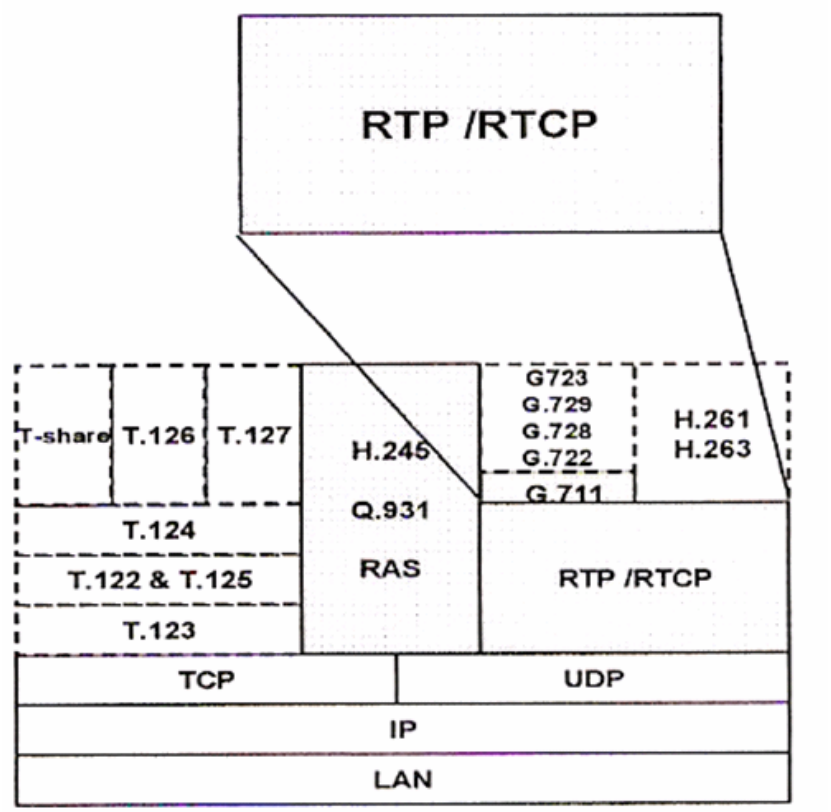


Figura 3.10 Transporte en H.323

3.3.5 Audio Codec H.323

El Audio Codec (coder/decoder) es el equipo que transforma la conversación analógica en un formato digital (y viceversa). El desafío para todos los desarrollos de Codec es proporcionar buena calidad usando una pequeña velocidad de bits en la medida de lo posible. Esto ha sido posible utilizando algoritmos para codificar y recodificar y esto no es tan complejo en comparación con las ventajas que ofrece. Las ventajas más importantes de Codec son:

- Regenerar la conversación cuando los paquetes se han perdido.
- Minimizar el retrazo cuando la conversación es codificada y decodificada.
- Asegurar que los paquetes no son demasiado largos porque esto puede generar atraso.
- Asegurar que los paquetes no sean demasiado pequeños en comparación con los protocolos que utiliza.
- Minimizar la carga de trabajo al procesador, para codificar y decodificar.

La obligatoriedad de H.323 esta especificada como G.711 y esto es los requerimientos mínimos para operar H.323.

- G.711 Modulación por código de pulso (PCM), 64kbits/segundo.

Sin embargo, otros "Codecs" están situados sobre telefonía IP y como resultado de H.323 también especifican "Codecs" opcionales. Algunos ejemplos de "codecs" opcionales son:

- G.723.1, Forward Adaptive IPAS (Linear Predietion Analysisby.Synthesis), 5.3/6.4 Kbit/s.
- G.729, Low Delay Codebook Exitation Linear Prediction (LD-CEIP), 8kbit/s.
- G.728, Low Delav Codebook Exitantio Linear Prediction (LD-CEIP), 16kbits/s.
- G.722, Adaptive Differential Pulse Code Modulation (ADPCM), 32kbit/s.

Lo anterior se observa en la figura 3.11.

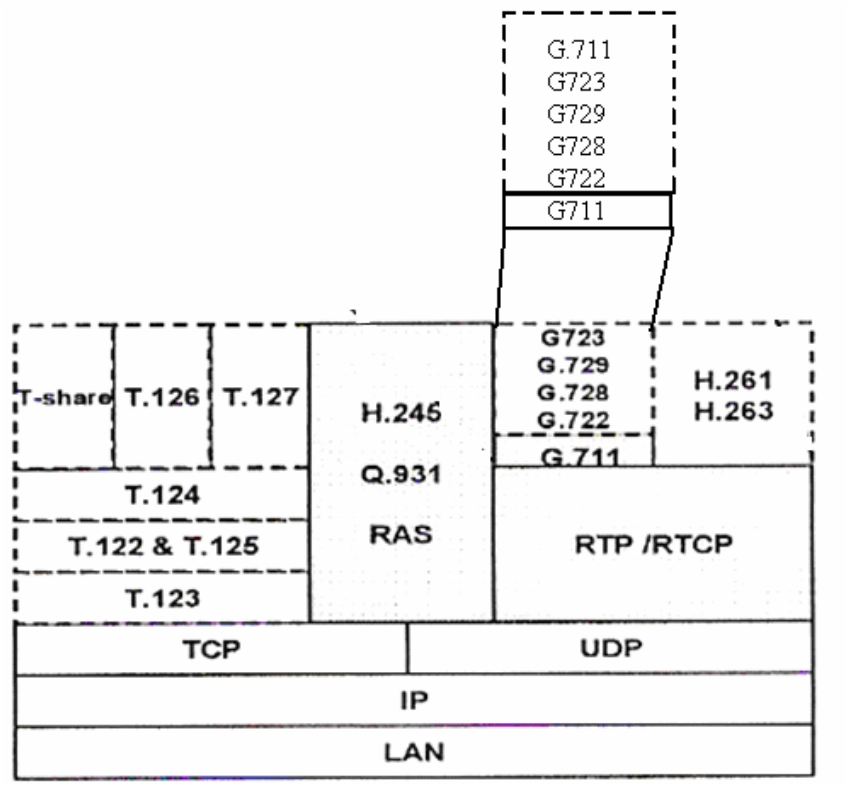


Figura 3.11 Audio Codec

3.3.6 Video Codec H.323

El video es opcional en H.323; sin embargo si el video es soportado los "codecs" especificados son: H.261 y H.263.

El H.261 es un estándar de compresión de video de desarrollado por ITU antes de 1992 para trabajar con RDSI. Los datos están comprimidos a una velocidad de 64 kbits/s. Este estándar fue desarrollado para soportar video conferencias.

El H.263 es un estándar de compresión de video para operar a una velocidad de 28.8 kbits/s. H.263 es una tecnología mas reciente y proporciona una mejor calidad de definición de video que el H.261. Lo anterior se muestra en la figura 3.12.

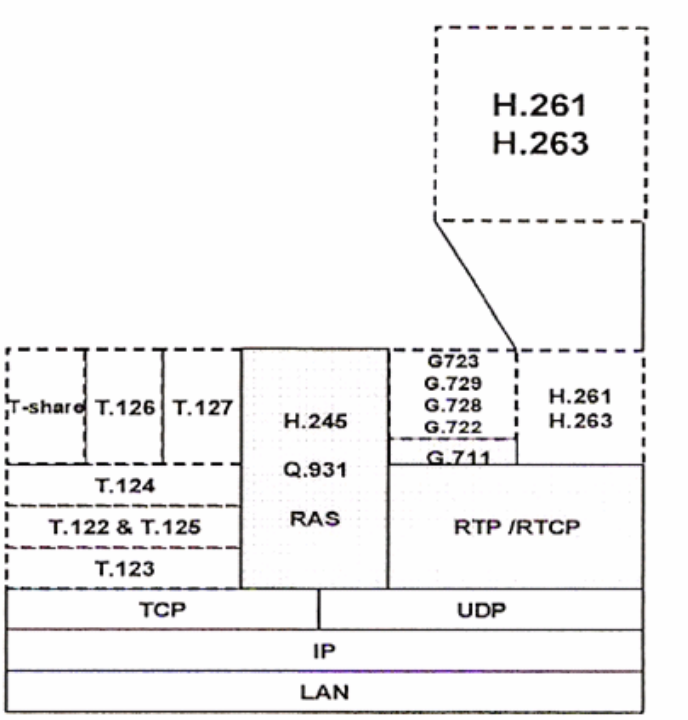


Figura 3.12 “Codec” de video en H.323

MPEG-4 es un estándar ISO/lEC que fue desarrollado por MPEG ("Mobing Picture Experts Group"). MPEG-4 trabajara en el futuro en el estándar H.323. MPEG-4 esta construido sobre tres campos de prueba exitosos: televisión digital, aplicaciones de gráficas interactivas y la www.

MPEG-4 tiene aplicaciones de velocidad definidas como 176 X 144 X 10 Hz y velocidades de codificación entre 4,800 y 64,000 bits/s. Este nuevo estándar podría ser usado en teléfonos con video sobre líneas de telefonía analógicas.

3.3.7 Señalización en H.323.

H.323 especifica tres fases para establecer una conexión entre uno o más puntos en una red y, separar protocolos de señalización que son utilizados para cada una de las fases:

- Registro y Control de Admisión, (H.225).
- Localización y ruteo para el estableimiento de IIamada(s), (0.931).
- Negociación de "medios" entre los puntos de conexión de la red, (H.245).

El canal de control H.245 es usado para abrir y controlar lógicamente los canales entre los puntos finales de conexión H.323. Durante la llamada, toda la información de control es llevada por este canal. El canal de control podría ser la ruta de mantenimiento de la(s) llamada(s). A través del mismo canal la capacidad de intercambio de información en los extremos de la red y, la determinación de equipos "maestro-esclavo" son permitidas.

Q.931 es usado sobre el Canal de Señalización de Llamada ("Call Signalling Channel", CSC) para activar y realizar la llamada. Si un "gatekeeper" está presente, el canal de

señalización podría ser abierto entre los extremos de la conexión y el "gatekeeper' o directamente entre los extremos de la conexión de la red. La decisión es tomada por el "gatekeeper' el cual solicita a los extremos de la conexión que active y envíe el mensaje.

H.225.0 / RAS ("Registration, Admisión, Status') es el canal usado entre las terminales de H.323 y el "gatekeeper'. Esto permite el registro, la admisión y conocer el estatus, así como los cambios en el ancho de banda y los procedimientos de desenganche entre los extermos de la conexión y el "gatekeeper'. RAS no es usado si no está presente un "gatekeeper".

H.323 usa dos mecanismos diferentes de trasnporte: uno confiable y uno no confiable. El transporte confiable (TCP en una red TCP/IP) es por parte de la señalización de control H.245 y por 0.931 (señalización de llamada), porque estas señales deben ser recibidas en un orden especial y no se pueden perder. El mecanismo de transporte no confiable (semejante al UDP) es aplicado directamente en el canal RAS y sobre el grupo de audio y video, como lo muestra la figura 3.13

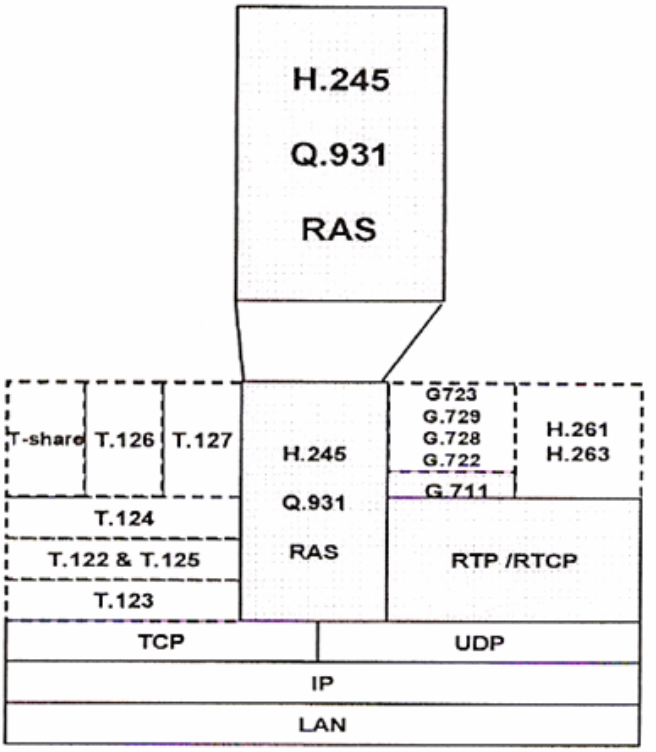


Figura 3.13 Señalización entre entidades

3.3.8 Levantamiento de Llamada en H.323.

La Figura 3.14 muestra como se lleva a cabo el proceso de una llamada utilizando H.323.

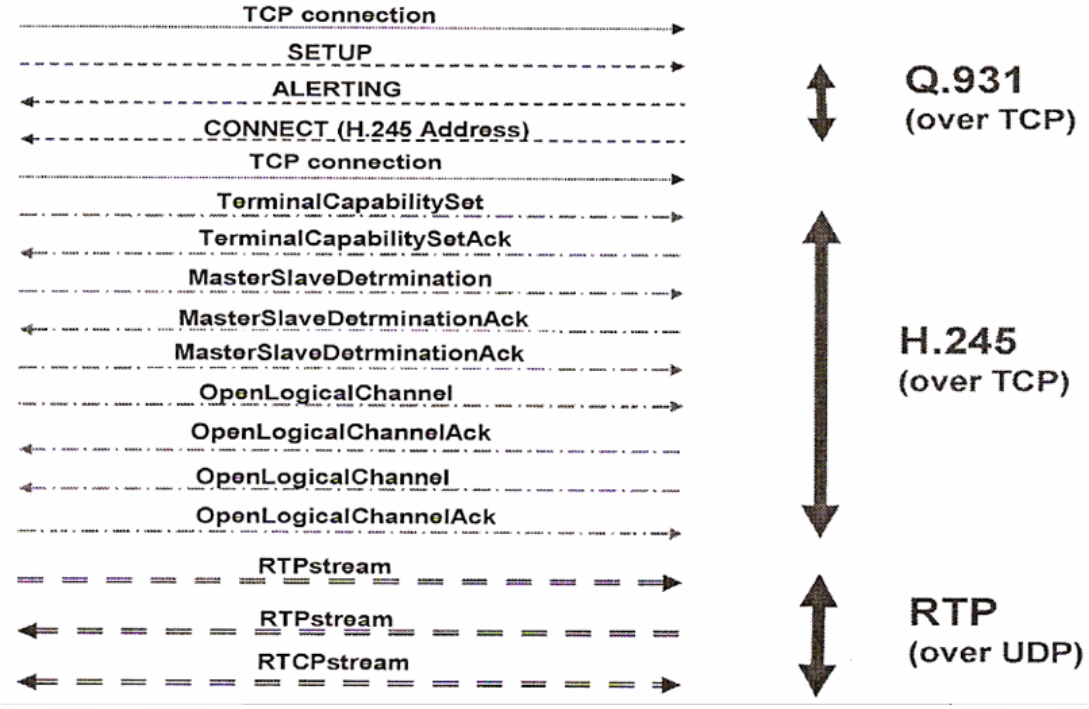


Figura 3.14 Llamada con H.323

Quien llama hace el procedimiento de conexión TCP utilizando el número de puerto 1720 usado por Q.931 como trasnmisión de señal. En el mensaje de conexión se coloca un número mayor a 1024. Una vez que la asignación de número de puerto fue hecha, quien llama crea una nueva conexión TCP a partir del control, de señalización H.245 para ubicar el puerto. Una vez que H.245 establece la conexión, la conexión Q.931 puede caerse o levantarse.

A través de la conexión TCP, H.245 comienza la fase de cambio, esto quiere decir que todos los parámetros de negociación son llevados a cabo. La sesión de H.245 ejecuta la secuencia de Apertura Lógica del Canal ("Open Logical Channel", OLC) con un comando que genera las conexiones UDP para llevar el flujo de información en tiempo real.

Con la secuencia de Apertura Lógica del Canal (OLC), las direcciones de los transmisores RTCP y los números de puerto para la recepción RTP y, las direcciones RTCP así como los números de puerto, son enviados. Este proceso debe ser hecho por cada grupo particular de información a ser enviado.

Dos canales lógicos deben ser abiertos para dos clientes que intercambian audio; por instancia, uno desde la terminal de cliente A hacia el Cliente B y el otro canal para llevar la información desde el cliente B hacia el cliente A.

El grupo RTP requiere dos conexiones UDP utilizando grupos adjuntos. Una conexión es para RTP (el actual grupo de datos), y otro es una conexión para RTCP, la cual tiene la información de control bidireccional. Los grupos asociados RTCP y RTP tiene que ser un puerto aparte, con un número par para la conexión del puerto RTP y el próximo que es mayor, será para uno de los puertos RTCP.

3.3.9 El H.323 "Fast-Start".

La Versión 1 (Circa, 1996) del H.323 especificó un estándar para la Telefonía IP sobre Redes de Área Local (LAN's) cuando el retraso en la señalización no era un serio problema. Sin embargo, para Redes de Área Amplia (WAN's) el tiempo de retraso es punto importante y por lo tanto, un procedimiento diferente llamado "FastStart" fue introducido como parte de la versión 2 del H.323 en 1998.

El objetivo del "FastStart" es para que las llamadas ocurran en el menor tiempo posible. El procedimiento del "FastStart" permite que los extremos de la conexión establezcan un una llamada punto a punto con una habilitación inmediata del grupo de información al establecer la conexión.

El mensaje "set-up" envía al cliente que llama, un campo adicional de contenido: el elemento "FastStart". Este elemento contiene la misma información que la secuencia de Apertura de Canal Lógico (OLC) de H.245, muy similara la descripción de capacidades enviado y recibido desde el cliente y por el número de puerto RTP; pero los parámetros necesarios para abrir inmediatamente la transferencia de información sobre los canales de comunicación, como se ve en la figura 3.15.

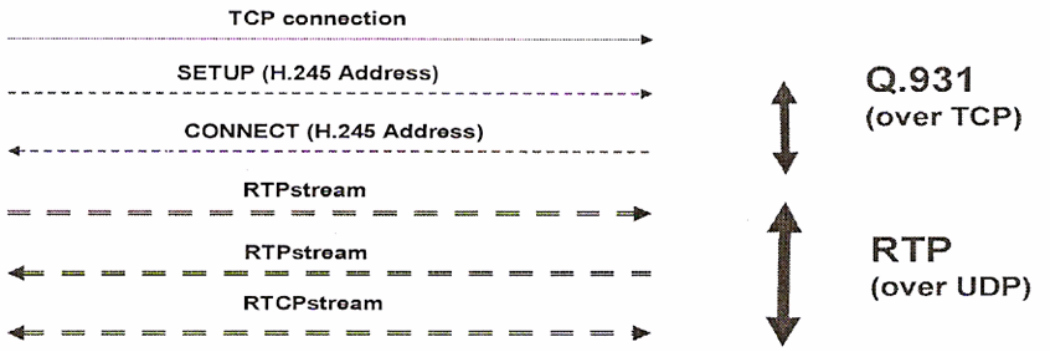


Figura 3.15 Llamada rápida con H.323

La ventaja obvia por usar el procedimiento de "FastStart" es el corto tiempo que toma el establecer la llamada, debido al poco intercambio de mensajes.

El siguiente ejemplo puede dar una idea sobre el tiempo "ganado" por usar el "FastStart". Para establecer una llamada normal a través de H.323 la suma total de señales es de 13 y, asumiendo un tiempo de ejecución de cada señal de 0.5 segundos, la llamada se realizará en 6.5 segundos. Mientras que con el "FastStart" la llamada se puede llevar a cabo en tan sólo 2 segundos.

3.3.10 Conferencias en H.323.

La Unidad de Control Multipunto ("Multipoint Control Unir, MCU) soporta la función de permitir conferencias multimedia entre tres o más terminales. Los MCU's toman tareas de coordinar todas las capacidades de multimedia de los clientes participantes en la conferencia. Un MCU puede suministrar características para la conexión de la red que no podrían ser suministrados de forma local (por ejemplo; selección de video y mezcla de audio). Bajo un sistema H.323, la MCU consiste de un Controlador Multipunto

("Multipoint Controller', MC) y un Procesador Multipunto opcional, ("Multipoint Processor', MP).

La característica más importante de un Controlador Multipunto es que asume las negociaciones entre el H.245 y todas las terminales en secuencia de determinar capacidades comunes para el procesamiento de audio y video. La determinación de los recursos para una conferencia (el flujo de audio / video que se necesita para ser repartido) son totalmente controlados por un Controlador Multipunto (MC).

Subsecuentemente, el Procesador Multipunto (MP) es responsable de negociar con el flujo de información acerca de los switches del procesamiento multipunto, procesar y mezclar todo el audio / video / bits de datos. Existen dos tipos de conferencia multipunto:

- Centralizada.
- Descentralizada.

3.3.10.1 Conferencia Centralizada en H.323.

Las conferencias centralizadas multipunto requieren la existencia de un MCU para facilitar dicha conferencia. Todas las terminales envían audio, video, datos y flujos de control desde el MCU de forma punto a punto. El MC maneja centralmente la conferencia usando las funciones de control de H.245 que también definen las prestaciones de cada una de las terminales.

El MP da la mezcla de audio, la distribución de datos y la mezcla y selección de video; así como funciones típicas permitidas en conferencias multipunto y envía el flujo de resultados hacia las terminales participantes. El MP también proporciona conversiones entre diferentes codificadores y decodificadores ("Codecs') y velocidad de bits; así como distribuir video ya procesado. Un MCU típico que soporta conferencias centralizadas multipunto consiste de un MC y un procesador de audio, de video y/o de datos. La figura 3.16 muestra una conferencia centralizada.

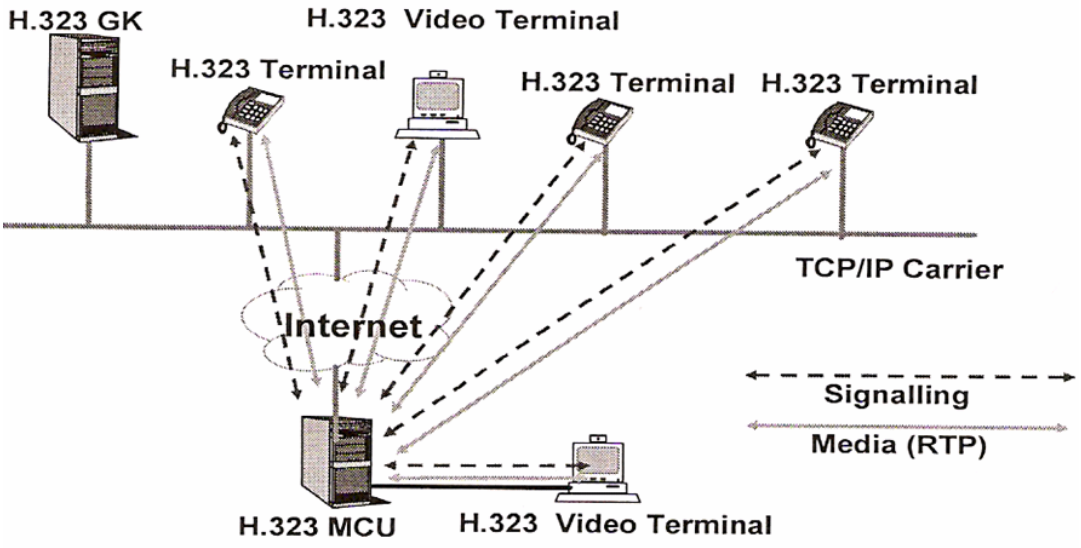


Figura 3.16 Conferencia centralizada en H.323

4.3.10.2 Conferencia Descentralizada en H.323.

Las conferencias descentralizadas multipunto pueden hacer uso de tecnología repartida o, en su caso, no centralizada. Las terminales que participan en el multireparto de audio y video hacia otras terminales lo hacen sin enviar datos hacia un MCU. Nótese que el control de datos en un proceso multipunto es todavía un proceso centralizado por el MCU, y la información en el Canal de Control es aún transmitida en modo punto a punto en un MC.

Las terminales receptoras son responsables por el procesamiento múltiple recibiendo flujos de audio y video. Las terminales usan H.245 ("Control Channels") para indicar al MC cuántos flujos simultáneos se pueden decodificar. El número de prestaciones simultáneas de una terminal no limita el número de flujos de audio y video se pueden repartir en una conferencia. El MP puede también proporcionar selección de video y mezcla de audio en una conferencia multipunto descentralizada. Lo anterior se muestra en la figura 3.17

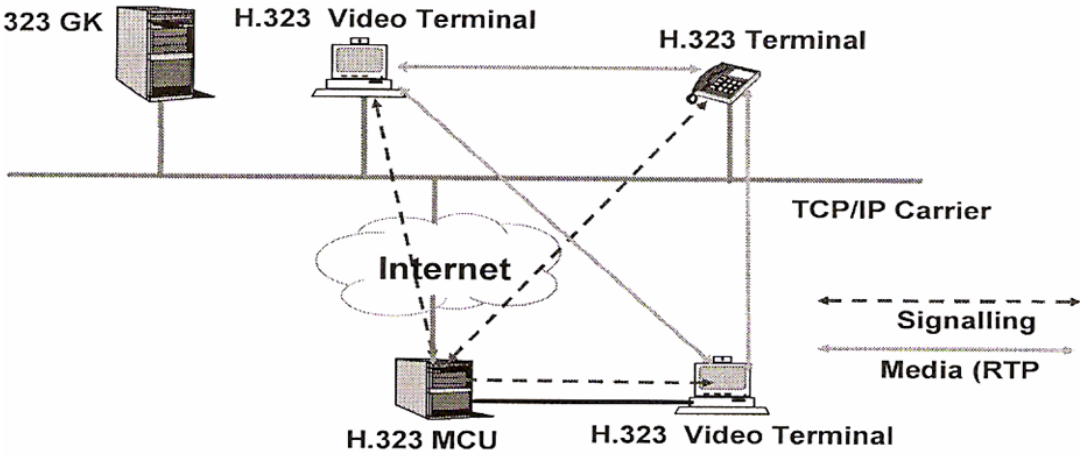


Figura 3.17 Conferencia descentralizada en H.323

3.4 Codificación

3.4.1 Codificación y Decodificación del Habla.

Para ser capaz de enviar una conversación telefónica sobre paquetes digitales, primero se requiere un proceso de conversión analógico / digital. Mientras que la respuesta en frecuencia de la voz humana cubre un rango de frecuencias cercana de los 20 Hz o quizá un poco mayores, la mayoría de la información importante que existe está contenida en un ancho de banda de entre 300 Hz y 3400 Hz. Lo anterior es importante en el mundo de la telefonía porque al hablar se utiliza un ancho de banda bajo.

Un "Codec" (codificador / decodificador) es un equipo (en términos generales) que toma una señal analógica, que usualmente representa audio o datos de video y posteriormente, los decodifica a un formato binario para almacenarlos o procesarlos después. Un "Codec" puede también decodificar los mismos datos y reconstruirlos en la señal analógica original, como lo muestra la figura 3.18.

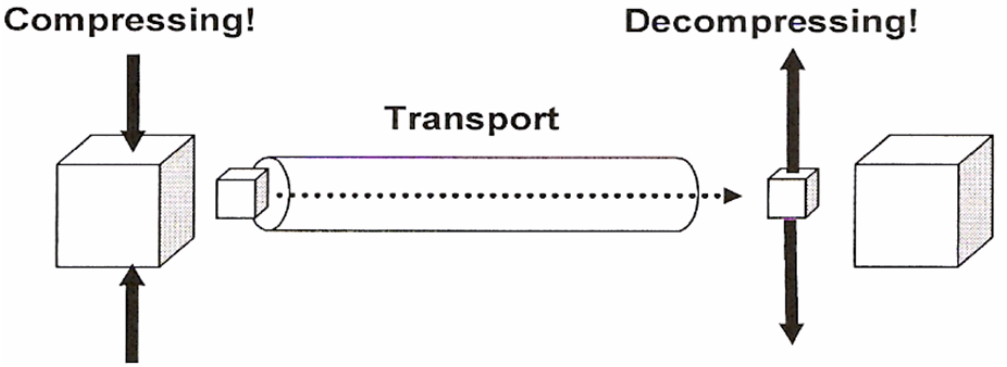


Figura 3.18 Codificación/decodificación del habla

El "Codec" requiere procesar rangos de voltaje, pero salva recursos dando un formato a la señal para aproximarla lo mejor posible al formato requerido para su transporte. Similarmente, se utiliza cierto voltaje para comprimir los datos para ser enviados como archivos adjuntos en un correo electrónico o simplemente, para salvar espacio en disco duro.

Generalmente, cuando se habla por teléfono, el mayor consumo de potencia está siendo usado; es decir, un ancho de banda amplio, demanda potencia, pero en cambio proporciona calidad.

3.4.2 El "Codec" y el Proceso de Enmarcar la Información.

El procesamiento íntegro de una señal de voz analógica (o video) que cae en los paquetes enviados de IP, consiste en diferentes pasos.

Primero, la entrada analógica (la voz o la señal de video) es muestreada y medida en una forma digital en un paso dado del proceso. Este paso podría ser a cualquier frecuencia, pero en el caso de "Codecs" de voz se hace el muestreo a una velocidad de 8 kHz correspondiente a un muestreo simple cada 0.125 milisegundos.
Segundo, el flujo de datos medido es codificado de acuerdo con un "Codec" ya escogido. Los resultados obtenidos son diferentes, pequeños y con cierto volumen de datos. Que tan pequeño debe ser el volumen de datos, esto depende del tipo de "Codec" seleccionado. El voltaje requerido para el procesamiento varía considerablemente dependiendo del "Codec" utilizado.

Tercero, el flujo de datos digitales está agrupado juntos dentro del paquete IP. Típicamente un paquete IP corresponde de 5 a 30 ms de voz dependiendo del "Codec", resultando entre 30 a 300 paquetes por segundo. Esto también depende del "Codec" que se está usando en el proceso de diseño de la aplicación IP.

La razón de muestrear a 8 KHz es que la respuesta de la frecuencia de la voz humana cubre un rango de frecuencias alrededor de 20 kHz, con mucha de la información importante contenida en la banda de los 300 a los 3400 Hz. Para evitar la distorsión una señal puede ser muestreada al menos dos veces cada ciclo, sin embargo la amplitud de la componente de frecuencia de la señal distorsionará la señal a bajas frecuencias. Pero, si la frecuencia muestreada es al menos dos veces más rápida que la más alta componente de frecuencia, la señal digital será una mejor aproximación de la señal

analógica. En este caso, se da un frecuencia de muestreo de dos tiempos: 3400 Hz y para varias posibilidades en 8000 Hz. Lo anterior se conoce como el Teorema de Nyquist.

Cuando un arreglo de datos digitalizados es enviado sobre un canal de datos (IP o Frame Relay). Esos datos viajan en paquetes, cada uno consiste de un encabezado, avance y un encabezado de bytes. Construyendo múltiples armazones de voz dentro de los paquetes se ayuda a minimzar los encabezados; por el contrario, se puede enviar cada grupo de datos en su propio paquete con su propio encabezado, avance y encabezado de bits.

3.4.3 Tipos de Codificadores y Decodificadores ("Codecs").

Hay diferentes formas para codificar voz. Pero los dos tipos básicos de codificación son:

- "Codecs" de forma de onda.
- "Vocoders", también llamados "Codecs" de fuente de onda.

Los más viejos, mejor conocidos y más extensos "Codecs" son los "Codecs" tipo Forma de Onda. Este "Codec" recrea la señal de entrada completa y la información no se pierde durante el procesamiento del "Codec". La común Modulación por Código de Pulso ("Pulse Code Modulation", PCM) y el "Codec" Diferencial Adaptado PCM ("Adaptive Differential PCM') , son de este tipo.

"Codecs" de Forma de Onda producen las más altas velocidades de transmisión de bits (16 kbps o más), pero ofrecen buena calidad de voz con bajo retraso, son muy simples y requieren poco voltaje. Los "Codecs" de Forma de Onda intentan reproducir las formas de eonda de audio tan exactas como les es posible.

En contraste con los "Codecs" de Forma de Onda están los "Codecs" de Fuente. Éstos se construyen sobre modelos de lo que es transmitido y recibido. En el caso de la voz, los "Codecs" de Fuente modelan tanto la voz como el oído humano.

El más conocido es el GSM, éste analiza la entrada de voz y la aproxima a la de un generador sintético de voz. El flujo de datos trasnmitido es una serie de cambios en parámetros para filtros digitales. En vez de tratar de reproducir el actual dominio del tiempo de la forma de onda como lo haría un "Codec" de Forma de Onda, esta técnica analiza tramas de voz de 20 milisegundos y, los números de salida que caracterizan la forma de las cuerdas bucales de los humanos "manejando la función" durante un periodo de tiempo.

Los "Vocoders" producen bajas velocidades de bits (típicamente entre 2.4 kbps a 8 kbps) con alta calidad en el procesamiento a altas velocidades. Lo anterior se debe a que se requieren grandes retrasos durante el procesamiento, semejante a las suma de ciclos de tiempos muertos durante una llamada telefónica.

Para permitir nuevas reducciones en el ancho de banda con aceptable calidad existe un "Codec" híbrido que ha sido desarrollado. Todos los "Codecs" de bajo ancho de banda

para VoIP son de este tipo (los "Codecs" H.323, G.723 Y el G.729). Esto combina el "Codec" de Forma de Onda con el "Voeoder" de rendimiento simultáneo de procesamiento y ajuste para diferencias significativas entre la señal codificada de una forma de onda específica y la señal codificada de un "Vocoder".

El muy bajo ancho de banda del flujo de datos del "Vocoder' es complementado por una "corrección" producida por el flujo de datos vía el codificador de forma de onda.

3.4.4 Ejemplos de "Codecs".

El muy conocido "Codec" usado en redes PSTN es el PCM Modelo G.711. Éste muestrea a 8 kHz y tiene un formato de código de muestreo usando 8 bits, resultando en una velocidad de transmisión de datos de 64 kbps. El G.711 es un ejemplo de un "Codec" de Forma de Onda.

En el sistema de telefonía móvil europea GSM se tienen diversos tipos de "Codecs" llamados Vocodecs, alguna de esas aplicaciones puede darse sobre VoIP. La tasa de velocidad es 13 kbps para un, "CodecFull Rafe GSM (FR)" y 12.2 kbps para un "Codec GSM Enhanced Full Rafe (EFR)".

Los "Codecs" estandarizados H.323, G.728, G.729 Y G.723 están diseñadas para aplicaciones sobre VoIP. Estos son algunos ejemplos de "Codecs" Híbridos:

- G.728: Low Delay Codebook Excitation Linear Prediction (LD-CEIP), 16 kbps.
- G.729: Forward Adaptive IPAS (Linear Prediction Analysis- by-Synthesis), 8 kbps.
- G.723.1: Forward Adaptive IPAS (Linear Prediction Analysis- by-Synthesis), 5.3/6.4 kbps.

3.4.5 Tasa de Velocidad del "Codec". Calidad y Procesamiento.

Para "Codecs" en general, la tasa de velocidad depende de la potencia requerida para el procesamiento para alcanzar la tasa de velocidad requerida y la pobreza en el sonido.

Bastante interesante es el requerimiento entre PCM y cualquier medición extrema, es dramáticamente diferente. El "Codec" PCM requiere muy poca potencia de procesamiento y el resultado es bastante ubicable en el indicador de línea de implementación de bajo costo en intercambio telefónico.

La medida de calidad ("Mean Opinión Store", MOS) es una medida subjetiva de calidad de voz en los extremos de la red.

El MOS está basado sobre índices de audiencia. El MOS es una medida, la cual es ampliamente usada para cuantificar la calidad de voz sobre un "Codec". El MOS usualmente implica de 12 a 24 escuchas, quienes están estructurados para balancear la tasa de velocidad de bits fonéticamente de acuerdo a 5 niveles de una escala de calidad. Los índices de la escala de calidad de MOS son:

1.- Mala.
2.- Pobre.
3.- Justo.
4.- Buena.
5.- Excelente.

Una excelente calidad de voz implica que la codificación de la voz es indistinta desde el arreglo original sin ruido perceptible. Por otro lado, una mala calidad implica la presencia de gran cantidad de ruido en la codificación de la voz.

Algunas pruebas de escucha de MOS están "calibradas" en la idea que se debe familiarizar con las condiciones de los escuchas y el rango de calidad de transmisión de voz. Los índices son obtenidos por promedio numérico de valores sobre cientos de grabaciones de voz. El rango de MOS relativas a la calidad de transmisión de voz son las siguientes: un MOS de 4-4.5 implica un nivel de calidad en la red entre 3.5 y 4; mientras que un MOS con valores entre 2.5 y 3.5 es una calidad sintética.

3.4.6 Calidad en la Voz.

La medida subjetiva de percepción de calidad de voz en los extremos de la red, es una nueva cuestión en la comunicación en el "datacom" mundial donde la calidad es ubicada en términos de pérdida de paquetes o errores de bit. El propósito de la Telefonía IP es proporcionar un nivel de calidad de recepción de voz que al menos iguale el que se tiene en el PSTN.

La calidad de voz es más exacta cuando se liberan los datos y esto lleva muchos factores entre ellos resaltan: retraso, pérdida de paquetes, ancho de banda y tipo de "Codecs" así como, la implantación de la aplicación. Hay muchos factores que influencian la percepción de calidad de voz. Los más importantes son:

- Retraso de paquetes.
- Variación en el retraso.
- Pérdida de paquetes.
- Ancho de banda.

Otros factores importantes para la calidad de voz son:

- Codificación silenciosa.
- Eco.

Es totalmente posible tener dos sistemas: uno para un mejor sonido y otro para garantizar la mejor calidad de transmisión. Esto lo muestra la figura 3.19

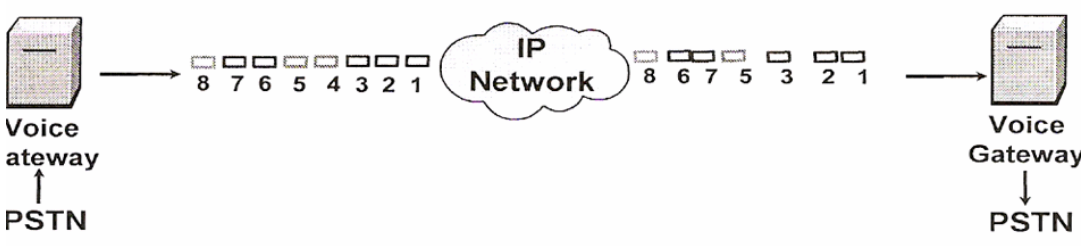


Figura 3.19 Calidad de voz

3.5 Retraso de Paquete(s) y sus Variaciones.

La aplicación VoIP es requerida considerando el hecho de que el flujo original de paquetes será retrasado y algunos paquetes individuales serán retrasados más que el resto de los paquetes. Algunos paquetes se pueden perder al sobrepasar la capacidad de los ruteadores o también debido al viaje alterno en rutas que causa la pérdida de paquetes de forma irreversible.

El sistema VoIP es "justamente otra aplicación de IP" y usa la red como su propia interfaz, pero esto no puede permitirse en una conexión segura libre de errores.

El eco es un problema serio en la comunicación de voz; se determina de forma primaria en los primeros 50 milisegundos de iniciada la transmisión, por lo tanto los sistemas VoIP deben cuantificar el valor del eco e implementar después, una forma de cancelario de la transmisión.

El problema de saturación al hablar es el problema que afronta uno de los usuarios que llama a otro en una transmisión de voz; esto es significativo si se llega a tener un retraso en la transmisión mayor a 250 milisegundos. El objetivo es reducir el retraso de las transmisiones de tal forma que se tenga una buena calidad en la transmisión de un paquete de información en la red.

Si los paquetes transmitidos son retrasados en su totalidad, éstos llegarán algún tiempo después de ser enviados. Sin embargo, este retraso nunca es constante y varía de paquete a paquete. Esta variación es llamada "Variación" ("Jitter) y se mide como la máxima diferencia en retraso a partir de un valor promedio de retraso.

La variación ("Jitter) es la desviación o desplazamiento de los pulsos en una señal de alta frecuencia digital. Como su nombre sugiere, la variación puede ser minuciosa en los pasos que se consideren inseguros. La desviación puede ser en términos de amplitud, fase o en el ancho de banda del pulso. Otra definición es que "es el periodo de frecuencia desplazado de la señal desde su ubicación ideal".

La variación puede introducir chasquidos u otros efectos indeseables en las señales de audio y por consiguiente, pérdida de datos transmitidos entre los equipos que conforman la red. El valor de la variación depende de la aplicación que se esté dando. Los siguientes valores son los más significativos en la medida de la variación ("Jitter'):

- Retraso en una LAN de una sola ruta, 10 ms
- Variación en una LAN, 1 ms .

- Retraso en una WAN de una sola ruta, 100 ms .
- Variación en uan WAN, 10 ms .
- Los retrasos de Internet están sobre 100 ms, típicamente son 300 ms o más.

Retraso y variación es causada por diferentes partes en un sistema de Telefonía IP, como los "Codecs", el sistema operativo en la terminal y en la compuerta ("Gateway") y el propio manejador del IP. La "Variación" es generada por interferencia electromagnética (EM) y su mezcla con otras señales. La figura 3.20 muestra el retraso en los paquetes.

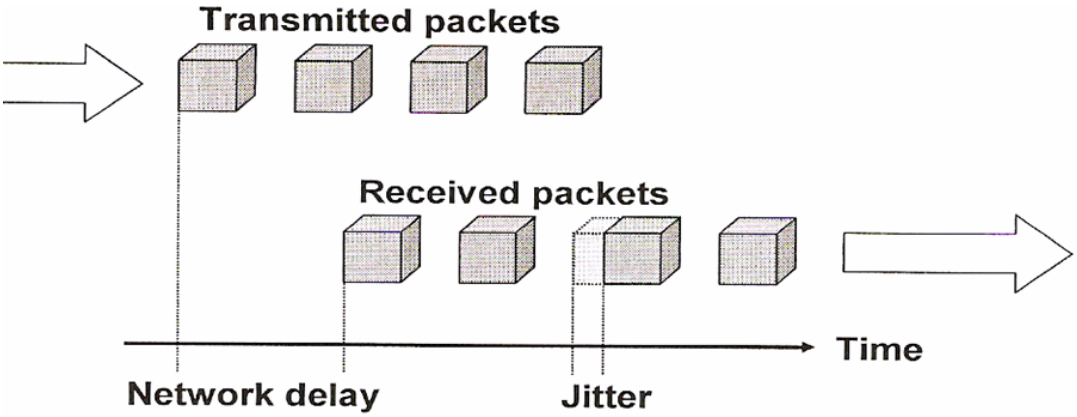


Figura 3.20 Retraso de paquetes y variación

3.5.1 Almacenamiento Momentáneo de Paquetes ("Buffering") y Pérdida de Paquetes.

En estricto sentido, el flujo de datos es almacenado temporalmente antes de su decodificación. Esto permite recibir los datos de una forma ordenada. El tamaño correcto del canal de retención momentáneo ("Buffer) depende del valor de la variación ("Jitter') y existen varias implantaciones ya elaboradas las cuales usan tamaños de "Buffer" dependiendo de las condiciones de la red. Hay dos tipos de manejo de variación del "Buffer": Fixed play-out delay (el "Buffer" almacena cad uno de los paquetes por un tiempo específico); y Adaptive play-out delay (este tiempo se ajusta de acuerdo a la variación del retraso de la red).

Las Redes IP no pueden garantizar que todos los paquetes serán liberados en el orden requerido debido a la variación de los retrasos. Bajo cargas pico y durante periodos de congestión causados por ejemplo por fallas en el enlace o por problemas de capacidad, los paquetes pueden ser abandonados. Esto debido a lo crítico de los tiempos en las transmisiones de voz; sin embargo, los esquemas normales de retransmisión basados en TCP no está disponible. Un número de accesos o aproximaciones son usados para compensar cada paquete perdido incluyendo la interpolación de voz por una retransmisión del paquete perdido enviando información redundante. Una pérdida de paquetes mayor al 10%, generalmente no es aceptable. Es importante considerar que un almacenamiento temporal de datos ("Buffering") no previene pérdidas en la transmisión, ya que sí se pueden presentar en un proceso real de transmisión. La figura 3.21 muestra lo anterior.

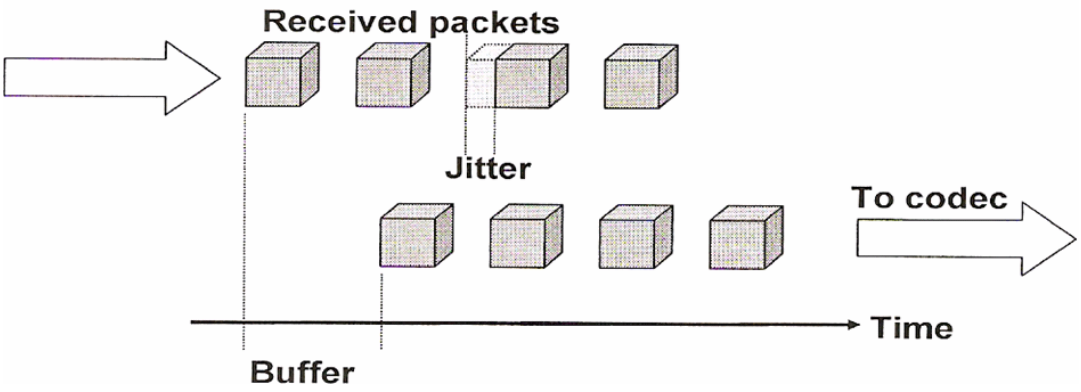


Figura 3.21 Almacenamiento temporal de paquetes

3.5.2 VoIP vs Retrasos en PSTN.

Esta sección permite comparar los retrasos asociados con VoIP y además, lo que ocurre al utilizar PSTN. Para VoIP los retrasos son debidos a que:

- Los procesos de codificación y decodificación toman tiempo de proceso en los extremos de la conexión.
- El proceso de enmarcado ("framing') toma cierto tiempo. ~ Hay retrasos asociados con la transmisión.
- Hay retrasos causados por el uso de una Variación del canal de retención momentáneo ("Buffer).

Para VoIP la gran diferencia entre una "buena" y una "mala" red es el valor del retraso ("delay') y la variación ('Jitter). En el peor de los casos se tiene alto retraso en la red y/o un alto valor de variación; una alta variación del "buffer' es usada resultando en un cierre de retraso intolerable.

Para Internet, el mejor caso es con un tiempo de 180 ms y el peor caso es con 330 ms. Lo recomendado para la LAN son 90 ms y 140 ms, respectivamente.

En el caso de PSTN los valores están listados sólo como alta o baja frecuencia de retraso porque ITU-T tolera diferentes retrasos sobre diferentes valores en frecuencia (baja y alta, respectivamente).

El Organismo ITU-T recomienda el máximo retraso entre dos abonados en 150 ms y para conexiones internacionales un máximo de 400 ms para permitir al satélite realizar la conexión. Un Módem de telefonía digital de intercambio (poe ejemplo, un PBX) tiene un retraso menor a 10 ms.

En el mejor de los casos, VoIP crea un escenario de un retraso por cada vía de comunicación, el PSTN es un caso típico de esta situación. Por otra parte, en el peor caso, el retraso característico de PSTN se considera bajo en comparación con el mejor de los casos en VoIP.

3.5.3 Percepción de la Calidad de Voz.

La calidad de voz es siempre una cuestión de qué se está usando para la comunicación y qué se requiere para que dicha comunicación se dé. En páginas previas se han desarrollado temas como retraso, pérdida de paquetes y la variación en los retrasos que puede llegar a tener un enlace de voz. El diagrama de la Figura 111.38 es el resultado de pruebas donde las personas han percibido una buena calidad en la recepción de voz y esto es considerado como una buena conclusión en relación a lo que la transmisión de voz demanda para VoIP y para cualquier transmisión de información por voz.

El diagrama de la Figura 3.22 muestra el nivel de calidad de voz percibida durante las transmisiones en relación a la pérdida de paquetes y los retrasos en la llegada de la información. La gráfica muestra:

- Área aceptable (buena calidad), <5% de pérdida de paquetes y <200 ms en el retraso.
- Área aceptable (baja calidad), <10% de pérdida de paquetes y <400 ms en el retraso.

- Área no aceptable, >10% de pérdida de paquetes y >400 ms en el retraso.

Para una buena calidad en el retraso, éste debe ser menor a 200 ms y la pérdida de paquetes debe ser menor al 5%.

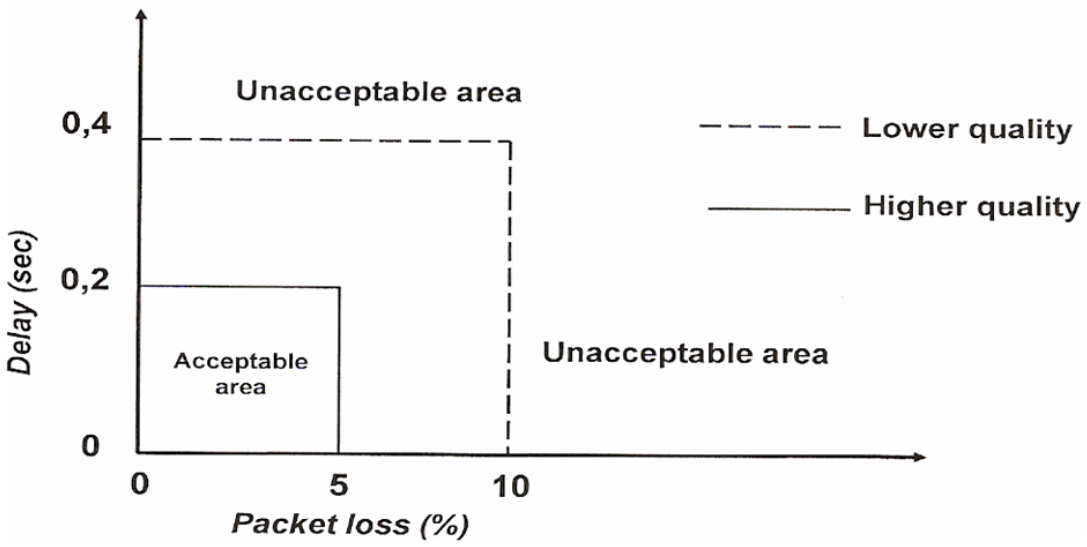


Figura 3.22 Nivel en la calidad de voz

3.5.4 Ejemplo de Implantación - Codificación Silenciosa.

Hay muchas formas para diseñar los diferentes componentes del sistema de VoIP. Un ejemplo del componente de codificación silente en VoIP es mostrado en la Figura 3.23.

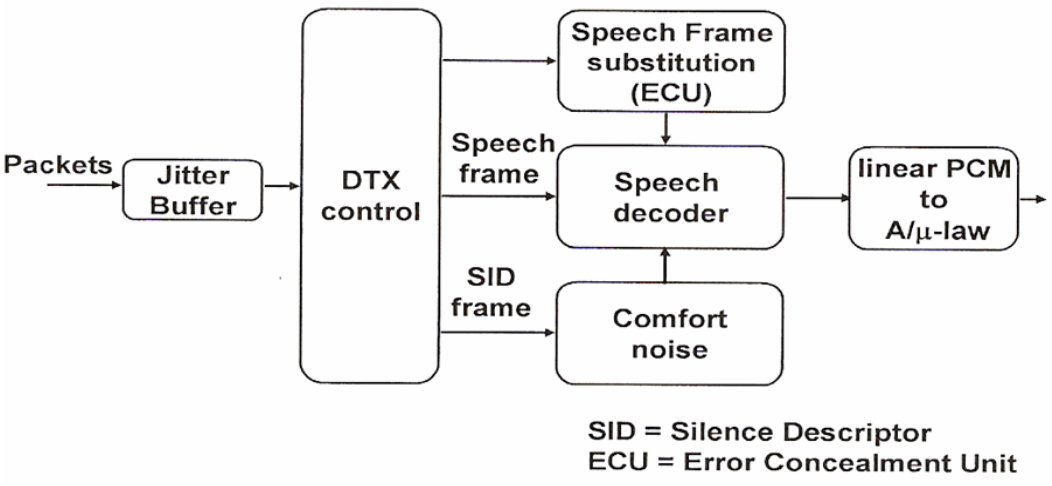


Figura 3.23 Codificación silenciosa

Los paquetes recibidos son almacenados temporalmente para ser clasificados por su tipo (OTX Control). Un flujo normal de voz es decodificado (a través del decodificador de voz), mientras que un descriptor silente (810) o un detector de paquetes perdidos es manejado en un sentido especial. La forma para retomar los paquetes perdidos es totalmente sobre la aplicación de diseño y varias técnicas elaboradas pueden ser aplicadas para proporcionar mejor calidad de voz sin simplemente ignorar los paquetes perdidos.

Estas técnicas son conocidas como "ocultar errores" y están diseñadas para superar temporalmente alguna congestión in la red IP, esto causa claros o huecos en el flujo de información que se encuentra en el paquete. El "error oculto" intenta ocultar esos huecos desde "el oyente" utilizando el "Speeeh Frame Substitution", (SFS). Algunos métodos son:

- Generar una copia de lo recibido previamente.
- Generar un "Buen Cálculo" estimado en los parámetros proporcionados por el "Codec" a partir de previos flujos de información.

Este tipo de técnicas son generalmente aceptables ya que el número de paquetes perdidos es mínimo.

Cuando se llega a detectar un "silencio" en la transmisión de la señal, hay menos datos a ser transmitidos y entra en operación un descritor silente. Cuando ese espacio silenciosos es detectado en la etapa de recepción, se utiliza una técnica de generación de "ruido confortable" con el objetivo de crear una señal natural que complete el tramo de silencio.

3.5.5 El Eco en PSTN en Comparación con la Telefonía IP.

Existen dos tipos de eco: Acústico, el cual es causado por el eco generado por las paredes o el cuarto en donde el usuario efectúa la llamada; y el Híbrido, el cual ocurre en la red de telefonía debida a la imperfección de la impedancia que hace juego. El Eco es generalmente una cuestión de retraso de alrededor de 50 ms y por lo tanto en Eco

debe ser considerado en una transmisión de VoIP. La figura 3.24 muestra el comportamiento del Eco en PSTM en comparación con el Eco en telefonía IP.

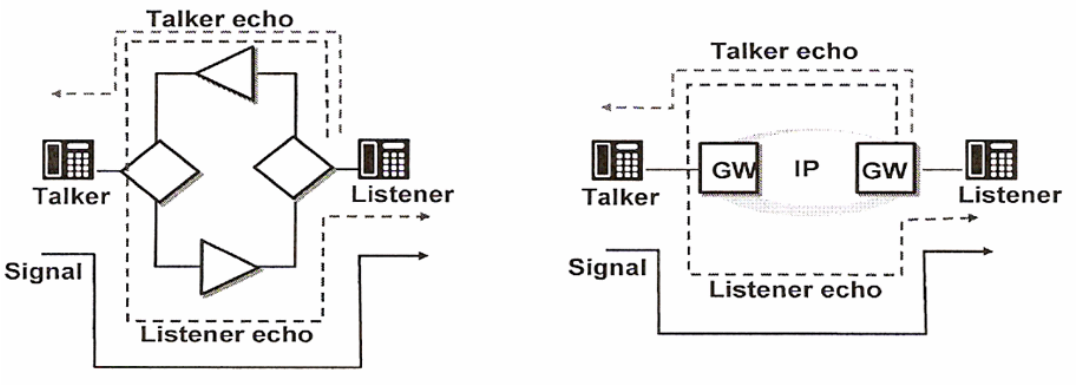


Figura 3.24 Eco

El Eco es un problema en el acceso a la red a través de PSTN, donde dos pares de alambre son usados para establecer una comunicación doble. La red de conferencia interurbana usa cuatro canales simples para la comunicación, en los cuales es muy sencilla la amplificación. El Eco Híbrido introduce Eco debido a sus propias imperfecciones.

El sistema de VoIP, también tiene sus imperfecciones de implantación para atravesar diferentes puntos de la red en una comunicación simple. Las estaciones de trabajo estan conectadas sobre el PSTN para acceder a la red, dichas terminales utilizan señales dobles en dos pares de líneas. De esta manera, la misma situación que crea el Eco en el PSTN, crea el Eco en la aplicación de VoIP.

El Eco puede ser suprimido o cancelado completamente si se aplica un correcto procesamiento de señales proporcionado por los arreglos DSP's o a través de una arquitectura dedicada como es el caso de los modernos intercambiadores PSTN.

La señal original y la señal de Eco están identificadas y de esta manara la señal de Eco puede ser suprimida o cancelada. El máximo valor de Eco que puede ser cancelado o suprimido es medido en el tiempo y la magnitud es medido en décimas de milisegundos.

3.6 Recomendación G.711

MODULACIÓN POR IMPULSOS CODIFICADOS (MIC) DE FRECUENCIAS VOCALES.

Definición de la cabida útil de ruido de confort para utilización según la Recomendación UIT-T G.711 a 64 Kbps en los sistemas de comunicaciones multimedios por paquetes
(Ginebra, 2000)

3.6.1 Alcance.

Este artículo define un formato de cabida útil de ruido de confort (o tren de bits) para utilizar el "Codec" de la Recomendación UIT-T G.711 en los sistemas de

comunicaciones multimedios por paquetes. El formato de cabida útil es genérico y puede también utilizarse con otros "Codecs" vocales sin capacidad de transmisión discontinua (DTX, "Oiscontinuous Transmisión') incorporada, como los de las Recomendaciones UIT-T G.726 [1], G.727 [2], G.728 [3] y G.722 [4].

El formato de la cabida útil proporciona una especificación de interoperatibilidad mínima para la comunicación de parámetros de ruido de confort. El análisis y la síntesis de ruido de confort, así como los algoritmos de detección de actividad vocal (VAD, "Voice Activity Oetection') y DTX no se especifican y siguen siendo específicos de la implementación. Sin embargo, se ha aprobado y se describe un ejemplo de solución. Utiliza el VAD y el DTX del anexo 8/G.729 [5] Y un algoritmo de generación de ruido de confort (CNG, "Comfort Noise Generation) que se proporciona como una información.

El formato de la cabida útil está destinado a su utilización por sistemas por paquetes que tienen una gran tara de encabezamiento, donde la velocidad de transmisión de paquetes desempeña un papel significativo en la velocidad binaria global del sistema. En esta situación, el uso de algoritmos VAD/DTX/CNG puede reducir significativamente la velocidad de transmisión de paquetes y por tanto mejorar la eficacia de anchura de banda.

3.6.2 Definición de la Cabida Útil de Ruido de Confort.

La cabida útil de ruido de confort se compone de una descripción del nivel de ruido y de información espectral en forma de coeficientes de reflexión. El uso de información espectral es opcional y el orden del modelo de todos polos no se especifica.

El codificador puede determinar el orden del modelo apropiado basándose en consideraciones de calidad, complejidad, ruido ambiental previsto y anchura de banda de la señal. El orden del modelo no se transmite explícitamente, ya que puede obtenerse de la longitud de la cabida útil en el receptor.

Por razones de complejidad o de otro tipo, el decodificador puede reducir el orden del modelo fijando a cero los coeficientes de reflexión de orden superior

3.6.2.1 Nivel de Ruido.

El nivel de ruido se expresa en -dBov con valores de O a 127 que representan O a -127 dBov. "dBov" es el nivel relativo a la sobrecarga del sistema. El nivel de ruido se empaqueta con el bit más significativo (MSB, most significant bit) con el bit no utilizado siempre puesto a cero según la Figura 3.25.

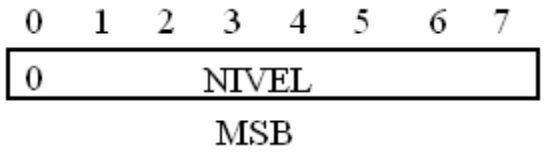
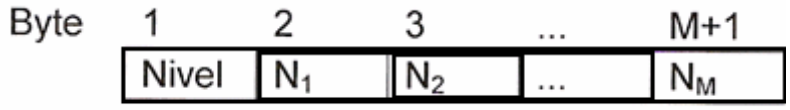


Figura 3.25 Empaquetamiento de Bits de Nivel de Ruido

3.6.2.2 Empaquetamiento de la Cabida Útil.

El primer byte de la cabida útil debe contener el nivel de ruido como muestra la Figura 3.25. Los coeficientes de reflexión cuantificados se empaquetan en bytes diferentes por orden ascendente como en la Figura 3.26, donde M es el orden del modelo.



La longitud total de la cabida útil es M+1 bytes. Obsérvese que un modelo de orden 0 (es decir, sin información de envolvente espectral) se reduce a transmitir únicamente el nivel de energía.

Figura 3.26 Formato de empaquetamiento de la Cabida útil de CN

3.6.3 Directrices de Uso.

La Figura 3.27 presenta el diagrama de bloques de un sistema de comunicación vocal con capacidades VAD/DTX/CNG. La misión del algoritmo VAD es discriminar entre segmentos de voz activa e inactiva en la señal de entrada. Durante los segmentos de voz inactiva, el papel del CNG es describir suficientemente el ruido ambiente, pero reduciendo al mínimo la velocidad de transmisión. Una trama de descriptor de inserción de silencio (SID, silence insertion descriptor) que contiene una descripción del ruido se empaqueta en la cabida útil de CN y se envía al receptor.

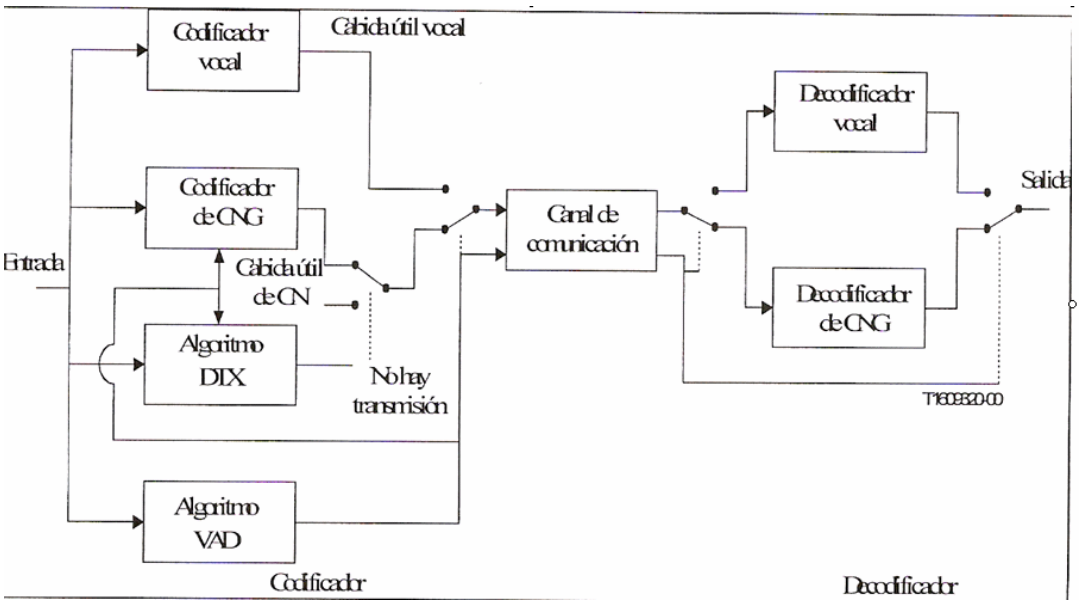


Figura 3.27 Sistema de comunicación vocal con DTX

El algoritmo DTX determina cuándo se transmite una trama SID. La trama SID puede enviarse periódicamente o sólo cuando hay un cambio significativo en la característica de ruido de fondo. El algoritmo CNG en el receptor utiliza la información del SID para

actualizar su modelo de generación de ruido y producir luego una cantidad apropiada de ruido de confort.

3.6.3.1 Factores que Afectan la Calidad de Funcionamiento del Sistema.

La finalidad de los componentes VAD/DTX/CNG es reducir la velocidad de transmisión durante los periodos de señal vocal inactiva, pero manteniendo un nivel aceptable de calidad de salida. La calidad y la eficiencia son ambas afectadas por las prestaciones de cada uno de los componentes. Debe procurarse considerar conjuntamente las características de los algoritmos VAD, DTX y CNG, ya que de otro modo la calidad de funcionamiento obtenida por el sistema resultante podría ser deficiente.

3.6.3.1.1 VAD.

El papel del algoritmo VAD es clasificar la señal de entrada en señal vocal activa y señal vocal inactiva o un ruido de fondo. La clasificación incorrecta de señal vocal inactiva como señal vocal activa tiene un efecto adverso en la eficiencia del sistema, al aumentar innecesariamente la velocidad de transmisión. En este caso, la calidad vocal no es afectada.

Sin embargo, cuando la señal vocal activa se clasifica indebidamente como inactiva, se recorta la señal vocal y se degrada la calidad vocal. La mayoría de los algoritmos DTX emplean un periodo de retención cuando pasan de señal vocal activa a inactiva a fin de evitar recortar el extremo de cola de la señal vocal. Durante el periodo de retención, las tramas de señal vocal inactiva se reclasifican como señal vocal activa. El periodo de retención es también importante a fin de que el codificador de CNG obtenga una estimación exacta del ruido ambiente.

3.6.3.1.2.- DTX.

El algoritmo DTX determina la frecuencia de la transmisión de tramas SID durante los periodos de señal vocal inactiva. Los esquemas DTX simples se actualizan periódicamente (por ejemplo, 5 Hz a 30 Hz). Los algoritmos DTX más complejos analizan la señal de entrada y transmiten sólo cuando se detecta un cambio significativo en el carácter del ruido ambiente [5].

3.6.3.1.3 CNG

El papel del CNG es describir y reproducir el ruido ambiente. El ruido puede describirse adecuadamente por su energía y contenido espectral. A fin de evitar cambios bruscos en el carácter del ruido de confort, es importante promediar la estimación del parámetro en un periodo de tiempo. La cantidad de promediación apropiada depende del ruido ambiente, la calidad de funcionamiento y la retención del VAD, así como de la velocidad de actualización del DTX.

El orden del modelo utilizado es un factor en la exactitud de la estimación espectral. El orden óptimo es dependiente del ruido ambiente presente y de la anchura de banda de la señal. Es también importante adaptar el carácter espectral del ruido producido por el CNG con el del códec vocal. Por consiguiente, se sugiere que todo procesamiento previo de la señal de entrada antes del análisis dentro del codificador vocal se efectúe también dentro del codificador de ruido de confort.

3.6.3.2.- Ilustración de las Economías de Anchura de Banda en las Aplicaciones a Redes de Paquetes.

La tabla ilustra cómo el uso de transmisión discontinua en un sistema de comunicación por paquetes puede reducir significativamente la velocidad de transmisión y por ende mejorar la eficacia de anchura de banda. El ejemplo supone una tara de paquetes de 40 bytes, actividad vocal del 60% y una velocidad de actualización de DTX de 10Hz.
Cuadro 111.1. - Economías de Anchura de Banda.

Códec	Velocidad binaria (bit/s)	Tamaño de paquete (ms)	Velocidad binaria IP (bit/s)	Cabida útil de CN de 1 byte		Cabida útil de CN de 11 bytes	
				Velocidad binaria IP (prom. bit/s)	Economias (%)	Velocidad binaria IP (prom. bit/s)	Economias (%)
G.711	64000	5 ms	128000	78 112	39,0	78432	38,7
G.711	64000	10 ms	96000	58 912	38,6	59232	38,3
G.711	64000	20 ms	80000	49312	38,4	49632	38,0
G.726	32000	5 ms	96000	58912	38,6	59232	38,3
G.726	32000	10 ms	64000	39712	38,0	40032	37,5
G.726	32000	20 ms	48000	30 112	37,3	30432	36,6
G.728	16000	5 ms	80000	49312	38,4	49632	38,0
G.728	16000	10 ms	48000	30 112	37,3	30432	36,6
G.728	16000	20 ms	32000	20512	35,9	20832	34,9

Por ejemplo, suponiendo un encabezamiento RTP/UDP/IP de 40 bytes, 60% de actividad vocal y una velocidad de actualización de DTX de 10Hz, la velocidad binaria IP media con G.711 y una cabida útil CN de 11 bytes viene dada por: ((64000 bit/s) + (40 bytes x 8bit/byte x (1,0/0,005s))) x (0,6) + ((40+11) bytes x 8 bit/byte x 10/s) x (0,4) = 78432 bits.

3.6.4.- Resultados de Calidad de Funcionamiento

Se realizó una evaluación subjetiva de un ejemplo de implementación de CNG utilizando la cabida útil de CN. Se utilizó como método de evaluación el método de determinación de índices por categorías absolutas (ACR, absolute category rating) definido en la Recomendación UIT-T P.800. El material vocal utilizado en el experimento estaba compuesto por frases breves significativas y sencillas. El material

de origen era IRS modificado filtrado (anexo D/UIT-T P.830) y organizado por pares. Cada par de frases duraba aproximadamente de 7 a 8 segundos, con un intervalo de tiempo entre frases de 1 segundo aproximadamente. En la evaluación se aplicaron condiciones de entradas calmadas y ruidosas, tales como ruidos de conversación confusa, de la calle, de oficina y de tráfico.

El "Codec" vocal utilizado en el experimento era un códec G.711, procesado por el procedimiento de la Figura 3.28 En este experimento, la implementación sólo disponía del algoritmo CNG. Se utilizaron los algoritmos VAD y DTX del anexo 8/G.729 [5]. Se obtuvieron ficheros de rastreo que contenían decisiones VAD y DTX con la bandera "SYNC" activada a fin de alinear la salida con el fichero de entrada. Esto se ve, más a fondo, en la figura 3.29

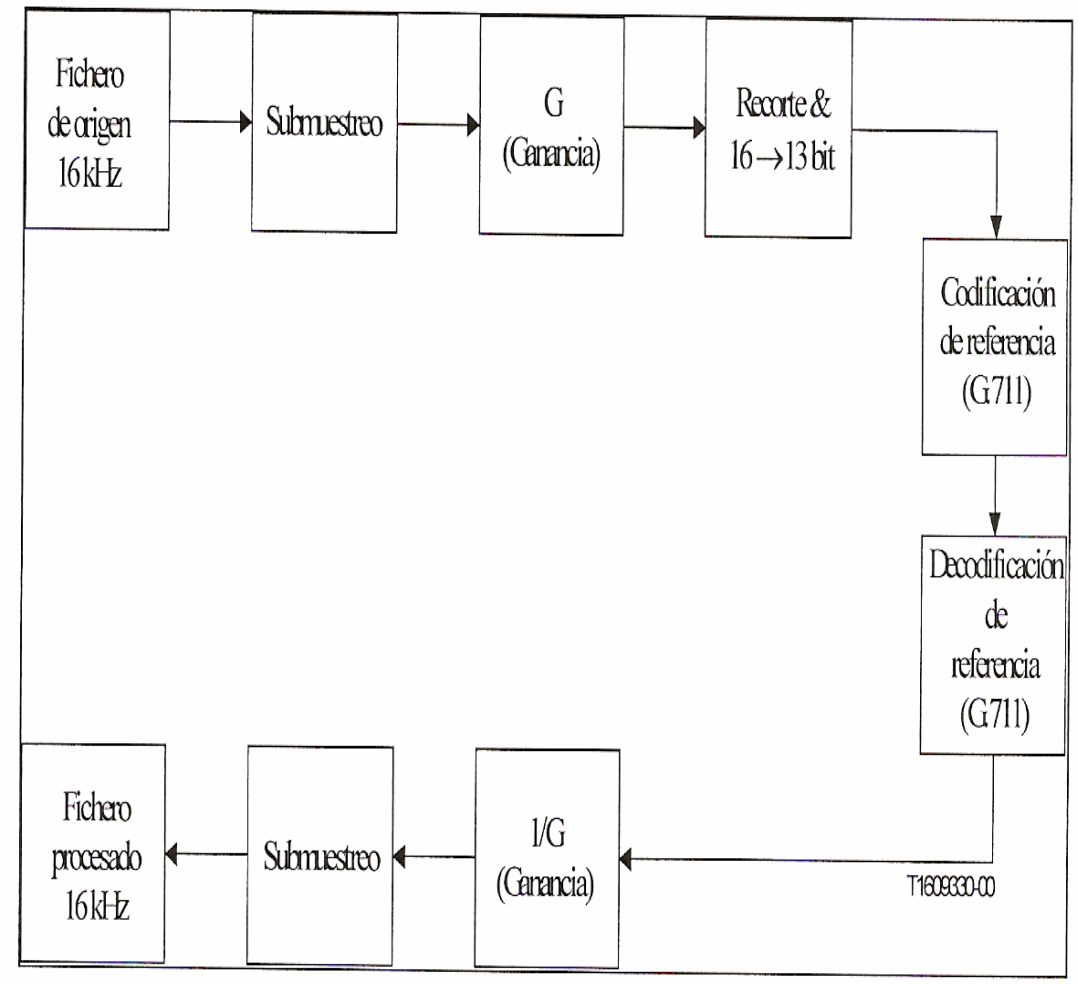


Figura 3.28 Procesamiento G.711 sin CNG

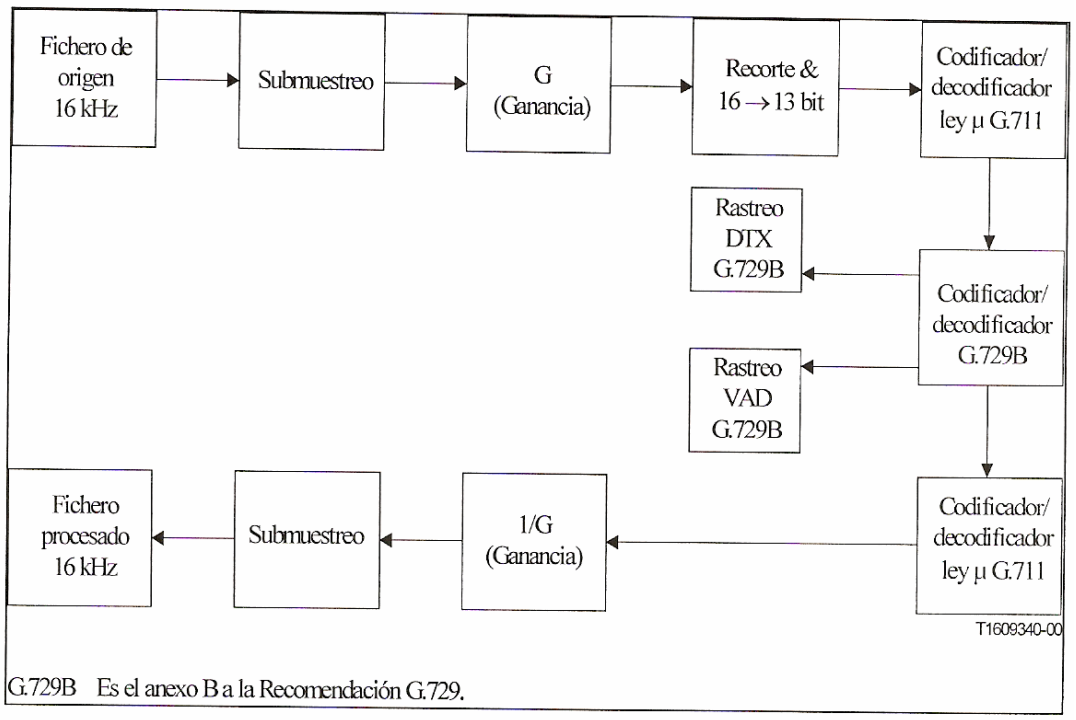


Figura 3.29 Procesamiento G.729B para obtener ficheros de rastreo VAD/DTX

El "Codec" G.711 con ruido de confort se obtuvo utilizando el procedimiento de la Figura 3.30. El fichero de origen fue submuestreado y ajustado en nivel por una ganancia G y a continuación codificado por la combinación del códec G.711 y el algoritmo CNG. Los datos de entrada se pusieron en memoria intermedia en tramas de 10 ms. La codificación de trama del algoritmo CNG se alineó con el comienzo del fichero vocal a fin de "sincronizarse" con el tramado correspondiente a los ficheros de rastreo VAD y DTX. Sobre la base de tramas de 10 ms, los ficheros de rastreo VAD y DTX se utilizaron para controlar el funcionamiento del algoritmo CNG.

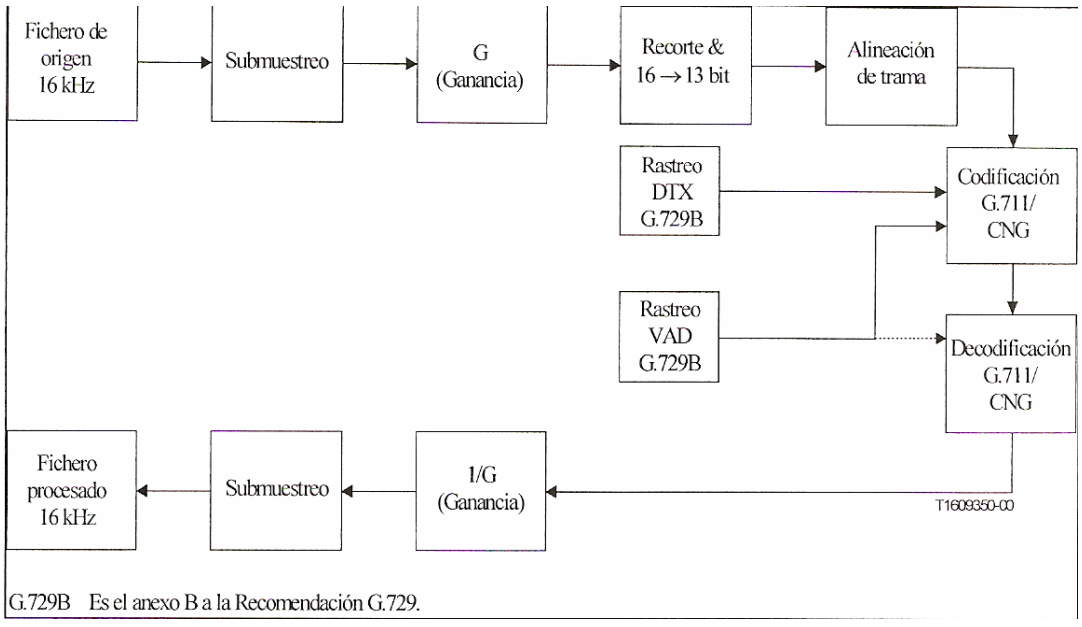


Figura 3.30 Procesamiento G.700 con CNG

Para tramas vocales activa, se utilizó G.711 para procesar la trama de datos de entrada. Para tramas inactivas, se empleó el algoritmo CNG. La bandera DTX controló la actualización de los parámetros CNG. En el decodificador, la bandera VAD se utilizó para indicar si la trama en curso era señal vocal activa o inactiva.

Se aplicó entonces una ganancia complementaria 1/G (para producir un nivel de audición constante) y el resultado se sobremuestreó y almacenó como "fichero procesado"

Los resultados de este experimento ACR con ruido revelaron que, en todos los casos de interés, el códec G.711 con el algoritmo CNG de prueba actúa de manera equivalente al códec G.711 sin VAD/CNG. Se incluye aquí el caso de un fondo en calma y también los casos de fondo ruidoso (ruido de conversación confusa, de tráfico, de oficina y de la calle).

3.6.5.- Ejemplo de Solución.

Se describe en esta subcláusula un esquema de generación de ruido de confort utilizando el formato de cabida útil de ruido de confort descrito en este artículo, que se utilizó en la evaluación descrita anteriormente.

3.6.5.1.- Descripción del Algoritmo.

3.6.5.1.1 Codificador.

El codificador debe ser llamado en cada trama por el programa llamante. Para tramas de voz activa, la señal de entrada es procesada previamente y las memorias intermedias internas se actualizan antes de volver. Para tramas inactivas, se actualizan las estimaciones de la energía de ruido de fondo y el contenido espectral

En caso de una trama SID, los parámetros estimados se cuantifican y empaquetan en la memoria intermedia de canal para su transmisión al decodificador.

La velocidad de actualización del SID fue determinada por el DTX del anexo 8/G.729 [5]. Los detalles del codificador CNG figuran en las subcláusulas siguientes.

3.6.5.1.1.1.- Procesamiento Previo.

La señal de entrada es procesada previamente por un filtro IIR paso alto de primer orden para suprimir cualquier componente de baja frecuencia no deseada. El filtro paso alto viene dado por:

$$H(z) = \frac{1 - z^{-1}}{1 - (127/128)z^{-1}}$$

3.6.5.1.1.2.- Análisis de Autocorrelación.

Los coeficientes de autocorrelación normalizados r_m y la energía de trama E se calculan sobre la base de la señal previamente procesada presentada en una ventana asimétrica de 25 ms. Para una velocidad de muestreo de 8,0 kHz, la ventana viene dada por:

$$w(n) = \begin{cases} 0{,}54 - 0{,}46\cos\left(\dfrac{2\pi n}{339}\right) & n = 0, 1, \ldots, 169 \\ \cos\left(\dfrac{2\pi(n-170)}{119}\right) & n = 170, 171, \ldots, 199 \end{cases}$$

Las medias móviles de los coeficientes de autocorrelación normalizados y la energía de trama se calculan entonces para la i-ésima trama por las fórmulas:

$$\bar{r}_m(i) = \bar{r}_m(i-1)\cdot\beta_1 + \bar{r}_m(i)\cdot(1{,}0-\beta_1) \qquad m = 1, 2, \ldots, M$$
$$\overline{LE}(i) = \overline{LE}(i-1)\cdot\beta_2 + \overline{LE}(i)\cdot(1{,}0-\beta_2)$$

donde LE es el logaritmo en base 2 de la energía de trama, y M es el orden del modelo. β1 y β2 son constantes dependientes del tamaño de trama. Si el tamaño de trama es menor o igual que 7,5 ms, β1 y β2 se fijan a 0,8, o en otro caso se fijan a 0,6. Las medias se reponen a los valores de trama vigentes si la trama anterior era de señal vocal activa.

3.6.5.1.1.3.- Cálculo de los Coeficientes de Reflexión.

El error cuadrático medio entre los coeficientes de autocorrelación instantáneos y normalizados medios se calcula por la ecuación:

$$d = \frac{1}{M}\sum_{m=1}^{M}\left(\bar{r}_m(i) - r_m(i)\right)^2$$

Si d es menor que un umbral adaptativo Th y la última trama era inactiva, se utilizan los coeficientes promediados $r_m(i)$ para el cálculo de los coeficientes de reflexión; de otro modo, se utilizan los coeficientes instantáneos $r_m(i)$. El umbral Th se determina cada trama de acuerdo con el algoritmo siguiente:

```
if (PrevVad == 1)
        Th = 0.0
else
Th += 0.2857*(FRAME_SIZE/SAMPLlNG_RATE)
        if (Th > 0.06)
                Th = 0.06
        end
end
```

Los coeficientes de reflexión km (i) se calculan a partir de los coeficientes de autocorrelación seleccionados utilizando el algoritmo de Levinson-Durbin.

3.6.5.1.1.4 Cuantificación.

Para las tramas del descriptor de inserción de silencios (SID, Silence Insertion Descriptor), se cuantifican y empaquetan la energía LE(i) y los coeficientes de reflexión km(i) con arreglo al formato de cabida útil especificado.

3.6.5.1.2 Decodificador.

El decodificador produce ruido de confort haciendo pasar una excitación de ruido blanco escalada a través de un filtro de síntesis de predicción lineal. Los detalles siguen en las subcláusulas siguientes.

3.6.5.1.2.1.- Actualización de Parámetros.

Los coeficientes de reflexión de la última trama SID recibida se utilizan en la trama en curso. Designemos por LE_{SID} los últimos parámetros de ruido de confort recibidos, donde la energía se ha convertido de dBov a logaritmo en base 2. La energía utilizada en la trama en curso viene dada por

$$LE(i) = LE(i-1)\cdot\alpha + LE_{SID}\cdot(1{,}0-\alpha)$$

donde α = 0,9. Este procedimiento de alisamiento se aplica para evitar cambios bruscos de la energía de la señal en el ruido de confort.

3.6.5.1.2.2.- Generación de la Excitación.

Se utiliza un generador de número aleatorio con una distribución gaussiana para producir la secuencia Rn que es escalada por el factor η a la energía correcta según la ecuación:

$$\eta = \sqrt{\frac{E(i)\cdot\prod_{m=1}^{M}\left(1{,}0-\hat{k}(N_m)^2\right)}{\frac{1}{L}\cdot\sum_{j=0}^{L-1}Rn(j)^2}}$$

donde L es la longitud de la excitación, y E(i) es la energía de trama.
Se utiliza una aproximación constante para el denominador de la ecuación citada a fin de evitar la operación producto escalar y reducir la complejidad.

3.6.5.1.2.3.- Síntesis de LP.

Los coeficientes de reflexión se convierten en coeficientes de predicción lineal para su utilización en el filtro de síntesis de predicción lineal (IP, linear prediction) aplicando la recursión siguiente [6]:

$$a_i^{(i)} = -\hat{k}_i(N_i)$$
$$a_j^{(i)} = a_j^{(i-1)} + \hat{k}_i(N_i)a_{i-j}^{(i-1)} \qquad 1 \le j \le i-1$$

que se resuelven para i = 1, 2, ... , M, Y con el conjunto final definido como:

$$\alpha_j = a_j^{(p)} \qquad 1 \le j \le M$$

El filtro de síntesis de predicción lineal se define como:

$$\frac{1}{A(z)} = \frac{1}{1 - \sum_{j=1}^{M} \alpha_j z^{-j}}$$

La excitación escalada se pasa a través del filtro para producir el ruido de confort final. La longitud de la excitación L es, en general, igual a la longitud de trama. Sin embargo, para la primera trama inactiva que sigue a una trama activa, L es igual a la longitud de trama más el orden del modelo (M). En este caso, se ignoran las primeras muestras de salida M del filtro de síntesis.

3.6.5.1.2.4 Retardo

No hay retardo inherente en el algoritmo de ruido de confort.

3.6.5.1.2.5 Complejidad

El algoritmo se ha implementado en punto fijo de 16 bits utilizando la biblioteca de herramientas de soporte lógico de la UIT. La memoria y la utilización de recursos a diferentes tamaños de tramas que operan a una velocidad de muestreo de 8,0 kHz y un modelo todos polos de orden 10 se resumen en la tabla siguiente. Los WMOPS (millones ponderados de operaciones por segundo) se obtienen utilizando el contador de operaciones dentro de la biblioteca y representa el caso más desfavorable. La ROM es el tamaño estimado de un DSP de punto fijo

Tamaño de trama	RAM (palabras)	ROM (palabras)	WMOPS
5 ms	650	1300	1,1
10 ms	690	1300	0,66
20 ms	760	1300	0,47
Necesidades de recursos CNG para un modelo de décimo orden			

3.6.5.3 Configuración Probada.

El algoritmo probado se especifica en la tabla siguiente:

Parámetro	Probado
Velocidad de muestreo	8,0 kHz
Tamaño de trama	10 ms
Orden del modelo	10
Retardo de indagación	5 ms

Se añadió una indagación de 5 ms retardando la entrada al códec vocal acompañante (G.711) como se aprecia en la figura 3.31. La indagación se introdujo para ajustar adecuadamente la utilización del algoritmo VAD del anexo 8/G.729 al ejemplo de solución CNG. El retardo de indagación puede evitarse en la práctica añadiendo un tiempo de retención extra al algoritmo VAD del Anexo 8/G.729.

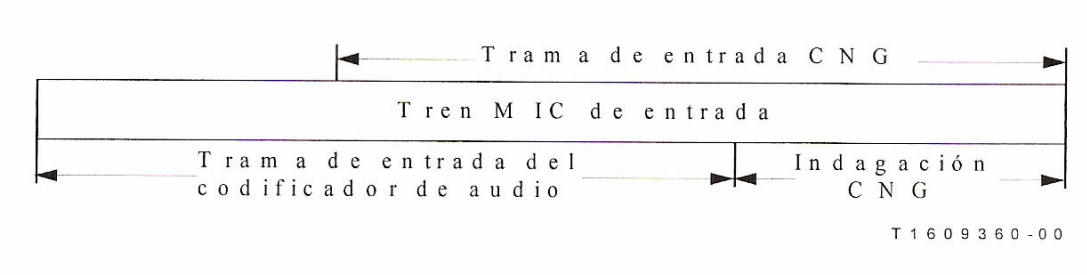


Figura 3.31 Indagación CNG durante la prueba

Referencias:

[1] Recomendación CCITT G.726 (1990), Modulación por impulsos codificados diferencial adaptativa (MICOA) a 40, 32, 24, 16 kbit/s.

[2] Recomendación CCITT G.727 (1990), Modulación por impulsos codificados diferencial adaptativa (MICOA) jerarquizada con 5, 4, 3 Y 2 bits/muestra.

[3] Recomendación CCITT G.728 (1992), Codificación de señales vocales a 16 kbits/s utilizando predicción lineal con excitación por código de bajo retardo.

[4] Recomendación CCITT G.722 (1988), Codificación de audio de 7 kHz dentro de 64 kbit/s.

[5] Recomendación UIT-T G.729 Anexo B (1996), Esquema de compresión de silencios para la Recomendación G.729, optimizado para terminales conformes a la Recomendación V.70.

[6] RABINER (L.R.), SCHAFER (R.W.): Digital processing of speech signals, Prentice-Hall, 1978.

[7] Recomendación UIT-T G.191 (1996), Herramientas de soporte lógico para la normalización de la codificación de señales vocales y de audio

3.7 Recomendación G.723.1

CODEC DE VOZ DE DOBLE VELOCIDAD PARA LA TRANSMISIÓN EN COMUNICACIONES MULTIMEDlOS A 5,3 Y 6,3 kbit/s
(Ginebra, 1996).

3.7.1 Introducción.

3. 7.1.1.- Alcance.

Esta Recomendación especifica una representación de "Codec" (codificador-decodificador) que se puede utilizar para comprimir la voz u otras señales audio componentes de servicios multimedios a velocidad binaria muy baja. Al diseñar este Códec, la principal aplicación considerada fue la telefonía visual a velocidad binaria muy baja como parte de la familia general de normas H.324.

3.7.1.2.- Velocidades Binarias.

Este "Codec" tiene asociadas dos velocidades binarias. Se trata de 5,3 y 6,3 kbitls. La velocidad más alta tiene mucha mejor calidad. La velocidad más baja da una buena calidad y proporciona a los diseñadores de sistema más flexibilidad. Ambas velocidades son una parte obligatoria del codificador y del decodificador. Se puede conmutar entre ambas velocidades en cualquier frontera de trama de 30 ms. También se puede utilizar el funcionamiento con velocidad variable mediante la transmisión discontinua y el relleno de ruido durante los intervalos sin voz.

3.7.1.3.- Señales de Entrada Posibles.

El "Codec" se optimizó de forma que represente la voz con gran calidad a las velocidades mencionadas y con una complejidad restringida. La música y otras señales de audio no se representan con la misma fidelidad que la voz, pero con este "Codec" se pueden comprimir y descomprimir.

3.7. 1.4. - Retardo.

Este "Codec" codifica la voz u otras señales audio en tramas de 30 ms. Además, tiene un preanálisis de 7,5 ms, lo que resulta en un retardo algorítmico total de 37,5 ms. Todos los demás retardos en la implementación y el funcionamiento de este códec se deben a:

- El tiempo real del procesamiento de los datos en el codificador y el decodificador;
- El tiempo de transmisión por el enlace de comunicaciones;
- El retardo adicional de la memoria intermedia para el protocolo de multiplexación.

3.7.1.5.- Descripción del "Codec" de Voz.

La descripción del algoritmo de codificación de la voz en esta Recomendación se hace en términos de operaciones matemáticas de coma fija y exactitud de bits. El código C de ANSI que se indica en la cláusula 5, y que constituye una parte integrante de esta Recomendación, refleja este enfoque de descripción de coma fija y exactitud de bits.

Las descripciones matemáticas del codificador y del decodificador, que aparecen en las cláusulas 2 y 3, respectivamente, pueden tener realizaciones diversas, que quizá conduzcan a una realización de "Codec" que no cumple las disposiciones de esta Recomendación.

Por consiguiente, la descripción del algoritmo del código C de la cláusula 5 tendrá precedencia sobre las descripciones matemáticas de las cláusulas 2 y 3 en el caso de que se aparezcan discrepancias. Puede solicitarse a la UIT una lista no exhaustiva de secuencias de prueba para utilizar junto con el código C.

3.7.2.- Principios del Codificador.

3.7.2.1.- Descripción General.

Este "Codec" está diseñado para el funcionamiento con una señal digital obtenida filtrando primero la entrada analógica con la anchura de banda de telefonía (Recomendación G.712), muestreándola luego a 8000 Hz y convirtiéndola a señal MIC lineal de 16 bit para su entrada en el codificador.

Habrá que convertir la salida del decodificador a señal analógica mediante medios similares.

Otras características entrada/salida, como las especificadas en la Recomendación G.711 para los datos MIC a 64 kbit/s, se convertirán a MIC lineal a 16 bit antes de la codificación o de MIC lineal a 16 bit al formato apropiado después de la decodificación. En esta Recomendación se define el tren de bits que va del codificador hasta el decodificador.

El "Codec" se basa en los principios de la codificación de predicción lineal análisis por síntesis, y trata de hacer mínima una señal de error ponderada perceptualmente. El codificador funciona con bloques (tramas) de 240 muestras cada uno. Ello equivale a 30 ms a una velocidad de muestreo de 8 kHz.

Cada bloque se pasa primero por un filtro paso alto para suprimir la componente continua, y luego se divide en cuatro subtramas de 60 muestras cada una. Para cada subtrama, se calcula un filtro de códec de predicción lineal (IPC, linear predietian eader) de décimo orden utilizando la señal de entrada no procesada. El filtro IPC para la última subtrama se cuantifica con un cuantificador vectorial de división predictiva (PSVQ, predietive split vectar quantizer). Los coeficientes IPC no cuantificados se utilizan para construir el filtro de ponderación perceptual de corto plazo, que se utiliza para filtrar toda la trama y obtener la señal de voz ponderada perceptualmente.

Para cada dos subtramas (120 muestras), se calcula el periodo de tono en bucle abierto LOL mediante la señal vocal ponderada. Esta estimación del tono se realiza con bloques de 120 muestras. El periodo de tono se busca en la gama de 18 a 142 muestras.

A partir de ese punto, la voz se procesa a 60 muestras por subtramas. Utilizando el periodo de tono estimado calculado anteriormente, se construye un filtro de conformación de ruido armónico. La combinación del filtro de síntesis IPC, el filtro de

ponderación perceptual formante y el filtro de conformación del ruido armónico se utiliza para crear una respuesta de impulso. La respuesta del impulso se utiliza para los cálculos posteriores.

Con la estimación del periodo de tono, LOL y la respuesta de impulso, se calcula un predictor de tono en bucle cerrado. Se utiliza un predictor de tono de quinto orden. El periodo de tono se calcula como un valor diferencial pequeño respecto de la estimación de tono en bucle abierto. La contribución del predictor de tono se resta del vector objetivo inicial. Tanto el periodo de tono como el valor diferencial se transmiten al decodificador.

Por último, se aproxima la componente no periódica de la excitación. Para la velocidad alta, se utiliza la excitación del tipo cuantificación multiimpulso de máxima verosimilitud (MP-MLQ), y para la velocidad baja, una predicción lineal con excitación por tabla de códigos algebraicos (ACEIP). Lo anterior se muestra en la tabla siguiente:

File: LBCCODER.C	Procedure: main ()	Lee tramas de entrada de 240 muestras
File: CODER.C	Procedure: Coder ()	Ejecuta la división en subtramas

3.7.2.2.- Formador de Trama.

El Códec procesa la voz mediante el almacenamiento en memoria intermedia de muestras vocales consecutivas, y[n], en tramas de 240 muestras, s[n]. Para el cálculo de la estimación del tono, cada trama se divide en dos partes de 120 muestras. Cada parte se divide a su vez en dos, de manera que cada trama queda dividida en cuatro subtramas de 60 muestras cada una.

3.8.- Recomendación G.729.

CODIFICADOR DE LA VOZ MEDIANTE PREDICCIÓN LINEAL CON EXCITACIÓN POR CÓDIGO ALGEBRÁICO DE ESTRUCTURA CONJUGADA A 8 kbit/s DE COMPLEJIDAD REDUCIDA.
(Ginebra, 1996).

3.8.1 Introducción.

El presente artículo proporciona la descripción de alto nivel de una versión de complejidad reducida del "Codec" de señales vocales G.729. Esta versión puede interfuncionar en trenes de bits con la versión completa, es decir, puede utilizarse un codificador de complejidad reducida con una realización completa del decodificador y viceversa. No obstante, los realizadores del códec definido en este anexo deben ser conscientes de que la calidad de funcionamiento de este códec puede no ser tan buena como la realización completa de la Recomendación G.729 en ciertas circunstancias.

La versión de complejidad reducida del "Codec" ha sido preparada para aplicaciones de voz y datos simultáneos en multimedios, aunque la utilización del códec no se limita a tales aplicaciones.

La descripción del "Codec" es similar a la de la realización completa de la Recomendación G.729. Este atículo describe los cambios introducidos en la realización completa con el fin de reducir la complejidad del algoritmo del códec.

3.8.2.- Descripción General del Codificador.

La descripción general del algoritmo de codificación/decodificación es semejante a la de la versión completa. Tiene también el mismo retardo (trama vocal de 10 ms y preanálisis de 5 ms). Los principales cambios algorítmicos con respecto a la versión completa de la Recomendación G.729 son:

- El filtro de ponderación perceptual utiliza los parámetros de filtro de predicción lineal (IP) cuantificados y viene dado por W(z) = A(z)/A(z/y) con un valor fijo de y = 0,75.
- El análisis de tono en bucle abierto se simplifica mediante un diezmado al tiempo que se calculan las correlaciones de la señal vocal ponderada.
- El cálculo de la respuesta de impulsos del filtro de síntesis ponderado W(z)/A(z), el cálculo de la señal objetivo y la actualización de los estados del filtro se simplifican al reducirse W(z)/A(z) a 1/A(z/y).
- La búsqueda de la tabla de códigos adaptativos se simplifica. La búsqueda maximiza la correlación entre la excitación pasada y la señal objetivo filtrada hacia atrás (no se considera la energía de la excitación anterior filtrada).
- Se simplifica la búsqueda de la tabla de códigos algebraicos fijos. En vez de una búsqueda enfocada a bucles encajados se sigue un método de búsqueda en árbol iterativa, en profundidad primeramente.
- En el decodificador se simplifica el postfiltro de armónicos utilizando solamente retardos enteros.

Estas características se pueden sintetizar como sigue:

Nombre de subprograma G.729	Nombre de subprograma G.729A
Coder_1d8k ( )	Coder_1d8a ( )
Decod_1d8k ( )	Decod_1d8a ()
Pitch_01 ()	Pitch_01_fast ( )
Pitch_fr3 ( )	Pitch_fr3_fast ( )
ACEIP _ Codebook ( )	ACEIP _Code_A ()
Post ( )	Post-Filter ( )
Resumen de los Principales Subprogramas que se han Modificado.	

La descripción del "Codec" de señales vocales de complejidad reducida se hace en términos de operaciones matemáticas de coma fija y exactitud de bits. El Código C de ANSI indicado. Las descripciones matemáticas del codificador y del decodificador pueden aplicarse también de varias otras maneras, dando lugar quizá a aplicaciones del "Codec". La descripción del algoritmo del Código C ANSI prevalecerá en caso de discrepancia con cualquier otra descripción matemática contenida. Sin llegar a ser exhaustivo, puede obtenerse de la UIT un juego de señales de prueba utilizables al

aplicar el Código C de ANSI. Los convenios de notación son los mismos expresados en G.729.

3.8.3 Funciones del Codificador.

Se hace referencia al cuerpo principal de la Recomendación en la mayor parte de esta subcláusula, excepto en las partes en que se han realizado simplificaciones de algoritmo. Las principales funciones del codificador son:

- Preprocesamiento
- Analisis y cuantificación de la predicción lineal
  - a) Ventanización y cálculo de la autocorrelación
  - b) Algoritmo de Levinson-Durbin
  - c) Conversión de LP a LSP
  - d) Cuantificación de los coeficientes LSP
  - e) Interpolación de los coeficientes LSP
  - f) Conversión de LSP a LP
- Ponderación perceptual
- Análisis de tono de bucle abierto
- Cálculo de la respuesta de impulso
- Cálculo de la señal objetivo
- Búsqueda de la tabla de códigos adaptativos
  - a) Generación del vector de tabla de códigos adaptativos
  - b) Cálculo de palabras de código para retardos de tabla de códigos adaptativos
  - c) Cálculo de la ganancia de tabla de códigos adaptativos
- Tabla de códigos fijos. Estructura y búsqueda
  - a) Procedimiento de búsqueda de la tabla de códigos fijos
  - b) Cálculo de la palabra de código de tabla de códigos fijos
- Cuantificación de las ganancias
- Actualización de la memoria

3.8.4 Funciones del decodificador

Se utilizan los parámetros decodificados para calcular la señal vocal reconstruida. Esta señal reconstruida se mejora mediante una operación de postprocesamiento consistente en un postfiltro, un filtro de paso alto y un escalamiento ascendente. El único cambio en el decodificador es en el postfiltro.

3.8.5 Descripción Binaria Exacta del Codificador de Complejidad Reducida CS-ACEIP.

El codificador de complejidad reducida CS-ACEIP se simula en el código C de ANSI utilizando el mismo conjunto de operadores básicos de coma fija definido en el Cuadro G.729.

El empleo de soporte lógico de simulación es el mismo que en G.729, al igual que la organización del soporte lógico de simulación.

3.9 Red digital de servicios integrados (RDSI)

Con el gran salto tecnológico de las últimas décadas, el incremento en el uso de técnicas digitales y el crecimiento enorme de los volúmenes de información que se almacenan y se trasmiten, surge la conveniencia económica y la posibilidad técnica de crear una red nueva, flexible, de gran capacidad de transporte, que evolucione a partir de las redes existentes aprovechando su gran penetración mundial (como es el caso de la red telefónica) y sea capaz de integrarlas y adaptarse dinámicamente a la incorporación de futuros servicios, como lo muestra la figura 3.32

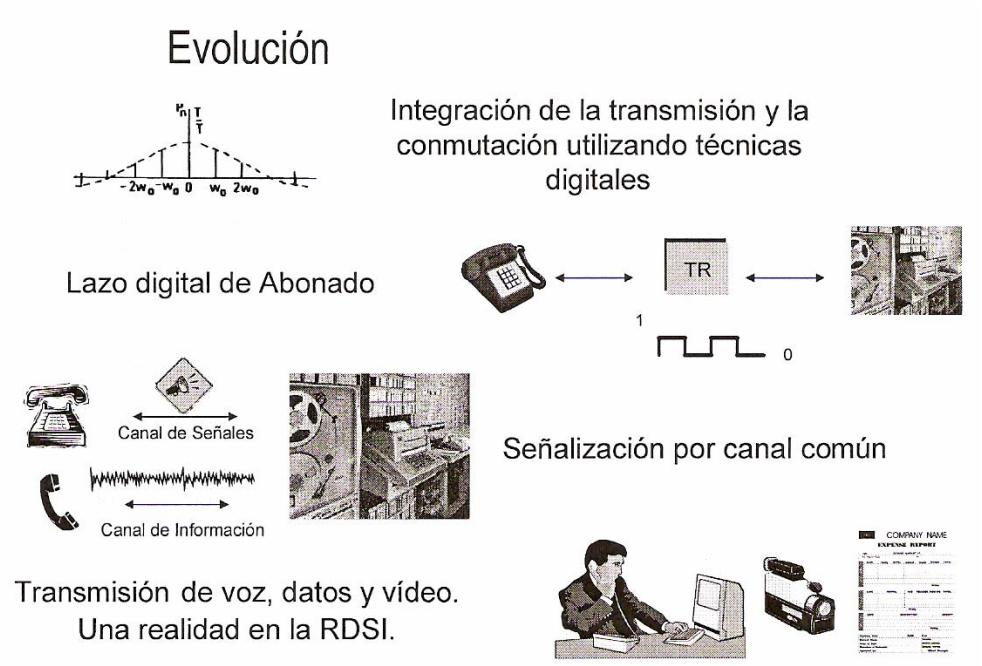


Figura 3.32 Evolución de las redes de comunicación

Se han estudiado diversas posibilidades de integración, introduciendo voz en las redes de datos, o datos en la red telefónica, aunque debido a los diferentes propósitos con que fueron diseñadas estas redes, hacen pensar en la necesidad de aprovechar al máximo sus posibilidades actuales, pero ir gradualmente tendiendo hacia una RED DIGITAL DE SERVICIOS INTEGRADOS (RDSI).

La RDSI es un sistema digital de comunicaciones, que evoluciona partiendo de la red telefónica pública conmutada. Una vez en operación, ofrecerá conexiones normalizadas entre puntos extremos y soporte simultáneo para servicios de voz y datos; todo a través de un acceso único.

La RDSI beneficiará a usuarios y prestadores de servicios por igual, debido a las economías que es posible obtener del uso de la tecnología digital.

La RDSI puede definirse a partir de dos elementos: Los servicios que presta y los métodos en los que se apoya para brindarlos. Este último punto comprende, en realidad, dos aspectos distintos: la tecnología con que se construye el sistema y la estructura con que se organiza.

De acuerdo con la recomendación 1.120 de CCITT la principal característica de la ROSI es el soporte de un amplio rango de servicios, incluyendo voz y datos, para los que el usuario tiene acceso mediante un conjunto limitado de interfaces normalizadas y de propósito múltiple.

Estos servicios incluyen aplicaciones para conexiones digitales conmutadas y no conmutadas. En el primer caso puede tratarse de conmutación de circuitos o paquetes. Los servicios no conmutados se proveen utilizando líneas dedicadas.

La RDSI tiene la capacidad de asegurar las características de servicio y las funciones de mantenimiento y gestión de la red. En la especificación del acceso a la ROSI se utiliza una estructura estratificada de protocolos.

La telefonía pública y las redes de telecomunicaciones en general, han basado su evolución en la asimilación de la tecnología digital. Las principales modificaciones que esta tecnología ha permitido son:

- La integración de las funciones de transmisión y conmutación .
- El lazo digital de abonado .
- La señalización por canal común.

En una red telefónica analógica, los sistemas de transmisión y conmutación se diseñaban y administraban por grupos funcionalmente distintos. En las compañías operadoras estos sistemas se conocían como planta externa y planta interna, respectivamente. Las líneas de voz que llegaban a la central se modulaban y multicanalizaban para transmitirse por FDM.

En cada centro de conmutación la portadora de FDM debía atravesar por el procesamiento inverso antes de pasar por una etapa de conmutación espacial. Después de la conmutación las señales volvían a multicanalizarse y modularse para su transmisión. Este proceso que se repetía en cada central de conmutación, tenía como consecuencia una acumulación de ruido y costos.

Cuando la transmisión y la conmutación son digitales, puede llevarse a cabo la integración de estas funciones. Las señales de voz son digitalizadas usando modulación por pulsos codificados (PCM) y multicanalizadas por división en tiempo (TDM).

Los conmutadores digitales por división en tiempo, dispuestos sobre la trayectoria de comunicación, pueden manejar las señales individuales sin necesidad de decodificarlas.

Tradicionalmente, en una red telefónica analógica, los sistemas de transmisión y conmutación se diseñaban y administraban por grupos funcionalmente distintos. En las compañías operadoras estos sistemas se conocían como planta externa y planta interna, respectivamente. Las líneas de voz que llegaban a la central se multicanalizaban para transmitirse por un canal FDM.

En cada centro de conmutación la portadora de FDM debía demodularse antes de pasar por una etapa de conmutación espacial. Después de la conmutación las señales volvían a multicanalizarse para su transmisión. Este proceso que se repetía en cada central de conmutación, tenía como consecuencia una acumulación de ruido y costos.

Cuando la transmisión y la conmutación son digitales, puede llevarse a cabo la integración de estas funciones. Las señales de voz son digitalizadas usando modulación por pulsos codificados (PCM) y multicanalizadas por división en tiempo (TDM). Los conmutadores digitales por división en tiempo, dispuestos sobre la trayectoria de comunicación, pueden manejar las señales individuales sin necesidad de decodificarlas.

Hay que observar que, tratándose de señales PCM-TDM, se pueden utilizar técnicas de conmutación espacial (como en el caso de las señales analógicas) mediante dispositivos como las matrices de conmutación (ttCrossbar). Por otro lado, también se pueden usar técnicas de conmutación temporal, mediante dispositivos conocidos como "intercambiadores de ranuras".

En la práctica, los sistemas se construyen como una combinación de ambas técnicas ya que la conmutación temporal es muy barata, pero está limitada a una cantidad muy pequeña de ranuras, debido a las velocidades de acceso a la memoria digital. En contraste, la conmutación espacial puede ser más cara pero no tiene restricciones en el tamaño de las tramas que se manejan. Luego, la conmutación espacio-temporal es un compromiso entre ambas soluciones. El ESS5 de AT&T, por ejemplo, es un sistema TSSSST, diseñado para manejar alrededor de cien mil llamadas simultáneas.

Llevar el enlace digital hasta el domicilio del abonado o suscriptor, es una parte esencial de la evolución de la RDI. No es suficiente que las funciones de transmisión y conmutación sean digitales. Para ofrecer el amplio rango de servicios planeados para la RDI y la RDSI, el enlace entre el abonado y su oficina de adscripción, conocido como lazo local o lazo de abonado, debe ser digital.

La manera más simple de construir este lazo digital, sería tendiendo dos pares de cables trenzados entre la oficina y el abonado, uno para cada dirección de la comunicación. Sin embargo, la red telefónica mundial instalada basa su funcionamiento en un solo par entre el abonado y la oficina. Por razones económicas, en general no puede ofrecerse el nuevo lazo de abonado pensando en un par de cables por cada dirección.

Llevar el enlace digital hasta el domicilio del abonado o suscriptor, es una parte esencial de la evolución de la ROS!. No es suficiente que las funciones de transmisión y conmutación sean digitales. Para ofrecer el amplio rango de servicios planeados, el enlace entre el abonado y su oficina de adscripción, conocido como lazo local o lazo de abonado, debe ser digital.

La manera más simple de construir este lazo digital, sería tendiendo dos pares de cables trenzados entre la oficina y el abonado, uno para cada dirección de la comunicación. Sin embargo, la red telefónica mundial instalada basa su funcionamiento en un solo par entre el abonado y la oficina. Por razones económicas, en general no puede ofrecerse el nuevo lazo de abonado pensando en un par de cables por cada dirección.

Se sabe que, para una compañía telefónica, sus cables representan aproximadamente la mitad de sus activos contables. Esta es la razón por la que el lazo de suscriptor no puede volverse a cablear para satisfacer las necesidades que plantea la ROS!. Será necesario buscar soluciones técnicas alternativas:

1. Cancelación de eco.
2. Separación de frecuencias.
3. Transmisión alternada en ranuras de tiempo.

El problema de la RDSI (al menos en su etapa de banda angosta), es que esta decisión impacta directamente sobre el costo de los aparatos del lado usuario y, por otro lado, nunca se especifico a cargo de quién correrían estos gastos

En la red telefónica analógica, la señalización se lleva a cabo usando los mismos medios y canales por donde viaja la información del usuario, lo que hace imposible el intercambio de señales durante la fase de comunicación. Esta limitación puede superarse al adoptar un modo de señalización que usa mensajes fuera de banda, es decir, donde las señales de control viajan por un canal distinto de aquel por donde viaja la información de usuario.

La señalización por canal común es más flexible y poderosa que la señalización dentro de banda y responde eficazmente a las necesidades de la ROS!. Actualmente se utiliza el Sistema de Señalización Número 7 (SS7), elaborado por CCITT. SS7 es el mecanismo que provee el control interno y la inteligencia esencial para el manejo de RDSI.

El término señalización designa el intercambio de señales entre las distintas entidades funcionales de la red, necesario para establecer y terminar las comunicaciones y el manejo de los recursos.

Mientras que la información intercambiada entre los usuarios se transporta a través de la red de manera transparente, la información de señalización implica un tiempo de procesamiento en cada nodo de la red.

Por tanto la señalización debe considerarse como el sistema nervioso de la red de telecomunicaciones y su desempeño tiene una relación muy estrecha con la diversidad y la calidad de los servicios que se ofrecen.

En la red telefónica analógica, la señalización se lleva a cabo usando los mismos medios y canales por donde viaja la información del usuario, lo que hace imposible el intercambio de señales durante la fase de comunicación. Esta limitación puede superarse al adoptar un modo de señalización que usa mensajes fuera de banda, es decir, donde las señales de control viajan por un canal distinto de aquel por donde viaja la información de usuario.

Se puede decir que la señalización ha pasado por varias etapas de perfeccionamiento:

En banda -> fuera de banda -> de canal común.

La señalización por canal común, es del tipo "fuera de banda", pero agrega características que la hacen más eficiente y confiable. Por lo general, un solo canal de señalización puede servir para administrar varios canales de aplicación. Por otro lado, la información de señalización tiene una estadística de tráfico que se acomoda mejor sobre una red de conmutación de paquetes.

En consecuencia, es más flexible y poderosa que la señalización dentro de banda y responde eficazmente a las necesidades de la RDSI. Actualmente se utiliza el Sistema de Señalización Número 7 (SS7), elaborado por CCITT. Se trata de estandarizar las operaciones de un sistema de canal común para volverlo una norma internacional que garantice la interoperabilidad de las redes modernas, con independencia de su fabricante u operador. SS7 es el mecanismo que provee el control interno y la inteligencia esencial para el manejo de RDSI.

Aunque han sido muchos los organismos reguladores que han intervenido en los distintos aspectos de la ROSI, el cuerpo coordinador de estos esfuerzos es el Consejo Consultivo Internacional de Telegrafía y Telefonía (CCITT).

El desarrollo de la ROSI fue impulsado por un conjunto de normas propuestas por CCITT, conocidas como las recomendaciones de la serie 1. Estas recomendaciones fueron propuestas por primera vez en 1984 y revisadas en 1988; se observan en la figura 3.33

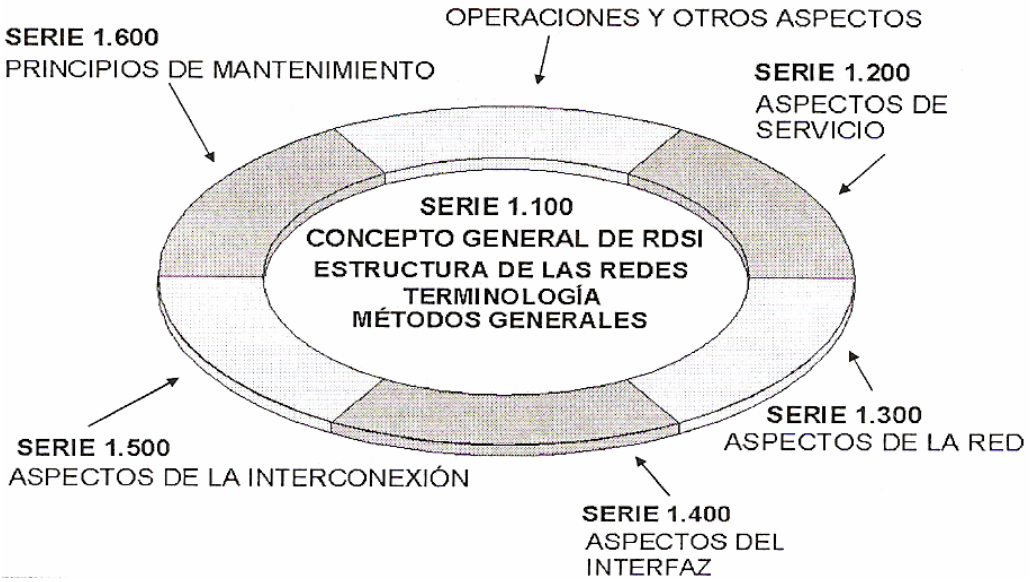


Figura 3.33 Normas

- Serie 1.100. Conceptos generales. La serie 1.100 sirve de introducción general a la RDSI. La estructura general de las recomendaciones y el glosario de términos relacionados se presentan en este documento. La recomendación 1.120 proporciona una descripción de la RDSI y de la evolución de ésta a partir de la RDI. La recomendación 1.130 presenta la terminología y conceptos que se usan en la serie 1.200 para describir los servicios específicos que se proveerán.
- Serie 1.200. Capacidades del servicio. En esta serie se definen los servicios que la ROSI ofrecerá. Un usuario potencial tiene que remitirse a ella para

decidir sí sus expectativas de servicio pueden satisfacerse abonándose a la RDSI.

- Serie 1.300. Aspectos relacionados con la red. Mientras que la serie 1.200 se centra en el usuario, en términos de los servicios que se le ofrecerán, la serie 1.300 hace hincapié en la red, desde el punto de vista de las operaciones que ésta tiene que desarrollar para cumplir su cometido.
- Serie 1.400. Interfaces usuario-red. La serie 1.400 tiene que ver con la interfaz entre el usuario y la red. Los puntos más importantes que son considerados son: las configuraciones físicas, las velocidades de transmisión y la especificación de las reglas que norman la comunicación entre los equipos de ambos lados de la interfaz.
- Serie 1.500. Interfaces para interconexión de redes.
- Serie 1.600. Principios de mantenimiento.

Con el fin de definir las características técnicas de la RDSI, se adoptó un enfoque que pudiera parecer abstracto, pero cuya importancia debe enfatizarse. De hecho no hubiera podido realizarse la integración de los servicios directamente con la definición de los equipos físicos o los interfaces usados. La coherencia de los servicios de telecomunicación, nacionales e internacionales, depende de esta medida. Por otro lado, esta coherencia tenía que ser garantizada sin imponer una rigidez excesiva sobre el desarrollo de los equipos compatibles.

Es necesario distinguir, en la interfaz usuario-red, entre los datos de señalización intercambiados y aquellos relacionados con la operación y mantenimiento del equipo de usuario. De esta consideración se desprende el modelo tridimensional que se muestra en la figura 3.34

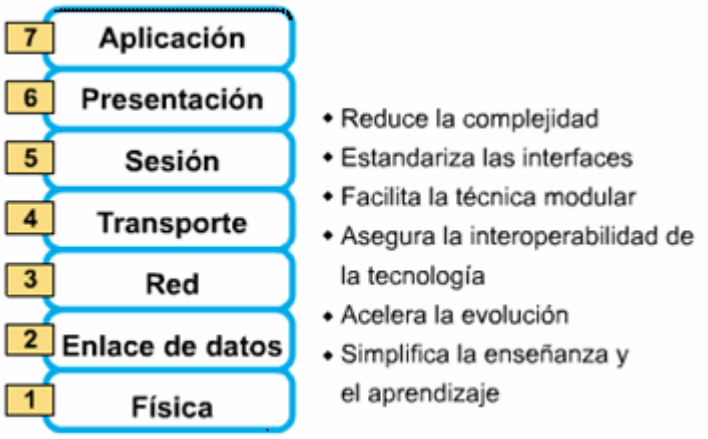


Figura 3.34 Modelo OSI

- El plano de control C: se organiza en siete niveles, relacionados con la señalización en el canal O y comprende todos los protocolos para invocación de servicios y facilidades.
- El plano de usuario U: que también se organiza en siete niveles y contiene los protocolos desarrollados para el intercambio de datos relacionados con la aplicación sobre la que se transfiere información de usuario (O, B o H).
- El plano de manejo M: que no está organizado en niveles y se relaciona con las funciones operativas de los TR2's y las terminales.

En general, los planos e y U pueden comunicarse con la entidad de manejo M usando primitivas de servicio de ésta última, que a su vez coordina las actividades en los planos e y u los cuales no se comunican directamente entre sí.

Otra manera de interpretar la operación y la relación entre los diferentes planos del modelo, puede ser analizando la secuencia de operaciones y señales intercambiadas entre el lado usuario y la red, durante las fases críticas de una aplicación. Por ejemplo, durante la fase del establecimiento, el plano C, es el encargado de gestionar con la red, los recursos que harán posible la aplicación.

De su parte, la red debe revisar sus condiciones de operación, para determinar si puede soportar los requerimientos del nuevo servicio que se le solicita. En cuyo caso elabora un perfil de la aplicación y un contrato de servicio que debe pasar hacia alguna entidad del plano M que verifique su cumplimiento, para que, una vez en operaciones, la aplicación (corriendo sobre el plano U) sea monitoreada y se cuide que no exceda sus requerimientos, para no poner en riesgo el servicio de otros usuarios

Los servicios portadores proporcionan los medios de transmisión entre usuarios, incluyendo las capacidades físicas y sus funciones de gestión.

No desarrollan operaciones de interpretación sobre el contenido de la información del usuario. Estos servicios coinciden con los niveles inferiores del Modelo OSI.

El ejemplo más común de servicio portador, es el caso de la telefonía RDSI de tipo convencional.

De acuerdo con la complejidad de un servicio y el conjunto de funciones implicadas en su solución, una RDSI debe ser capaz de ofrecer:

- Servicios portadores
- Teleservicios
- Servicios suplementarios

Los servicios portadores son resueltos por la red utilizando capacidades equivalentes a los primeros 3 niveles de OSI (e.g. telefonía convencional).

Los teleservicios incluyen algún tipo de operación asociada con los niveles superiores de OSI (videotelefonía).

Un servicio suplementario modifica alguna característica de un servicio portador o un teleservicio, sin que esto signifique la participación de un mayor número de niveles funcionales (conferencia multipartita, "follow-me').

Los teleservicios combinan funciones de transporte con funciones de procesamiento de la información. Estos emplean servicios portadores para transportar los datos, pero además, incluyen un conjunto de funciones de alto nivel, que corresponden con los niveles superiores de OSI. Mientras que los requerimientos de los servicios portadores son soportados por la red, los teleservicios incluyen capacidades de red así como de

terminal. Ejemplos de teleservicios son: el teletexto, el videotexto, el manejo de mensajes.

Para definir un servicio completamente y sin ambiguedad, ITU establece una lista de atributos que caracterizan cualquier tipo de servicio (portador o teleservicio).

Un servicio portador se define mediante tres categorías de atributos:

- De transferencia de información: modo de transferencia (circuitos o paquetes), velocidad, permanencia, simetría, configuración del enlace (punto a punto, multipunto).
- De acceso: canal de transmisión, protocolo de señalización, protocolo de transferencia de datos.
- Generales: calidad de servicio, servicios suplementarios, tarifas, etcétera.

Para caracterizar a un teleservicio es necesario agregar atributos para definir los protocolos de los niveles superiores, así como atributos generales para estos mismos.

Estos tipos de canales se agrupan en estructuras de transmisión ofrecidas al usuario como capacidades de acceso. Las estructuras definidas hasta el momento son el acceso básico y el acceso primario.

Un acceso básico consiste de dos canales B, full-dúplex de 64 kbps y un canal O a 16 kbps. La velocidad de información de esta estructura es de 144 kbps, sin embargo, debido a los bits que delimitan la trama, los bits de sincronización y algunos de control, la velocidad de tranmisión es de 192 kbps. El acceso básico se disenó para satisfacer las necesidades de usuarios pequeños.

Un acceso primario está orientado hacia los usuarios con requerimientos de capacidad superiores, tales como una oficina con un PBX digital o una LAN.
Debido a las diferencias en las jerarquías de transmisión digital usadas en distintos países, no fue posible llegar a un acuerdo sobre una velocidad de transmisión única para esta estructura.

Los Estados Unidos, Canadá y Japón utilizan una estructura de transmisión basada en 1.544 Mbps, mientras que en Europa la norma de transmisión es de 2.048 Mbps. Típicamente la estructura de 1.544 Mbps aloja 23 canales B y un canal O a 64 kbps, para el caso de 2.048 Mbps este arreglo puede contener 30 canales B mas un canal O a 64 kbps. El acceso primario también puede soportar canales H. En cualquier caso siempre habrá un acceso que contenga un canal O para señalización de control.

El canal B es un canal de usuario que puede usarse para transmitir datos digitales, voz digitalizada, o una mezcla de tráfico de baja velocidad, incluyendo datos y voz codificados a un submúltiplo de 64 kbps. Sobre un canal B pueden establecerse tres tipos de conexiones: por conmutación de circuitos, por conmutación de paquetes y semipermanente.

El canal D sirve para varios propósitos. Primero, transporta la información de señalización por canal común que controla las llamadas, sobre los canales B asociados con el interfaz de usuario. Además, el canal D puede usarse para conmutación de

paquetes o telemetría de baja velocidad, siempre que no haya información de señalización en espera.

Los canales H proporcionan velocidades de transmisión superiores. El usuario puede emplear uno de estos canales como troncal de alta velocidad, o subdividir el canal de acuerdo con sus necesidades. Algunos ejemplos de aplicación incluyen fax rápido, video, datos de alta velocidad, audio de alta fidelidad y flujos de información multicanalizados de velocidades menores.

Las interfaces de usuario se han definido por medio de puntos y grupos. Los grupos corresponden a un conjunto de funciones normalmente alojadas en un mismo equipo y son:

- TL: Terminador de línea: Se localiza en la central telefónica, realiza funciones de nivel 1 como la transmisión, alimentación, mantenimiento, activación, desactivación y supervisión.
- TR1: Terminador de red 1: Físicamente se ubica en el domicilio del abonado, agrupa funciones de nivel 1, terminación de línea, extracción de la temporización, monitoreo de la transmisión, alimentación y funciones de mantenimiento.
- TR2: Terminador de red 2: Agrupa funciones de nivel 2 y 3, conmutación, concentración, multiplexaje y puede actuar como PBX, o red de área local. Este equipo puede no existir, en la configuración más sencilla, en cuyo caso los puntos S y T coinciden.
- ET1: Equipo terminal compatible con RDSI: comprende funciones en todos los niveles del Modelo OSI.
- ET2: Equipo terminal no ROSI: requiere de un adaptador de terminal (AT) para funcionar (por ejemplo, un teléfono analógico o un terminal con interfaz RS232).

Los puntos de referencia, son puntos teóricos que separan grupos funcionales. Pueden corresponder o no, a interfaces físicamente existentes.

Varias compañías internacionales manufacturan conmutadores ROS!. Entre los sistemas más importantes se encuentran:

- El 5ESS de AT&T.
- El OMS-100 de Norte!.
- El sistema 1210 de Alcatel. El AXE-1 0 de Ericsson.
- El FETEX-150 de Fujitsu. El GX5000 de Mitel.
- El NEAX 61A de NEC.
- El EWSO de Siemens Stromberg-Carlson.

Una de las mayores limitantes que han inhibido el crecimiento de la ROSI, es la longitud del lazo local entre la oficina y el domicilio del abonado. Adtran ™ fabrica también varios tipos de extensiones para línea lAB.

La RDSI ha demostrado ser un servicio flexible y dinámico con posibilidades de uso comercial y residencial.

La actividad nacional e internacional en torno al tema, ha enseñado varias cosas:

- Primero, que la tecnología funciona y es viable. Esta era una de las mayores preocupaciones de sus diseñadores.
- Que se necesita desarrollar un mayor número de aplicaciones, para aumentar el número de usuarios y afianzar su éxito. Se sabe, al mismo tiempo, que la red tiene un potencial de aplicación muy grande.
- Que la adhesión a las normas es un aspecto crítico para el ofrecimiento universal de los servicios.

Entre las compañías que fabrican terminadores de red, de tipo TR1, se encuentran:

- Adtra n ™ .
- AIPha T elecom ™ .
- AT&TTM.
- E-TECH research TM.
- Fujitsu TM.
- Motorola TM.
- Nortel™.
- Tone Commander™.

Los terminadores de red de tipo 2, TR2, son equipos de distribución como un PBX, una red local o un multicanalizador. Algunos ejemplos de conmutadores privados compatibles con RDSI son los sistemas:

- AT&T Definity
- Ericsson Business Communications MD11 0.›NEC America NEAX 2400.
- Nortel Meridian 1.
- Rolm Systems 9750 CBX.
- Siemens Private Communications Systems Saturn IIE.

Por otro lado, existe un numeroso conjunto de puentes y ruteadores que conectan redes locales de datos con la RDSI, para usar a esta última como dorsal de interconexión entre sistemas locales:

- 3Com Arpeggio ISDN Bridge/Routers, Impact series and NETBuilder ISDN . Cisco 1003/2500/3000/4000/7000 .
- IBM 2210 Nways Multiprotocol Router .
- HP ISDN Server, ISDN Link/S700, ISDN Link/MS-DOS .
- DECwanrouter 90 ISDN.

Con las nuevas necesidades de comunicación impulsadas por Internet, la RDSI parece una respuesta obvia al incremento mundial en la demanda de servicios de transporte, como lo demuestraN sus aplicaciones corrientes en las áreas gubernamental, financiera, manufacturera, educativa y de servicios. En algún momento, sin embargo, el caudal de información que cada usuario necesite intercambiar, para soportar servicios multimedia, requerirá mejorar las capacidades del acceso básico. Ya se encuentran en desarrollo nuevas tecnologías que aborden esta problemática, como es el caso del sistema de portadora para línea de suscriptor (SLC) o la línea digital asimétrica (ADSL)

Por lo que se refiere al equipo terminal, un teléfono ROSI debe ofrecer una serie de funciones que incluyen:

- Pantalla de cristal líquido .
- Teclas suaves .
- Teclas programables por el usuario .
- Teclas de retención y liberación .
- Interfaz asíncrona para terminal de datos o PC.

Normalmente, los fabricantes de conmutadores son los mismos que producen esta clase aparatos, pero las estrictas normas de ROSI garantizan la funcionalidad de cualquier aparato con independencia de su fabricante, incluso provenientes de terceras partes. Al mismo tiempo, también han empezado a producir equipos terminales para videoconferencia (Hitachi) y fax (NEC, RICOH, VCON).

Entre las capacidades técnicas que pueden implantarse con la ROSI y servir de base para otros servicios más complejos se puede mencionar:

- Servicios de seguridad criptográfica.
- El almacenamiento y la recuperación de documentos multimedia.
- Terminales punto de venta.
- Adaptación de terminal remota.
- Construcción de redes corporativas.
- Herramientas de desarrollo cooperativo.
- Conversión de protocolos.
- Acceso a redes locales.
- Acceso a redes de paquetes de alta velocidad.
- Fax.
- Video texto y conferencia.
- Radio y Televisión por cable.

En lo que toca a los equipos no compatibles (tipo ET2), las normas prevén la conversión de protocolos mediante los adaptadores de terminal. Su funcionalidad varía, desde el simple soporte para acceso básico con teléfonos analógicos, terminales X.25, hasta complejos circuitos para PC con funciones de vídeo sobre IAP. Normalmente, las grandes empresas de computación y comunicaciones tienen una línea de productos para estas necesidades, pero también pueden encontrarse pequeñas empresas que compiten en esta arena.

Por último, alrededor de los equipos relacionados con la RDSI se deben considerar los aparatos de prueba; necesarios para garantizar el funcionamiento de los protocolos, la respuesta del medio, así como para evaluar la interoperabilidad entre equipos de distintos fabricantes. También durante el proceso de desarrollo de equipos compatibles es necesario emular el resto de los componentes con los que el aparato bajo diseño deberá interactuar en condiciones normales de operación. En este campo, las empresas líderes no coinciden totalmente con aquellas que dominan en los otros renglones:

- Consultronics TM.

- Telebyte TechnologyTM.
- Wandel & Goltermann TM.
- GN Navtel™.
- Hewlett-Packard TM.
- Tektronix™.
- Tekelec TM.

Con las nuevas necesidades de comunicación impulsadas por Internet, la RDSI parece una respuesta obvia al incremento mundial en la demanda de servicios de transporte, como lo demuestran sus aplicaciones corrientes en las áreas gubernamental, financiera, manufacturera, educativa y de servicios. En algún momento, sin embargo, el caudal de información que cada usuario necesite intercambiar, para soportar servicios multimedia, requerirá mejorar las capacidades del acceso básico. Ya se encuentran en desarrollo nuevas tecnologías que aborden esta problemática, como es el caso del sistema de portadora para línea de suscriptor (SLC) o la línea digital asimétrica (ADSL).

A grandes rasgos, las aplicaciones de la RDSI pueden c1asificarse en horizontales y verticales. Las horizontales son aquellas que pueden instalarse sobre un conjunto extenso y heterogéneo de organizaciones, este es el caso de aplicaciones tales como:

- Correo de voz y texto
- Directorios.
- Servicios de atención a clientes.
- Tele y video conferencia.
- Redes de datos.
- Telemercadeo.
- Seguridad y otros servicios de supervisión.
- Automatización de oficinas.
- Interconexión con redes locales de datos.
- Comunicación de terminal remota.

En tanto, las aplicaciones verticales son aquellas que se ajustan a las necesidades particulares de una organización, como:

- La educación.
- La banca y los servicios financieros.
- El sistema judicial.
- El sector salud.
- Los servicios turísticos.
- El sector transporte.
- El sector inmobiliario.
- Las ventas departamentales.
- La publicidad.
- Las oficinas corporativas.

3.11 Componentes de Telefonía IP.

Existen varios tipos de terminales para la telefonía IP. Esto incluye a cualquier equipo capaz de conectar VoIP de igual manera, posibilidades para video son incluidas. Una terminal puede ser un equipo LANIIP que parezca un equipo de telefonía, para logra esto es necesario contar con paquetes especiales de aplicación los cuales estan cargados dentro del ordenador o sobre un POA. Algunos ejemplos de terminales son:

- Ordenadores personales equipados con paquetes de telefonía IP PDA's equipados con paquetes de telefonía IP.
- Teléfonos ordinarios (a través de compuestas).
- Teléfonos móviles.
- Teléfonos con IP.

Las compuertas ("Gateways") son los equipos responsables para conectar una red Telefónica con IP con otros tipos de redes, para poder conectarlos es necesario el protocolo de red H.323 hacia un PSTN o a una red RSOI. Esto permite a cualquier dispositivo telefónico PSTN convertirse en una terminal. La principal aplicación de la compuerta es traducir entre diferentes formatos de comunicación. Existen tres tipos de compuertas que se aplican en:

- Voz.
- Fax.
- Conferencias a través de RDSI.

Un "Gatekeeper" permite manejar el tráfico, establece la ruta del flujo de información y proporciona un manejo de llamadas como una autorización de llamada o el manejo del ancho de banda.

De igual manera, garantiza la calidad de servicio, el conteo y los servicios de telefonía básica también son manejados por este dispositivo. Es opcional usar un "gatekeeper" en el estándar H.323. Los servidores se pueden utilizar en muchas configuraciones. Existen servidores para:

- Correo de voz.
- Funciones para un equipo PBX. Conferencias.
- Manejo de archivos.
- Otros servicios.

3.12 El Gatekeeper

Originalmente, la compuerta manejaba todas las funciones requeridas para comenzar y ejecutar una llamada telefónica en IP. Sin embargo, existe una clara división entre la codificación y la decodificación, y todo el proceso de señalización así como las llamadas funciones administrativas; las compuertas para VoIP comenzaron a ser divididas en dos diferentes componentes de sistema:

- El "Gatekeeper' fue creado para ser quien controlara todas las tareas administrativas, de esta manera se permintía a la compuerta concentrarse hacia sus propias tareas, codificando y decodificando entre diferentes tipos de redes.
- El "GateKeeper' es un estándar conceptual para H.323, pero es usado para buscar soluciones a través de la plataforma IPT de la empresa Ericsson, donde el dispositivo es conocido como un "Sitekeeper" .

Si un "gatekeeper' es incluido, la comunicación para conectar clientes con los equipos a los que desean acceder, requiere de la adecuada conexión del "gatekeeper', de tal forma que este dispositivo registre tanto las direcciones como a los usuarios que utilizan la red. Los usuarios estan capacitados para poder acceder a ciertos servicios del "gatekeeper'. Los usuarios deben seguir las direcciones y rutas que el "gatekeeper' le permita utilizar como son: el ancho de banda y las conexiones.

El "gatekeeper' sólo es un componente de señalización (no pasa a través de él flujo de información) el flujo de información es llevado directamente por el cliente y la red de VoIP. El "gatekeeper' tiene canales abiertos de señalización para los clientes.

3.13 Compuertas para Telefonía IP.

Una compuerta es un punto de red que actúa como una entrada hacia otra red. La función principal de una compuerta en el caso de telefonía IP es tender un puente hacia el PSTN y las redes IP de manera conjunta, también manejar la codificación y decodificación, y servir como interfaz.

La codificación y decodificación es una tarea que puede ser realizada a través de paquetes y programas, pero requiere de un soporte a través de circuitos adicionales con el uso de un DSP ("Digital Signalling Processors").

Algunas aplicaciones de las compuertas incluyen tareas administrativas como por ejemplo el direccionamiento y la autenticación. Sin embargo, esas funciones han sido cambiadas para que en la actualidad sean responsabilidad de los "gatekeeper's" de la red. Esta tendencia es una función especializada de la compuerta.

Un ejemplo de una compuerta de la marca Ericsson es el modelo Webswwitch 2000. Ésta permite la conexión entre un equipo PBX hacia una intranet basada en IP. Esta opción habilita a los clientes para acceder a los servicios del sistema PBX a través de la compuerta Webswwitch 2000.

La primera generación de compuertas usadas fue bajo el concepto de ordenadores de propósito general e implantaban todas las funciones necesarias en paquetes y programas. La interfaz PSTN era analógica.

La segunda generación tenía características de arquitectura asistida e interfaces para la Red Digital de Servicios Integrados (RDSI). Las compuertas fueron montadas sobre plataformas del servidor.

La tercera generación es el "estado del arte" de las compuertas con una plataforma dedicada características de arquitectura integrada, asistencia para la codificación y

decodificación y algunas otras características (por ejemplo, cancelación de Eco y manejo de señalizaciones). Sus interfaces incluyen la conexión en la capa de red con el protocolo del Sistema de Señalización No. 7 (SSITT &7).

En el futuro se podrá escalar a una arquitectura de compuertas a través del uso del BUSPCI, lo que permitirá acceder en mejores condiciones de comunicación hacia los sistemas.

El estándar para establecer conferencias a través de ROSI es el protocolo H.320 y hay compuertas que permiten conferencias entre la ROSI y la Red basada en IP a través de protocolo H.323.

3.14 Terminales de Telefonía IP.

El escenario de llamadas PC-to-PC con el acarreo de voz en Internet en gran escala fue introducido por la Compañía "Vocaltec" con sus clientes que usaban paquetes y programas sobre telefonía IP en 1995. En esa época, las comunicaciones estaban basadas en un arreglo "HALF DUPLEX" y la baja calidad en el sonido era poco relevante sobre el hecho de que podía hacerse una llamada sin costo sobre Internet. Posteriores investigaciones con VoIP en el laboratorio determinaron que esto no era factible, sin embargo a ésta empresa puede atribuírsele el inicio del concepto de VoIP en las redes comerciales.

La introducción de compuertas entre el PSTN e Internet en 1996, fue un paso adelante en el uso de telefonía a través de ordenadores. Con la implantación de las compuertas fue posible conectar a cualquier usuario a una red de telefonía pública.

El siguiente paso fue usar compuertas en ambos extremos de la conexión. Esto creaba una nueva clase de operador conocido como la nueva generación u operadores de telefonía IP. Esos operadores ofrecían servicios de telefonía a través de una infraestructura de comunicación de datos. El paso para completar el uso de redes IP fue tomado con la introducción de teléfonos IP, los cuales representaban un sistema telefónico completo. El primer teléfono bajo el concepto IP fue puesto en operación en 1998.

La combinación de terminales utilizando aplicaciones de telefonía, teléfonos bajo IP y buscadores integrados sobre la Web, es una posibilidad de una terminal activa.

La llegada de los teléfonos IP a creado la necesidad de distinguir al teléfono IP conectado sobre un ordenador personal, contra los sistemas tradicionales. Los sistemas estructurados para el uso de telefonía IP controlada por un ordenador, requiere de paquetes y programas especializados; mientras que la telefonía tradicional, opera bajo estándares convencionales.

3.15 Protocolo SIP.

El Protocolo de Inicio de Sesión ("Session Initiation Protocol", SIP) es una aplicación de diseñada como parte del manejo multimedia por IETF, además de ser un control de

arquitectura. El IETF es para trabajo en grupo a partir del estándar "Multiparty Multimedia Session Control", (MMUSIC). El SIP toma control de la señalización básica de llamadas, activa la localización de servicios y controla los registros básicos.

SIP (RFC2543) es utilizado para usuarios que utilizan conferencias como parte del los servicios de multimedia. Se tiene la necesidad de describir una sesión de multimedia dentro de los recursos de SIP. Sin embargo, SIP establece como llevar a cabo una comunicación entre "la parte que invita" y la "parte invitada", direccionando dando a los usuarios una ubicación dentro de los servicios de la red. La descripción de una sesión en términos de tiempo y de capacidades de multimedia debe ser dada con ayuda de otro Protocolo; por ejemplo, el Protocolo de Descripción de Sesión ("Session Description Protocol", SDP).

SIP es un protocolo de señalización para poner en operación sesiones entre clientes a través de la red; es decir, en Internet. Esas sesiones no deben ser necesariamente sesiones de telefonía a través de Internet. SIP podría ser usado para activar sesiones de juegos o para aprendizaje a distancia (Escuela Virtual) donde la lectura de flujos de información está fuera del proceso de los participantes en la enseñanza a distancia.

La facturación, la descripción del contenido de una aplicación del uso de una sesión y otras funciones son "ortogonales" y son tomadas por otros protocolos. Esto hace pensar que un Protocolo puede ser modificado sin afectar el uso de otros protocolos intermedios.

La interacción con la Calidad sobre Servicios (QoS), separa la señalización de las llamadas y la reservación de recursos a utilizar durante el proceso; ver las siguientes condiciones:

- Diff-serv with no per-call resource reservation.
- RSVP for end-to-end connections.

3.16 Componentes de SIP.

Existen varios componentes de operación de SIP; dichos componentes se muestran en la figura 3.35

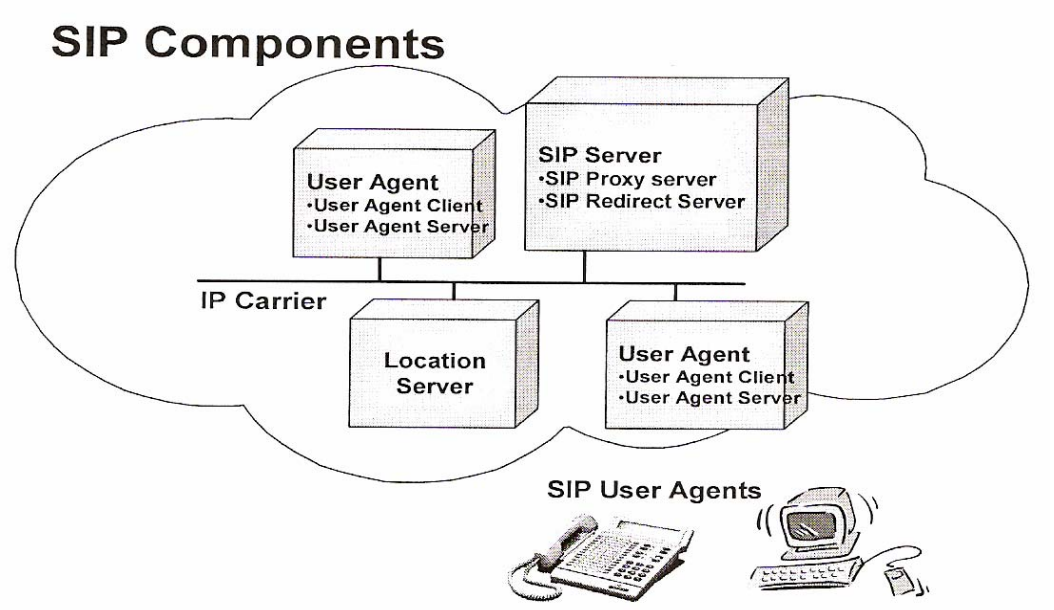


Figura 3.35 Componentes SIP

El "User Agent", (UA) es un programa de aplicación que corre en los extremos de una llamada; es decir, aplica sobre los usuarios del servicio. El UA consiste de dos partes: el denominado "User Agent Client", (UAC) y el "User Agent Server", (UAS). El UAC envía requerimientos de SIP en nombre del usuario y el UAS escucha las "respuestas" y notifica al usuario cuando éstas llegan.

SIP User Agent puede ser cualquier equipo o terminal. Éste puede ser un conjunto de paquetes y programas o una terminal dedicada en la oficina o en el hogar. Existen también equipos dedicados para otros propósitos, pero son de todas formas, habilitados por el SIP; por ejemplo, un PDA.

El Servidor del SIP es el responsable hacia los usuarios dentro del dominio de la red. El Servidor de SIP puede operar en un "modo aproximado" o en "modeo de redireccionamiento". En el modo de redireccionamiento retrasa información hacia quien llama sobre "localización de llamadas". En el "modo de aproximación" retrasa todos los mensajes entre quien llama y a quien se llama.

Los servidores "SIP Proxy Server" y el "SIP Redirect Server" son también denominados "SIP Server". La localización del servidor contiene la información acerca de las ubicaciones de usuarios.

SIP tiene la intención de integrar dentro de la existencia de Internet

3.17 SIP Call Set-Up.

SIP define seis diferentes métodos y seis tipos de códigos de respuesta que proporciona el cliente con la información de eventos. Bastantes campos de encabezados son usados por clientes y por los servidores, dando información adicional en dichos mensajes.

Las sesiones de SIP son puestas en operación utilizando tres procedimientos (muy parecido a TCP). Cuando el lado A quiere activar una sesión con el lado B; A envía una petición de INVITACIÓN requerida por B. El mensaje de INVITACIÓN contiene un identificador con una descripción de la sesión que se requiere activar con el lado B. Si el usuario (o usuaria) desea levantar una sesión de audio, el descriptor de instrucción contiene información acerca de los diferentes tipos de decodificador de audio que se tienen para suministrar el servicio solicitado.

Cuando el lado B acepta la llamada, se envía un mensaje de reconocimiento y aceptación (OK) con un número de código de respuesta identificado como 200. Cualquier respuesta con 2xx especifica que el mensaje fue recibido de forma satisfactoria en el lado receptor. El lado B agrega ciertas condiciones a su "Codec", además de proporcionar el número de puerto(s) en su respuesta, esto facilita al lado A para comenzar el proceso. La parte final del proceso de tripartita ocurre cuando A envía un reconocimiento hacia B. Para enviar la señal de ACK quien llama confirma que fue recibida la respuesta desde quien llamó. Después del procedimiento de levantado o activación, el procedimiento de culminación de la llamada puede comenzar.

SIP requiere:

- INVITE.- Invitar a un usuario a establecer una conferencia o modificar sesiones existentes.
- ACK.- Ésta sólo se usa en conjunto con la señal de INVITE.
- BYE.- Termina una conexión entre los dos participantes de una sesión.
- CANCEL.- Deja pendiente(s) la(s) lIamada(s); pero, se pueden cancelar utilizando nuevamente la instrucción CANCEL.
- REGISTER.- Los clientes SIP usan el método de REGISTER para enlazar con un Servidor SIP.
- OPTIONS.- Solicita información acerca de las prestaciones del sistema y especifica al cliente las diversas posibilidades de comunicación con el Servidor.

Las respuestas de SIP son:

- 1XX, Provisional: Da respuesta(s) provisional(es) e información acerca del curso de las acciones .
- 2XX, Success: Son las respuestas satisfactorias .
- 3XX, Redirection: Son respuestas e información acerca de la localización de nuevas llamadas .
- 4XX, Client Request Failure: Las requisiciones del cliente tienen problemas en la sintaxis .
- 5XX, Server Request Failure: El Servidor ha fallado durante una requisición .
- 6XX, Global Failure: Los mensajes fueron asimilados, pero otras fallas ocurrieron durante el proceso

3.18 Servicios de SIP

SIP proporciona el Protocolo requerido para los siguientes servicios:

- El establecimiento de la llamada incluye: El tipo de llamada(s) de 700, 800 Y 900; El establecimiento de llamada(s) sin respuesta; El tono de ocupado para la(s) llamada(s);El establecimiento de llamada(s) no condicionales; Otros servicios de cambio de dirección.
- Liberación del número que llama y del número llamado.
- Movilidad personal; es decir, la habilidad para investigar una llamada.
- Tipo de negociación de la terminal así como su selección aún cuando
- el usuario cambie de terminal(es)
- Posibilidad de negociación de la(s) terminal(es).
- Autenticación tanto de quien llama con de quien recibe la llamada.
- Supervisar una llamada transferida.
- Realizar la invitación a conferencia(s).

3.19 H.323 VS. SIP.

Los estándares IETF son interoperables con los estándares IUT-T en el transporte de voz, porque ITU-T incorpora el Protocolo RTP de los estándares IETF a través del estándar H.323. Sin embargo, existen diferentes formas de señalización por protocolos diferentes por parte de las dos instituciones: ITU-T usa el estándar H.323 ("Sistemas de Telefonía Visual y equipo para Redes de Área Local, los cuales prestan un servicio con calidad no garantizada"), mientras que la señalización SIP sí tiene un servicio de calidad garantizado. Frecuentemente, se tienen controversias y discusiones que sólo buscan ganar adeptos y popularidad.

Los promotores de ITU-T claman que el H.323 ha ganado el mejor soporte entre múltiples desarrolladores y vendedores de paquetes y programas (incluyendo Microsoft y NetMeeting). Lo anterior es en apariencia, el resultado de publicaciones recientes del estándar. Sin embargo, la rapidez en el trabajo no siempre es lo primero que se busca en los sistemas. Muchos promotores de SIP dudan que el H.323 tenga el poder de direccionamiento suficiente durante su operación. El número de versiones de H.323 parece confirmar los comentarios anteriores.

Por otra parte, los diseñadores y desarrolladores de SIP han mantenido los aspectos cruciales en sus mentes como son: el ancho de banda requerido por Internet, la integración de servicios con Internet y la modularidad y simplicidad. Mientras tanto, los productos SIP son desarrollados por líderes en la industria como: Cisco, 3Com, Ericcson, Nokia y Nortel.

En el siguiente cuadro se marcarán tanto ITU como IETF; el comparativo cubre puntos técnicos:

	SIP	H.323
Set up supported service.	Roughly the same.	
Media Transport.	Equivalent (RTP, identical codes).	

Call Set up Delay.	1.5 RTT	6-7 RTT (set up delay may also increase significantly in a lossy network due to a TCP property; see a time-line for more details of H.323 VI). Note: this has been improved with H.323V2 which allows for transportation of the H .245 messages over the signalling H.225 channel.
Complexity.	Adequate: http-like protocol.	High: ASN, use of several different protocols (H.450, H.225.0, H.245).
Extensibility.	The protocol is open to new protocol features.	ASN.1 vendor specific "nonstandardParam" at predefined positions only; lack of negotiation of the extended capabilities.
Codec Support.	Any IANA registered codecs.	ITU registered codecs (currently; Le. ITU developed codecs).
Third-party Call Control. (3PCC allows for additional services as blind transfer, operator assisted transfer, three-party calling, forwarding variations, etc.	Yes	None.
Arehiteeture.	Modular; SIP encompasses basic call signalling, user location and registration; other functions (QoS directory accesses, service discovery, session content description) reside in separate orthogonal protocols.	Monolithic: the mix of services provides by the H.323 components encompass capability exchange, conference control, maintenance operations, basic signalling, QoS registration and service discovery.

Server Stale-full/less.	Stateless	Statefull (servers are supported to keep call state for the entire duration of a call; they also have to keep the TCP states. Lower reliability and scalability.
Conference Control.	Distributed Multicasting Support.	Centralizad (MC may become a bottleneck for larger conferences and additional features as MC cascading have to be employed); unicast signalling only. Lower reliability and scalability, additional complexity of special handling of large scale conferences.
Loop Detection.	Yes	None. A redirection may cause infinite request
Firewall Support.	Accomplished by SIP Proxy.	formarding. Complicated by its complexity, usage of dinamic ports and multiple UDP streams
Multicast Captable Signalling.	Yes This simplifies user location, group invitations, call center applications, the bandwith is spared.	No.
Addressing.	Any URL, including e-mail address, H.323, http, etc.	Host (without username), gatekeeper-resolved alias (arbitrary case-sensitive string; e. g. e-mail address), E.164telephone numbers.
Transport Protocol.	Any, allowing for connectionless protocols (UDP) which result in lower call-setup time.	Reliable Protocol requiered.
Web-Integration.	Integration with other Internet services (e.g. a caller may send an e-mail to an unreachable callee). Click-to-dial feature.	?

Inter.-Domain User Location.	By existing Internet services, (DNS, LDAP, etcéte ra) ..	Weak.

La principal razón de que existan dos protocolos de señalización no interoperables es que tanto las telecomunicaciones como Internet, quisieron tener protocolos que cumplieran con sus respectivas especificaciones. ITU quizo tener normas complejas utilizando sus propias especificaciones; mientras que IETF definió un protocolo apropiado a sus propias herramientas. La Telefonía en Internet está ubicada sobre el límite de ambas tecnologías (las llamadas telecomunicaciones e Internet) y la dificultad principal estriba en cuál de los dos protocolos SIP y H.323) tendrá a futuro, mayor popularidad y aceptación por parte de los usuarios.

SIP y H.323 son diferentes aproximaciones hacia un mismo objetivo: la telefonía sobre una red basada en paquetes de información. H.323 proporciona a la comunidad, una aproximación tradicional hacia las telecomunicaciones, mientras que SIP proporciona una aproximación hacia Internet más ligera basada en los actuales modos de operación de Internet. Algunos factores acerca de H.323 son:

- Colección de estándares: H.225 para sesiones de administración: H.245 para control de multimedia, T.120 para compartir datos; H.235 para seguridad (nuevo); H.450 para servicios adicionales (nuevo) .
- Norma(s) compleja(s): ITU .... el mismo procedimiento año tras año; Usa ASN.1 y PER como "codecs" para definir los parámetros del protocolo; Existen ya dos versiones, y una tercera está en camino; Imprecisiones, muchos vendedores seleccionan opciones, las cuales hacen que sea interoperable .

Ejemplos de productos que utilizan H.323: Ericsson, Lucent, Nortel, Viena, Vocaltech, Rad y Selsius.

Ahora, se presentan las principales características de SIP:

- Simple, flexible y genérico como protocolo de señalización.
- Texto basado en el estilo http.
- SIP asume la señalización de llamadas, SOP y otros protocolos toman la
- transferencia de datos y algunas otras aplicaciones.
- Toma todo tipo de conversaciones.
- Presenta mejor escalabilidad que H.323.
- Ejemplos de organizaciones que usan SIP son: Cisco, Columbia Uni, ISI, Lucent, Netspeak, Mediatrix, Ericsson y algunos otros.

CAPÍTULO 4.
CONSTRUCCIÓN DE UNA RED CONVERGENTE A TRAVÉS DE ENRUTAMIENTO IP, UTILIZANDO PROTOCOLOS DISTINTOS.

4.1 Generalidades sobre Enrutamiento.

Los protocolos de enrutamiento dinámico son la tecnología que permite a los ruteadores realizar algunas de sus funciones más vitales. Esto incluye descubrir y mantener rutas, así como converger en un acuerdo sobre la Topología de una Red.

Los ruteadores pueden enrutar de dos modos básicos: Pueden utilizar rutas estáticas preprogramadas, o pueden calcular rutas dinámicamente utilizando cualquiera de los protocolos de enrutamiento dinámico. Los protocolos de enrutamiento dinámico son usados por los ruteadores para descubrir rutas. Entonces, los ruteadores envían paquetes mecánicamente (o datagramas) por esas rutas.

Los ruteadores programados estáticamente no pueden descubrir rutas; carecen de cualquier mecanismo para comunicar la información de enrutamiento a otros ruteadores. Los ruteadores programados estáticamente sólo pueden enviar paquetes usando rutas definidas por un Administrador de Redes. Además de la programación estática de las rutas, hay tres categorías amplias de protocolos de enrutamiento dinámico:

- Vector de Distancia.
- Estado del Enlace.
- Híbridos.

Las diferencias principales entre estos tipos de protocolos de enrutamiento dinámicos residen en el modo en que descubren y calculan nuevas rutas a los destinos.

Los protocolos de enrutamiento pueden clasificarse de muchos modos, incluso por muchas de sus características operativas, como su campo de acción, el número de rutas redundantes a cada destino soportado, etcétera. En otras palabras, dividirlos en categorías según el papel que desempeñan en una internetwork. Hay dos clases funcionales de protocolos de enrutamiento dinámico: los protocolos de gateway interior (IGP), y los protocolos de gateway exterior (EGP).

4.1.1 Enrutamiento Estático.

La forma más simple de enrutamiento son las rutas preprogramadas, y, en consecuencia, estáticas. Las tareas de descubrir rutas y propagarlas a través de una red se dejan al Administrador de la Internetwork. Un ruteador programado para el enrutamiento estático envía paquetes a través de puertos predeterminados. Una vez configurada la relación entre una dirección de destino y un puerto del ruteador, ya no hay necesidad de que los ruteadores intenten descubrir la ruta o incluso, comunicar información sobre rutas.

El uso de estas rutas estáticas tiene muchas ventajas. Por ejemplo, las rutas programadas estáticamente pueden hacer más segura la red. Sólo puede haber un camino dentro y

fuera de una red conectada con una ruta definida estáticamente, a no ser que estén definidas múltiples rutas estáticas.

Otra ventaja, es que el enrutamiento estático es un recurso mucho más eficaz. El enrutamiento estático utiliza bastante menos ancho de banda de los servicios de transmisión, no gasta ningún ciclo del Procesador del ruteador intentando calcular las rutas, y necesita bastante menos memoria. En algunas redes tal vez sea posible utilizar ruteadores más pequeños, más baratos, empleando rutas estáticas. A pesar de estas ventajas, se debe ser consciente de algunas limitaciones inherentes al enrutamiento estático.

El enrutamiento estático es bueno sólo para redes muy pequeñas, que sólo tienen una ruta a cualquier destino concreto. En tales casos, el enrutamiento estático puede ser el mecanismo de enrutamiento más eficaz porque no consume ancho de banda intentando descubrir rutas o comunicarse con otros ruteadores.

A medida que se hacen mayores las redes y añaden rutas redundantes a los destinos, el enrutador estático se convierte en una responsabilidad con mucha actividad. Cualquier cambio en la disponibilidad de los ruteadores o los servicios de transmisión de la Red de Área Amplia, (WAN) deben descubrirse manualmente y programarse. Las WAN con topologías más complejas y que ofrecen múltiples rutas potenciales, requieren absolutamente, enrutamiento dinámico. Los intentos de usar enrutamiento estático en WAN complejas de múltiples rutas, acabarían con el propósito de tener esa redundancia de rutas.

En ocasiones, son deseables las rutas definidamente estáticamente, incluso en redes grandes o complejas. Las rutas estáticas pueden configurarse para mejorar la seguridad. La conexión a Internet para una compañía en particular, podría tener una ruta definida estáticamente a un Servidor de Seguridad. No sería posible ninguna entrada sin haber pasado primero los mecanismos de autenticación que proporciona el Servidor de Seguridad.

Alternativamente, las rutas definidas estáticamente podrían ser muy útiles para construir conexiones Extranet usando el Protocolo de Internet (IP) de otras compañías. Finalmente, las rutas estáticas pueden ser el mejor modo de conectar pequeñas ubicaciones con redes internas a una WAN. Las rutas estáticas pueden ser bastante útiles. Sólo hay que entender lo que pueden y lo que no pueden hacer.

4.1.2 Enrutamiento por Vector de Distancia.

En el enrutamiento basado en los Algoritmos de Vector de Distancia, algunas veces llamados también "Algoritmos de Bellman-Ford"; los algoritmos transmiten periódicamente copias de sus tablas de enrutamiento a sus vecinos de red inmediatos.

Cada receptor añade un vector de distancia (es decir; su propio "valor" de distancia) a la tabla y lo envía a sus vecinos inmediatos. Este proceso, paso a paso hace que cada ruteador aprenda sobre otros ruteadores y desarrolle una perspectiva acumulativa de las "distancias" de la red. La Tabla Acumulativa se utiliza entonces, para actualizar las Tablas de Enrutamiento de los ruteadores.

Una vez completa, cada ruteador ha aprendido una vaga información sobre las "distancias" a los recursos conectados a la red.

En ciertas circunstancias, el Enrutamiento por Vector de Distancia puede realmente crear problemas de enrutamiento para los protocolos de vector de distancia. Una falla o cualquier otro cambio en la red, Por ejemplo, será necesario algún tiempo para que los ruteadores converjan en un nuevo entendimiento de la topología de la red. Durante el proceso de convergencia, la red puede ser vulnerable al enrutamiento incoherente, e incluso, los bucles infinitos. Las protecciones pueden contener muchos de estos riesgos, pero queda el hecho de que el rendimiento de la red está en riesgo durante el proceso de convergencia. Por tanto, los más antiguos protocolos de vector de distancia que resultan lentos para converger pueden no se apropiados para WAN grandes y complejas.

En redes más pequeñas, los protocolos de enrutamiento por vector de distancia pueden ser problemáticos en el pero de los casos, o por debajo de lo óptimo en el mejor de los casos. Esto se debe a que la sencillez, que es el punto fuerte, también puede ser una fuente de debilidad.

En cualquier internetwork con rutas redundantes, es mejor utilizar un protocolo de vector de distancia que rutas estáticas. Esto se debe a que los protocolos de enrutamiento por vector de distancia pueden detectar y corregir automáticamente fallas de la red.

Por desgracia, no son perfectos. Si todas las variables de la red se mantuvieran constantes (incluyendo aspectos como los niveles de tráfico, el ancho de banda de cada enlace e, incluso, la tecnología de transmisión), la ruta más corta geográficamente produciría la menor cantidad de retraso en la propagación. En realidad, dicha lógica está más allá de las capacidades de los simples protocolos de vector de distancia. Estos protocolos no están exactamente limitados por esto, porque el retraso en la propagación es a menudo menos significativo de los factores que inciden en el rendimiento de una ruta. El Ancho de Banda y los niveles de tráfico pueden ambos tener efectos más considerables sobre el rendimiento de una red.

4.1.3 Enrutamiento por Estado de Enlace.

Los Algoritmos de Enrutamiento por Estado de Enlace, más conocidos como Protocolos Primero la Ruta más Corta, (SPF), mantienen una Base de Datos compleja de la topología de la red. A diferencia de los Protocolos de Vector de Distancia, los Protocolos de Estado de Enlace desarrollan y mantienen un conocimiento completo de los ruteadores de la red, así como del modo en que se interconectan. Esto se consigue mediante el intercambio de Publicaciones del Estado del Enlace, (LSA), con otros ruteadores de una red.

Cada ruteador que ha intercambiado LSA construye una Base de Datos topológica usando todas las LSA recibidas. Se utiliza entonces un algoritmo SPF para computar la accesibilidad a los destinos de la red. Esta información se usa para actualizar la Tabla de Enrutamiento. Este procedimiento puede descubrir cambios en la topología de la red causados por la falla de un componente o e crecimiento de la red.

De hecho, el intercambio de LSA es disparado por un evento de la red, en lugar de ejecutarse periódicamente. Esto puede liberar mucho del proceso de convergencia, porque no hay necesidad de esperar a que expiren una serie de controles temporales arbitrarios para que los ruteadores de la red puedan empezar a converger.

A pesar de todas sus característias y de su flexibilidad, el Enrutamiento por Estado de Enlace despierta dos riesgos potenciales:

1. Durante el proceso de descubrimiento inicial, los Protocolos de Enrutamiento por Estado de Enlace pueden inundar los servicios de transmisión de la red y, por tanto, reducir significativamente la capacidad de la red para transportar datos. Esta degradación del rendimiento es temporal, pero puede ser muy notable. Que este proceso de inundación impida de forma notable el rendimiento de una red va a depender de dos cosas: la cantidad de ancho de banda disponible y el número de ruteadores que deben intercambiar la información de enrutamiento. La inundación en redes grandes con enlaces relativamente pequeños (como DL el de bajo ancho de banda sobre una Red Frame Relay), será mucho más notable que un ejercicio similar en una red pequeña con enlaces de gran tamaño (como los T3).

2. El Enrutamiento por Estado de Enlace es muy intensivo en cuanto a memoria y procesador. En consecuencia, se necesitan ruteadores más completamente configurados para soportar el Enrutamiento por Estado del Enlace, que en el caso del Enrutamiento por Vector de Distancia. Esto aumenta el costo de los ruteadores configurados para un Enrutamiento por Estado de Enlace.

Difícilmente, estos riesgos son fatales en el método de Enrutamiento por Estado del Enlace. Los impactos en el rendimiento de ambos pueden manipularse y resolverse con previsión, planificación y administración.

El método de Enrutamiento Dinámico por Estado de Enlace puede ser bastante útil en redes de cualquier tamaño. En una red bien diseñada, un protocolo de Enrutamiento por Estado del Enlace permitirá a una red sortear con facilidad los efectos de un cambio topológico inesperado. El uso de eventos, como los cambios, para controlar las actualizaciones (en lugar de temporizadores de intervalos fijos) permite que la convergencia empiece mucho más rápidamente después de un cambio en la topología.

También se evitan los excesos de consumo de las actualizaciones frecuentes, controladas por el tiempo, de un protocolo de Enrutamiento por Vector de Distancia. Esto permite utilizar más ancho de banda para el tránsito de enrutamiento en lugar de hacerlo para el mantenimiento de la red, siempre que se haya diseñado adecuadamente la red.

Una ventaja añadida de la eficiencia del ancho de banda de los protocolos de Enrutamiento por Estado del Enlace, es que facilitan la escalabilidad de la red más que las rutas estáticas o los protocolos de Vector de Distancia. En yuxtaposición con sus limitaciones, es fácil ver que el Enrutamiento por Estado de Enlace es mejor en redes mayores, más complejas, o en redes que deben ser altamente escalables. Puede ser un reto configurar inicialmente un protocolo de Estado del Enlace en una red grande, pero a la larga el esfuerzo bien merece la pena.

4. 1.4 Enrutamiento Híbrido.

La última forma de disciplina de enrutamiento es la Hibridización. Los protocolos de Enrutamiento Híbridos equilibrados utilizan la métrica de Vectar de Distancia, pero subrayan una métrica más exacta que los protocolos de Vector de Distancia convencionales. También convergen más rápidamente que los protocolos de Vector de Distancia, pero evitan los excesos de consumo en las actualizaciones del Estado del Enlace. Los híbridos equilibrados son eventos dirigidos más que periódicos y, por tanto, conservan ancho de banda para las aplicaciones reales.

Aunque existen los protocolos Híbridos equilibrados "abiertos", esta forma está casi exclusivamente asociada con la creación patentada de una sola compañía, Cisco System, Inc™. Su protocolo, Protocolo de Enrutamiento de Gateway Interior Mejorado (EIGRP), fue diseñado para combinar los mejores aspectos de los protocolos de Enrutamiento por Vectar de Distancia y por Estado de Enlace sin incurrir en ninguna de sus limitaciones de rendimiento. Dado que esta clase de Protocolo de Enrutamiento Dinámico está dominada por EIGRG.

Una de las tareas más difíciles, aunque críticas, qe deben superarse al construir una internetwork es la selección del Protocolo de Enrutamiento. Como indican las secciones anteriores, una amplia paleta de opciones espera al arquitecto de la futura in te m e twork. Aunque las explicaciones anteriores deberían ayudarle a diferenciar entre las distintas clases de Protocolos de Enrutamiento Dinámico, esto es sólo el principio. Todavía debe seleccionarse un protocolo de Enrutamiento específico, o unos protocolos, entre la gran variedad que puede estar disponible en cada clase.

Uno de los mejores modos de empezar a hacer más pequeña la lista de potenciales protocolos es evaluando las características de rendimiento de cada protocolo en relación con los requisitos proyectados. A diferencia del Hardware, no sirve comparar los paquetes por segundo o los valores de ancho de banda de los protocolos de Enrutamiento. ¡No existen! En su lugar, debe valorarse la eficacia con que cada protocolo ejecuta las distintas tareas que soportan el internetworking. Dos de las más importantes de entre estas tareas son: la Convergencia y el Cálculo de Rutas.

4.2 Convergencia.

Uno de los aspectos más importantes del Enrutamiento es un concepto conocido como Convergencia. De forma bastante simple, siempre que se produce un cambio en la topología, o forma, de una red, todos los ruteadores de esa red deben desarrollar un nuevo entendimiento de lo que es la topología de esa red. Este proceso es la vez cooperativo e independiente; los ruteadores comparten información entre sí, pero deben calcular independientemente los impactos del cambio de topología en sus propias rutas. Como deben desarrollar mutuamente un acuerdo sobre la nueva topología con independencia de las diferentes perspectivas, se dice que convergen en este consenso.

La convergencia es necesaria porque los ruteadores son dispositivos inteligentes que pueden tomar sus propias decisiones de Enrutamiento. Esto es a la vez una fuente de fortaleza y de vulnerabilidad. Bajo condiciones de operatividad normales, esta inteligencia independiente y distribuida es fuente de tremendas ventajas. Durante los

cambios en la topología de la red, el proceso de converger en un nuevo consenso en cuanto a la forma de la red puede realmente introducir inestabilidad y suponer problemas de Enrutamiento. Por desgracia, la naturaleza independiente de los ruteadores puede ser también una fuente de vulnerabilidad siempre que se produzca un cambio en la topología de la red. Dichos cambios, por su naturaleza, cambian la topología de una red.

Es virtualmente imposible para todos los ruteadores de una red detectar simultáneamente en cambio en la topología. De hecho, dependiendo del Protocolo de Enrutamiento que se use, así como de otros numerosos factores, puede haber un retraso de tiempo considerable antes de que todos los ruteadores de esa red alcancen un consenso, o acuerdo, sobre lo que es la nueva topología. Este retraso se llama tiempo de convergencia. Es importante recordar que la convergencia no es inmediata. Lo único que no se sabe es cuánto tiempo se necesita para que se produzca la convergencia. Algunos factores que pueden aumentar el tiempo de retraso intrínseco de la convergencia son los siguientes:

- La distancia (en saltos) al ruteador desde el punto de cambio.
- El número de ruteadores de la red que utilizan protocolos de Enrutamiento Dinámico.
- Ancho de Banda y cantidad de tránsito en los enlaces de comunicaciones.
- La carga de un ruteador.
- Patrones de tránsito cara a cara del cambio topológico.
- El Protocolo de Enrutamiento utilizado.

Los efectos de algunos de estos factores pueden minimizarse con una Ingeniería de Red cuidadosa. Puede diseñarse la red para minimizar la carga de un determinado ruteador o un enlace de comunicaciones, por ejemplo. Otros factores, como el número de ruteadores de una red, deben aceptarse como riesgos inherentes al diseño de una red.

Sin embargo, es posible diseñar la red de tal modo que se necesite que converjan menos ruteadores. Usando rutas estáticas para interconectar redes internas a la red, se reduce el número de ruteadores que deben converger. Esto disminuye directamente los tiempos de convergencia. Dados estos factores, está claro que las dos claves para minimizar los tiempos de convergencia son:

- Seleccionar un Protocolo de Enrutamiento que pueda calcular eficazmente las rutas.
- Diseñar adecuadamente la red.

La capacidad de convergencia de un Protocolo de Enrutamiento, es una función de su capacidad de cálculo de rutas. La eficacia del cálculo de rutas de un Protocolo de Enrutamiento se basa en los siguientes factores:

- Si el protocolo calcula y almacena, múltiples rutas a cada destino.
- La manera en que se inician las actualizaciones de Enrutamiento.
- Las medidas utilizadas para calcular distancias o costos.

Algunos Protocolos de Enrutamiento intentan mejorar su eficacia operativa registrando una sola ruta (idealmente, la mejor) a cada destino conocido. La desventaja de este

método es que cuando se produce un cambio en la topología, cada ruteador debe calcular una nueva ruta a través de la red para los destinos afectados.

Otros protocolos aceptan los excesos de consumo de procesamiento que acompañan a los mayores tamaños de Tabla de Enrutamiento, y almacenan múltiples rutas a cada destino. En condiciones operativas normales, múltiples rutas permiten al ruteador equilibrar las cargas de tráfico a través de múltiples enlaces. Cuando se produce un cambio en la topología, los ruteadores ya tienen rutas alternativas a los destinos afectados en sus Tablas de Enrutamiento. El tener ya asignada una ruta alternativa no acelera necesariamente el proceso de convergencia. Sin embargo, sí permite a las redes sostener mejor los cambios en la topología.

Una actualización temporizada es un mecanismo muy simple. El tiempo disminuye en un contador según transcurre. Cuando ha transcurrido un periódo específico de tiempo, se realiza una actualización con independencia de si se ha producido un cambio topológico. Esto tiene dos implicaciones:

- Muchas actualizaciones se realizarán innecesariamente, lo que consume ancho de banda y recursos del ruteador.
- Los tiempos de convergencia pueden inflarse innecesariamente si los cálculos de rutas son controlados por el paso del tiempo.

Las actualizaciones controladas por eventos son medios mucho más complejos de iniciar actualizaciones de enrutamiento. Aparentemente, una actualización se inicia sólo cuando se ha detectado un cambio en la topología de la red. Dado que un cambio en la topología es lo que crea la necesidad de convergencia, obviamente, este método es el más eficaz. Puede seleccionarse un iniciador de actualización tan sólo seleccionando un Protocolo de Enrutamiento. Por tanto, éste es un factor que debe considerarse al seleccionar un Protocolo de Enrutamiento. El Protocolo de Enrutamiento determina otro importante mecanismo: su(s) métrica(s). Hay una amplia disparidad de términos, tanto en número como tipo de métricas utilizadas.

Los protocolos de enrutamiento simples soportan como mínimo una o dos métricas de enrutamiento. Los protocolos más complejos pueden soportar cinco ó más métricas. Es seguro asumir que cuantas más métricas haya, más variadas y espeíficas son. Por tanto, cuanto mayor es la variedad de métricas disponibles, mayor es su capacidad de ajustar el funcionamiento de la red a las necesidades particulares. Los protocolos de Estado de Enlace pueden aportar la capacidad de calcular las rutas basándose en varios factores:

- Carga de tráfico.
- Ancho de Banda disponible.
- Retraso de la propagación.
- El costo de red de una conexión (aunque esta métrica tiende a ser más una estimación, que un valor real).

La mayoría de estos factores son altamente dinámicos en una red; varían según la hora del día, el día de la semana, etcétera. Importa recordar que, según varían, varía en consecuencia el rendimiento de la red. Por tanto, la pretensión de las métricas de enrutamiento dinámico es permitir que las decisiones de enrutamiento óptimo se hagan utilizando la información más actual disponible.

Algunas métricas son simplistas y estáticas, mientras que otras son altamente complejas y dinámicas. Las métricas estáticas ofrecen generalmente la capacidad de personalizar sus valores cuando se configuran. Hecho esto, cada valor permanece constante hasta que se cambia manualmente. Los Protocolos Dinámicos permiten tomar decisiones de enrutamiento basadas en información en tiempo real sobre el estado de la red. Estos protocolos son soportados sólo por los protocolos de Enrutamiento por Estado del Enlace, o son Híbridos más complejos.

4.3 Protocolos Distintos.

Muchas redes pequeñas presentan un solo Protocolo Enrutado y/o de Enrutamiento. Es un hecho que cada red necesitará uno de cada: un Protocolo Enrutado para encapsular y transportar datos a su destino, y un Protocolo de Enrutamiento para descubrir, comparar y seleccionar rutas óptimas a través de la red a ese destino. Tener un protocolo de cada tipo simplifica en gran medida muchas facetas del internetworking, incluyendo el cálculo de rutas y el intercambio de información de enrutamiento entre todos los nodos miembros. Por desgracia, con lo beneficioso que puede utilizar un único protocolo, no siempre es posible, ni siquiera práctico.

En la vida real, hay innumerables razones para que sea inevitable utilizar múltiples protocolos en una internetwork. Estas razones van desde la necesidad funcional a los requisitos comerciales. Con independencia de la razón real por la que un solo Protocolo de Enrutamiento sea inadecuado para cualquier situación dada, deben resolverse retos fundamentales.

La necesidad real de soportar dos o más Protocolos de Enrutamiento en una internetwork puede venir de diversas fuentes. En general, la necesidad deriva de las diferencias arquitectónicas entre redes que deben ser interconectadas. Estas diferencias pueden ser resultado de las preferencias de los administradores de redes. Un Administrador de Redes puede preferir OSPF (Primero la Ruta Libre más Corta) y un entorno con productos de varios fabricantes, por ejemplo, mientras que otro puede que prefiera una red sólo de Cisco Systems Inc TM, que ejecute EIGRP (Protocolo de Enrutamiento de Gateway Interior Mejorado).

Alternativamente, las arquitecturas de redes diferentes podrían indicar una distinción funcional dentro de una red, como ocurre con las funciones de un gateway interior y uno exterior. Algunos de los requisitos comerciales más comunes que pueden conducir a interconectar redes diferentes incluyen extender una Intranet para socios comerciales (lo que se conoce como Extranet), o incluso, conectarla a Internet. De forma similar, las fusiones y las adquisiciones también pueden dar como resultado la interconexión de arquitectura de red muy diferentes, o incluso de redes construidas con productos de diferentes fabricantes. Por tanto, por muy diversas razones, el objetivo purista de un solo Protocolo de Enrutamiento y un solo protocolo enrutado puede ser imposible.

Con independencia de las causas, puede encontrarse ante la necesidad de interconectar con Protocolos Enrutados y/o de Enrutamiento diferentes. A pesar de sus diferencias, puede interconectar con éxito dichas redes utilizando algunas técnicas relativamente

simples. Estas técnicas varían en cierta medidad, dependiendo de si los protocolos diferentes son de Enrutamiento o Enrutados, y de cuáles son en particular.

La diferencia en los Protocolos de Enrutamiento no es el único reto que puede encontrarse un Administrador de Redes. Los protocolos enrutados pueden ser problemáticos. Idealmente, una Organización selecciona un solo protocolo enrutado, como IP o IPX, y lo implanta ampliamente. Sin embargo, muchas de las circunstancias que podían dar como resultado Protocolos de Enrutamiento diferentes también pueden afectar a los Protocolos Enrutados. El resultado final podría ser múltiples protocolos enrutados diferentes usándose en diferentes dominios de una internetwork. Hay varias opciones para hacer frente a esta incompatibilidad:

- Soportar Protocolos Enrutados redundantes.
- Utilizar gateways de conversión de protocolo.
- Tunneling a través de regiones de red incompatibles.

4.3.1 Protocolos Enrutados Redundantes.

Los Ordenadores actuales y sus tarjetas de interfaz de red (NIC) pueden soportar simultáneamente múltiples protocolos de networking. En teoría, cada sistema final de una red puede soportar dos ó más protocolos Enrutados muy diferentes, como IP e IPX, simultáneamente. La tarjeta de interfaz de red del ordenador no busca esas direcciones de capa de red en las tramas de datos de una LAN; ni la tarjeta de interfaz de red mira sólo las direcciones MAC. Los datagramas del Protocolo Enrutado están encapsulados en las tramas que tienem direccionamiento MAC. Cuando el protocolo de la capa de enlace del sistema remoto desencapsula la trama. Se descubren los datagramas. Esto permite que el protocolo de capa de enlace de datos examine la dirección de capa de red y envíe los datos encapsulados a los Protocolos Enrutados apropiados para su posterior procesamiento.

El uso de múltiples protocolos de capa de red es completamente transparente para las tarjetas de interfaz de red del sistema final, así como para los distintos dispositivos de la LAN. Sin embargo, cada uno de estos protocolos tendría sus propios mecanismos de dirección, arquitectura de direcciones y envío de datagramas. Esto significa que las redes tendrían que soportar dos conjuntos de direcciones de internetwork: una por cada Protocolo Enrutado. Los dispositivos afectados serían los ruteadores y switches de la Capa 3 (si hubiera alguno en la red). Afortunadamente, los ruteadores están diseñados para soportar múltiples Protocolos Enrutados. Por tanto, la red podría ya utilizar simultáneamente Protocolos Enrutados diferentes por toda la red. Sus opciones para soportar Protocolos de Enrutamiento redundantes son de redundancia completa o parcial.

Una red que utiliza Protocolos Enrutados completamente redudantes necesita que cada dispositivo de networking ejerza simultáneamente ambos protocolos enrutados. Considérese, por ejemplo, el caso de un entorno de red que está en mitad de transición desde ordenadores y networking Apple ™ y networking a Windows NT de MicrosoffTM. El entorno de red original utilizaba el conjunto de protocolos AppleTalk™. El nuevo Sistema Operativo de Red, NT, se utilizará con IP. En semejante escenario, un proceso de migración razonable sería ejecutar ambos protocolos

en todos los dispositivos simultáneamente. Dicho escenario podría ser temporal, hasta que pudiera completarse la migración. Alternativamente, esa solución podría ser permanente, como sería en ell caso de la monitorización de los puertos de administración direccionados por IPv4 de los concentradores Ethernet más antiguos en una red IPv6.

Otro modo de usar los protocolos enrutados redundantes es instalar el protocolo redundante sólo cuando es necesario. En otros casos, algunos sistemas finales tendrían dos protocolos enrutados instalados y configurados. La ventaja de este método es que los sistemas finales que no necesitan el segundo protocolo se ven libres del consumo que supone ejecutarlo. Además, el Administrador de la Red se libra de instalar y soportar protocolos adicionales en dispositivos que no les requieren. La única desventaja es que los dispositivos que usan un protocolo sólo pueden comunicarse con otros dispositivos que ejecutan el mismo. En otras palabras, un sistema final sólo con AppleTalk™ no puede comunicarse con ningún sistema final sólo con IP. Esta desventaja, sin embargo, puede eliminarse con una planificación apropiada y la identificación de las necesidades de los usuarios. Una de las ventajas más importantes de la separación de las funciones en capas de una red es que dos ó más protocolos de red pueden operar simultáneamente sobre la misma LAN. Por tanto, no hay necesidad de volver a cablear o añadir otra red para soportar dos protocolos.

4.3.2 Protocolos de Enrutamiento Diferentes.

Los ruteadores que utilizan Protocolos de Enrutamiento para calcular rutas, comparten información sobre la topología de la red, e identifican los siguientes saltos óptimos para cualquier datagrama dado. Estos protocolos son completamente transparentes para los sistemas finales de una red. Por tanto, resolver incompatibilidades entre ellos puede que no sea un desafío tan grande o fastidioso como con los Protocolos Enrutados. La interconexión de dos o más redes que utilizan Protocolos de Enrutamiento diferentes puede realizarse de tres modos diferentes:

- Protocolos de Enrutamiento Integrados.
- Protocolos de Enrutamiento Redundantes.
- Redistribución de Información de Ruta.

Un método para soportar múltiples protocolos de Enrutamiento es usar un protocolo de Enrutamiento Integrado, único. Un Protocolo Integrado es capaz de enrutar simultáneamente dos protocolos y direcciones diferentes. Los ejemplos de esta forma de Protocolo de Enrutamiento son las series emergentes de protocolos ng que están diseñados para facilitar la migración entre IPv4 e IPv6. Ejemplos específicos de Protocolos Integrados son OSPFng, RIPng y RIP versión 2 (RIP2).

RIP 2 fue diseñado para ser completamente compatible retrospectivamente con la versión 1 de RIP. Por tanto, está calificado como un Protocolo de Enrutamiento Integrado.

El uso de un Protocolo de Enrutamiento Integrado (RIP), proporciona una integración sin fisuras de diferentes protocolos de enrutamiento. La única desventaja de este método es que hay pocos protocolos de enrutamiento integrados. La mayoría (si no todos) de

tales protocolos no son nada más que versiones avanzadas de protocolos de enrutamiento que son compatibles retrospectivamente con sus primeras versiones. Como tales, son mecanismos transicionales que facilitan una migración airosa desde una versión de un Protocolo de Enrutamiento a la siguiente. En teoría, toda la red se convertirá eventualmente para utilizar la versión más nueva del protocolo. Por tanto, una vez completada la transición, las características de integración del protocolo de Enrutamiento son discutibles. Sin embargo, la red se beneficia del conjunto de capacidades de la nueva versión del protocolo.

Las redes que utilizan un Protocolo de Enrutamiento Integrado (RIP), a diferencia de las redes que utilizan cualquiera de los otros mecanismos para soportar dos protocolos de enrutamiento, funcionan como una única red. No hay necesidad de convertir datagramas, traducir direcciones, o redistribuir información de enrutamiento entre el viejo protocolo y el nuevo, integrado. La interoperatividad entre RIP y RIP 2; por ejemplo, es una función nativa de RIP 2. La única limitación funcional es que los ruteadores que todavía ejecutan la versión antigua de RIP no pueden beneficiarse de ninguna de las características añadidas a RIP 2.

Existen también otros protocolos integrados. Algunos ejemplos son IS-IS que pueden transportar DECnet e IP, y EIGRP de Cisco Systems Inc. TM, que pueden compartir información de enrutamiento con redes IGRP. Seleccionar un Protocolo de Enrutamiento Integrado (RIP) es una cuestión de comprensión de sus requisitos particulares. Se puede encontrar uno que se ajuste perfectamente a las necesidades específicas de una aplicación, o puede descubrir que ninguno de los protocolos integrados disponibles funcionará en su situación particular.

Un modo de evitar incompatibilidades entre los protocolos enrutados consiste en implantarlos redundantemente. Este método puede implantarse en varios grados, dependiendo de las necesidades. En un extremo, por ejemplo, podría implantarse dos protocolos de enrutamiento en cada ruteador de la internetwork. Esto daría como resultado que cada ruteador:

- Tuviera dos conjuntos de Tablas de Enrutamiento.
- Ejecutara dos conjuntos de actualizaciones de Tabla.
- Convergiera dos veces después de cambios en la topología.

En otras palabras, cada ruteador tendría doble trabajo, además de la responsabilidad normal de enviar datagramas a favor de los sistemas finales. Por tanto, el uso de Protocolos de Enrutamiento redundantes consume recursos inevitablemente. Los recursos internos de ruteador, incluyendo los ciclos del Procesador y la Memoria, se consumen en proporciones prodigiosas. La red también puede sufrir cambios según aumenta el consumo de Ancho de Banda. La proporción en que se consumirá cada uno de estos recursos depende directamente de:

- El tamaño de la internetwork que utiliza protocolos redundantes.
- Los protocolos utilizados.
- Las métricas actuales o las configuraciones implantadas.

Dadas estas variables, puede que no sea fácil o viable valorar los efectos reales del uso de protocolos de Enrutamiento Redundantes. No obstante, estos factores afectan

adversamente al rendimiento de la red. Sin embargo, a diferencia de los protocolos enrutados, no tiene sentido usar los protocolos de enrutamiento redundante. Cada protocolo debería ser capaz de calcular rutas a través de la red a cualquier destino dado, no obteniéndose ningún beneficio de la redundancia del enrutamiento completo.
Un método más sensible es dividir las porciones de la internetwork que necesitan protocolos redundantes y utilizar un único protocolo en cualquier otra parte. Esto mejoraría la eficacia operativa de los ruteadores, así como la de toda la red. Se puede elegir, por ejemplo, crear redes internas dentro de la intemetwork. Cada una de ellas podría usar un Protocolo de Vector de Distancia como RIP o RIP 2. El resto de la red usaría un protocolo más robusto, como OSPF o EIGRP. En un escenario como éste, sólo los ruteadores fronterizos entre las dos regiones de la red tendrían que soportar ambos protocolos.

La redistribución de rutas es una de las más poderosas (aunque complejas), capacidades de un ruteador. En esencia, la redistribución de rutas es un concepto bastante simple. Los ruteadores gateway participan en el cálculo de rutas y en la convergencia de las redes de las cuales son miembros. La información de enrutamiento para esa red es resumida y distribuida a una red vecina (si bien una que ejecuta un protocolo de enrutamiento diferente). En la práctica, la configuración de una redistribución de rutas es bastante compleja. Una de las razones principales de la complejidad de la redistribución de rutas son las diferencias fundamentales que pueden existir entre los distintos protocolos de enrutamiento. Dichos protocolos pueden tomar sus decisiones de enrutamiento utilizando algoritmos muy diferentes (Vector de Distancia frente a Estado de Enlace), así como una sorprendente variedad de métricas de enrutamiento reales.

4.4 El cambio en los negocios

En esta sección se tratará la forma en la que los negocios han venido cambiando y el impacto que ha tomado la Tecnología Informática (IT) hacia el interior de las compañías. Las empresas buscan optimizar su infraestructura de Tecnología Informática, (IT). Ésta, al igual que las telecomunicaciones deben ser constantemente revisadas y evaluadas por los mandos medios y superiores de las compañías para lograr el equilibrio entre economía y eficiencia. Todavía, se espera encontrar aplicaciones más robustas y complejas de esta nueva tecnología. "Voice LAN", proporciona una forma para facilitar:

- Los procesos de reingeniería de los negocios.
- Manejar el "núcleo" de los equipos de trabajo.
- Operar las aplicaciones de multimedia en un entorno cliente/servidor.
- Controlar los costos de operación.

En los negocios de hoy, "lo único constante es el cambio". Las compañías están operando en la actualidad de una forma más volátil y con mercados en movimiento, en comparación a como se hacían negocios en el pasado inmediato; estas demandas requieren flexibilidad tanto en los servicios como en los productos. Ahora, el lapso de tiempo en que los productos llegan a los nuevos mercados en muy corto. Por lo que, ahora es el momento en que el cliente debe estar preparado para obtener respuestas.

4.5 La Tecnología Informática Tradicional Entregada.

Actualmente, los negocios están luchando para tener mejores inversiones en Tecnología Informática, el sentimiento generalizado es que aún, no se han podido deshacer de la Tecnología tradicional y esto significa, no poder crecer al ritmo que ellos esperarían. En vez de modelarse a sí misma en los negocios, la Tecnología Informática ha dejado crecer las expectativas de lo que finalmente podría ser el ambiente real de los negocios. En el ambiente cliente/servidor que utilizan los usuarios, ha sido difícil integrar los sistemas con los equipos de trabajo. Sin embargo, los usuarios que trabajan en la misma tarea siempre se encuentran ubicados en la misma oficina o en el mismo edificio, o al menos en el mismo continente.

Actualmente, los usuarios distribuidos y establecidos en varios lugares requieren colaborar en el mismo proyecto. Y, requieren más que un correo electrónico y de telefonía convencional: los usuarios necesitan compartir documentos en tiempo real, mostrar hoja(s) de cálculo, cambiar imágenes en documentos y la comunicación en grupos.

4. 6 Reingeniería de los Procesos en los Negocios.

Estas son algunas de las demandas que se requieren para poner en marcha la llamada Reingeniería de los Procesos en los Negocios ("Business Process Reengineering", BRP): Tecnología que realmente proporcione ventaja competitiva a los negocios (trabajar con los negocios y no contra ellos), además de dar a los usuarios todo lo que ellos necesitan.

La BRP ha presionado a los departamentos de Tecnología Informática de los negocios a ser por sí mismos rentables y comerciales al igual que ser más responsables hacia las necesidades y requerimientos de los usuarios. Los usuarios no son ya una multitud dócil para el Departamento de Tecnología Informática; es decir, los usuarios se han revelado. Ellos esperan respuestas rápidas y sistemas que les ayuden en los requerimientos del negocio.

4.7 Separación Histórica en los Equipos que Trabajan con Voz y Datos.

La computación y las telecomunicaciones comenzaron sus "vidas" comos dos disciplinas distintas. Los ingenieros en telecomunicaciones llevaban desarmadores y hablaban en baudios. Los aficionados a la computación vestían en "mangas de camisa" y se deslizaban en patines. La separación estaba latente, no podía esperar. A pesar de la diferencia en jerarquía, los dos equipos se han sobrepuesto tratando de evitar sus diferencias y trabajando por una solución común y compartida.

En el pasado fue la guerra. Pero ahora, en muchas compañías se ha dejado la batalla entre la Gerencia de Telecomunicaciones y la gerencia de Tecnología Informática.

4.8 Crecimiento en el Uso de Ordenadores Personales. Aumento del trabajo en Equipo

En la parte más difícil del conflicto, las dos gerencias han hecho crecer a sus equipos de trabajo de igual manera y de esta forma, han podido conocer lo suficiente acerca del trabajo de "los otros", como para comprometerse más y resolver así las problemáticas.

Pero con la digitalización de las telecomunicaciones, la introducción de redes en "estrella" y la conmutación en los circuitos de cómputo, el balance entre los equipos comenzó a cambiar.

El creciente número de equipos de escritorio subió al equipo de Tecnología Informática, mientras que el equipo de telecomunicaciones permanecía relativamente estático. Y, finalmente, cuando la tecnología de los equipos personales irrumpió en el mundo de las telecomunicaciones, los dos equipos de trabajo comenzaron a sobreponerse de forma considerable en cuanto a sus diferencias.

En la actualidad, se ha tratado de encontrar una razonable eficiencia en ambos grupos de trabajo. Y es importante reconocer que esto no representa el mayor logro que se haya podido dar. En vez de un intento por traer dos partes irreconciliables a platicar a la mesa, el proceso es más una integración del grupo que maneja voz con el grupo que trabaja con datos.

4.9 Manejando la Fusión de ambos Equipos de Trabajo, (Voz y Datos)

Para que el manejo de la fusión sea exitoso, se requiere involucrar y educar al equipo de voz en LAN y aplicaciones de datos, mientras que el equipo experto en datos tiene que aprender los fundamentos de las telecomunicaciones.

Con este entrenamiento en puerta, el equipo entero es preparado para un nuevo escenario en el cual la voz, al igual que otro contenido de multimedia como el video, es un ejemplo especializado del manejo de datos. Los sistemas tradicionales con PBX estarán soportados al lado de nuevos sistemas, requiriendo las gerencias de los equipos de voz y datos combinar el conocimiento de lo antiguo con lo moderno (lo viejo con lo nuevo). Pero esto no debe ser una dura carga. Moviendo los PBX basados en servidores se disminuirá la dificultad de transición en la gerencia de cada equipo de trabajo, y la situación más dura es igual a ser una compañía que intenta ir de un equipo centralizado en PBX hacia un ambiente de "VoiceLAN" en un único paso.

El punto importante a tratar aquí, es ahora dar un paso alejado del modelo centralizado de voz. Esto salvará a muchos de infartos en algunos años. En el "corazón" del manejo de "VoiceLAN" se tiene un reconocimiento muy complejo y elaborado para las máquinas de escritorio.

4.10 Expectativas de los Usuarios

Los usuarios, quienes hace sólo algunos pocos años fueron "enchufados" con sistemas de cómputo que sólo podían mostrar letras en color verde sobre fondo negro, ahora esperan que sus equipos realicen más "milagros" día a día.

Efectivamente, el usuario ha cambiado radicalmente su postura de una pregunta como ¿qué es esto?, y ahora, pregunta ¿por qué no puedo hacer esto o aquello?

4.11 Aplicaciones Multimedia.

Las aplicaciones Multimedia han dado mucho de que hablar en términos de tecnología. Ahora, se requiere una sinergia entre datos, voz e imagen para finalmente, combinarlos todos de manera eficiente para hacer más robustos los sistemas y resolver problemas de aplicación de los usuarios. A pesar de que Multimedia es un entorno relativamente nuevo, algunas aplicaciones están mostrando claramente sus beneficios.

4.12 Aprendizaje a Distancia

Por ejemplo, la capacitación es un tópico importante en los negocios de hoy, se tienen compañías tratando de seguir las habilidades que la actual mano de obra necesita en cuanto a capacitación. Con las normas establecidas, Multimedia puede dar el entrenamiento o capacitación a través del uso de video, tutores en "vivo", entrenamiento interactivo y la posibilidad de correr cursos donde actualmente el usuario está de forma presencial.

4.13 Voz y Video en la Red.

La educación a distancia es sólo la parte delgada de la cuña. Hay otras aplicaciones que pueden tomar "vida" en cuanto el video, la voz se puedan transmitir tan bien como se hace con los datos en los actuales equipos de escritorio. Esto es especialmente cierto para el Video sobre una LAN; ahora LAN ofrece un mayor ancho de banda, que el que tradicionalmente han usado las interfaces de la generación previa en sus comunicaciones. Esto ha mejorado las actuales aplicaciones. Algunas de las mejoras incluyen:

- Servicios nuevos de información como la posibilidad de conocer información financiera de primera mano.
- Videoconferencia en equipos de escritorio acoplados con técnicas compartidas semejantes a la del pizarrón blanco.

Estas aplicaciones traen un nuevo juego de requerimientos para la red. Éstas comparten un pequeño retraso en la transmisión.

4.14 Retrasos a través de los Equipos de la Red.

Cuando los datos (o voz en la forma de datos digitales) entran a un ruteador, éste tiene que esperar por todo el paquete para ser "tragado" antes de que el ruteador lo reenvíe. Hay retrasos en el equipo de cómputo, desde que la máquina tiene que esperar por el paquete de datos para que sea construido antes de ser enviado hasta otro tipo de retrasos inherentes a la transferencia. El diseño de la Red debe tomar en cuenta esos retrasos y tratar de eliminarlos en la medida de lo posible.

La mayoría de las plataformas que hay en la red, tienen su mayor retraso acumulado cuando los paquetes cruzan a través de los puentes ("bridges"); pero en la medida que esos retraso se puedan controlar como se hace en los ruteadores, esos sistemas serán más eficientes. Los paquetes en las redes tradicionales de datos tiene que esperar en una "cola" mientras los enlaces de la red están ocupados, esto retrasa la transmisión y hace menos eficiente la red.

Los problemas en el tráfico de Multimedia son dos: Primeramente, el retraso hace imposible que los enlaces corran en tiempo real, como lo demanda el video. Segundo, los paquetes retrasados por tiempo indeterminado en las "colas" significa que por ejemplo, un paquete importante consiga meterse detrás de los paquetes menos importantes que aún están esperando para ser cambiados, como puede ser la transferencia de un archivo que no es urgente. Claramente, "VoiceLAN" proporciona la solución a esos problemas

4.15 Mensajería Integrada

Las más diversas comunicaciones para negocios han llegado, las necesidades más grandes tendrán soluciones bajo un mismo entorno. Cada vez más popular y esencial para el correcto funcionamiento de los sistemas, es la mejor manera de tratar todas las distintas formas de tratar mensajes en una sola.

Por ejemplo, un colega puede enviar un mensaje vía telefónica, por fax, correo electrónico o correo de voz y en la parte de la recepción, se podrá tener la información en un equipo de escritorio. Esta forma de trabajar será todo un éxito y permitirá ver todos los mensajes a través de una sola vía de comunicación.

4.16 Calidad de Servicio, (QoS).

Al introducir video y voz en aplicaciones por la red, se requiere elevar los requerimientos de garantía de calidad de servicio en la red para garantizar las transferencias en forma adecuada, expedita y confiable.

4.17 Prioridades en "VoiceLAN".

Una buena solución de "VoiceLAN" debe agregar la posibilidad de que los paquetes de información de alta prioridad puedan saltar las "colas" de procesamiento. Lo anterior también permite a un equipo de escritorio especificar el aumento de ancho de banda

para cubrir sus necesidades y así, garantizar la correcta conexión del sistema mientras dura a operación con el ancho de banda adecuado.

4.18 Demanda de un gran Ancho de Banda para las Aplicaciones.

Mientras que el video y la voz requieren datos para ir a un equipo de escritorio a un paso regular, otras muchas aplicaciones semejantes no tienen restricciones aún y, sus beneficios se están incrementando muy rápidamente.

El ejemplo clásico es el de imágenes médicas, donde se requiere una alta resolución para que las imágenes sean posteriormente recuperadas, enviadas y finalmente, procesadas. Quizá, las mismas demandas puedan ser encontradas por la industria de la publicidad, donde avisos en colores intensos y otras aplicaciones gráficas de alta resolución demandan un gran ancho de banda. También se tienen aplicaciones de ingeniería muy parecidas a CAD/CAM.

Pero totalmente aparte de las especificaciones para las aplicaciones, los usuarios están esperando que los aumentos en el ancho de banda les ayude como por ejemplo, para transferir un archivo o para incrementar las prestaciones que se tiene actualmente en los equipos de escritorio. Por ejemplo, un archivo simple MPEG toma prácticamente todo el ancho de banda.

Claramente, la tecnología "VoiceLAN" tiene que proporcionar muy alta(s) velocidad(es) y proporcionar a los usuarios opciones escalables que permitan mantener el paso para cubrir sus expectativas.

4.19 Salvando Costos

Las comunicaciones en un ambiente de mezcla de multimedia hacen que los negocios operen de forma más rápida y eficiente. Esto se mostrará directamente en el modo más tangible: gastando menos dinero, pero consiguiendo más. Se tienen cuatro áreas principales donde la estrategia de "VoiceLAN" ofrece distintas ventajas de costo(s):

- Diversos Campos de Redes.
- Mejor Acceso a Redes de Área Amplia, (WAN). Estructuras más simples de Soporte.
- Una plataforma sobre Servidores normalizados para el uso de PBX.

4.20 Campo para las Redes

El aumento del ancho de banda que se puede suministrar en los entornas de redes sobre el "Backbone", es mucho más que un simple requerimiento de más ancho de banda para transmitir voz. Recuérdese que la Voz sólo requiere o necesita 64kbps, no se requiere pensar en el orden de megabits como cuando se piensa en datos. Absorbiendo la voz dentro de la transmisión de datos, puede eliminarse la necesidad de aumentar el sistema de alambrado para transmitir la Voz. Por ejemplo, el costo para poner un teléfono en un escritorio en términos de alambrado es de alrededor de $4,000.00 (M.N.).

4.21 Acceso a la Red de Área Amplia, (WAN)

El ancho de banda para transmitir en una Red de Área Amplia (WAN) cuesta dinero, por eso este servicio se renta. Los multiplexores pueden combinar voz y datos, pero no en un gran nivel de integración. Para integrar el tráfico de voz y datos en una fuente se requiere un buen enlace para establecer la comunicación.

Se podría pensar que "Frame Relay" es lo mejor. Y con aplicaciones integradas, como la anotación de voz en un documento; esto hace pensar en que varias partes de un mismo mensaje se pueden enviar juntas, peor en la realidad esto que puede ser sencillo de implantar requiere de cierta inversión adicional.

4.22 Mando Simplificado

La gerencia de equipos de trabajo (voz y datos) se pueden consolidar con un excelente entrenamiento y convertirse en un solo equipo y no en dos como ocurre en la actualidad. Esto podrá hacerse en la medida que los gerentes de ambos grupos traten de integrar protocolos comunes para la transmisión de voz y de datos, estos protocolos han sido desarrollados por la Tecnología Informática, y ahora se están comenzando a utilizar en el manejo de la Voz. Es decir, el trabajo final de los dos equipos de trabajo redundará en beneficios para los usuarios.

4.23 Plataformas de Servidor basadas en Normas para Voz.

Esto es para el futuro, pero no vale para la migración de PBX hacia arquitecturas normalizadas a menos que se disminuyan los costos para conmutar voz y llamadas de control. Implantando una estrategia de "VoiceLAN" se hará que los negocios comiencen de forma consolidada a través de una red que sea flexible en las aplicaciones y robusta en los equipos de infraestructura que utilice.

4.24 Perspectiva de los Proveedores de Tecnología en Redes Convergentes

No hay estrategia en computación o telecomunicaciones hoy en día que esté sólidamente basada en Sistemas Abiertos. La industria se ha dado cuenta de esto y las soluciones se pueden contar con los dedos de una mano.
Una de las mayores atracciones de "VoiceLAN" es que está concebido y construido sobre Sistemas Abiertos. Todos los componentes están construidos con elementos que se encuentran en el mercado. Por ejemplo, existen aplicaciones destacadas de Microsoft WindowS® que tienen aplicaciones comerciales que suministran una excelente opción en la infraestructura de "VoiceLAN".

4.24.1 Amplitud de la Comunidad de Punto de Venta

Una variedad de vendedores desde diferentes posiciones de la galaxia de la Tecnología Informática (IT), está impactando las normas de los Sistemas Abiertos (vendedores, así como los fabricantes tradicionales de PBX) son los que están comenzando con la

actualización primero, de los paquetes y programas. La amplitud de los vendedores en este mercado está creciendo enormemente, esto está dando como resultado un excelente nicho de soluciones al darse cierta competencia entre desarrolladores y vendedores de productos. La realización de las normas creará un campo fértil para dar valor agregado por parte de los proveedores hacia los usuarios; al igual que provocará en el corto tiempo, la integración de los sistemas.

4.24.2 La Industria toma Forma.

Se tienen tres grandes tipos de comercializadores de productos en cuanto a "VoiceLAN" se refiere:

- Los tradicionales proveedores de PBX.
- Los vendedores de sistemas operativos (incluyendo los sistemas operativos para redes, considerando los servidores; y los sistemas operativos para equipos de escritorio).
- Las aplicaciones de los desarrolladores.

El rol principal en esta fase del desarrollo de "VoiceLAN" ha sido tomado por los desarrolladores de sistemas operativos. Ellos han agregado capacidades para sus sistemas operativos, habilitando en pequeña escala grande s aplicaciones en el mercado de CTI's.

4.24.3 Aplicaciones de los Desarrolladores.

Las aplicaciones de los desarrolladores (proveedores) han sido apresuradas por el mercado para dar aplicaciones a los equipos de escritorio en primera instancia, principalmente aplicaciones telefónicas como marcación fuera de pantalla.

4.24.4 Proveedores de PBX.

Algunos proveedores de PBX están experimentando con incluir en sus equipos posibilidades de uso de LAN en forma limitada dentro de los módulos de PBX, pero la tendencia es claramente en la dirección opuesta, con la total funcionalidad de PBX en LAN; rápidamente LAN podrá entrar en los arreglos PBX.

4.24.5 Tendencia General.

La tendencia general es la aceptación de la llamada "arquitectura sin propietario" y la gradual apertura de las arquitecturas propietarias de paquetes y programas. Una forma de verlo es decir que la matriz de conmutación se está separando desde el resto de los PBX, dando la idea de un conmutador universal. Arquitectura dedicada puede ubicar la conmutación de circuitos en tiempo real, mientras que los programas de control de llamada(s) transfieren sobre las plataformas normalizadas de los servidores de la red. El PBX se está convirtiendo en un PBX virtual dentro del ambiente de LAN.

4.24.6 Normas y Organizaciones que las Regulan

4.24.6.1 Ethernet.

Ethernet en su entorno original de 10Mbits/segundo se controla a través de las normas de la IEEE y de ISO. Ethernet es ampliamente aceptado y comprendido. Esta es la principal solución en el mercado de LAN. El limitado rango de aplicaciones ha sido mejorado al usar las recomendaciones 10base T y por 100base T brindando conmutación y alta velocidad. Ethernet recuerda las colisiones; sin embargo, se considera que ya no es tan propenso a esa situación.

4.24.6.2 Foro ATM.

El poder para manejar la Norma ATM en el mundo corporativo de la Tecnología Informática ha sido el objetivo del Foro ATM, el cual ha tomado los primeros conceptos desarrollados por la industria telefónica internacional, ha acelerado las normas de trabajo y continúa considerando un juego de especificaciones que sean coherentes hacia los desarrolladores independientes.

El Foro ATM agregó sobre su Norma para 155 Mbits/segundo la Categoría 5 UTP en 1994. Después de eso, se decidió normalizar 51 Mbits/segundo sobre la Categoría 3 UTP en Noviembre de 1993.

4.24.6.3 Voz sobre ATM.

La Norma proyectada para Voz sobre ATM, es A TM Adaption Layer 1 (AAL 1). A la hora de escribir este artículo, AAL 1 aún no es una Norma Ratificada, sin embargo algunos proveedores queines desean ser los iniciadores de la Convergencia para Redes han adoptado soluciones que todavía no han sido liberadas. El Comité del Foro ATM está desarrollando modificaciones a esta Norma. Voice Telephony Over ATM (VTOM).

4.24.6.4 Alianza A TM para Equipos de Escritorio

Las Normas 155 Mbit/segundo y 51 Mbit/segundo para ATM basadas en alambrado de cobre se deben a las telecomunicaciones originales de ATM, y esto se muestra en el espacio de encabezados que suponen. Para contrarrestar esto, una Organización llamada "Alianza A TM para Equipos de Escritorio" fue formada alrededor de los equipos IBM para una velocidad de 25 Mbitlsegundo sobre una Categoría 3 de UTP usando tecnología de transmisión traida y probada en Redes de Área Local con topología Token Ring. Esto ha dado como resultado una baja en los costos. El Foro ATM adoptó la Norma de la Alianza a principios de 1995.

4.24.6.5 Normas para Vídeo

Uno de los objetivos del Foro ATM es Normalizar el Transporte de Video sobre A TM, pero esto puede tomar algún tiempo.

Un simple trabajo con alta calidad de video requiere un ancho de banda de más de 100 Mbit/segundo por lo tanto, algoritmos de compresión de video están siendo utilizados. Escoger el tipo de compresión depende de la aplicación.

Una conferencia de video puede correr alrededor de 128 kbitlsegundo, de esta manera la Norma H.261 es suficiente para establecer conexiones RDSI, que van sobre una WAN. Para altas velocidades se puede escoger de entre tres Normas:

- Correr desde 1.5 Mbit/segundo a 15Mbitlsegundo utilizando una distribución de video en formato MPEG-2 para aplicaciones tales como Playback y Video Server.
- Para videoconferencias se utilizan el formato JPEG que también corre desde 1.5 Mbit/segundo hasta 15 Mbit/segundo, pero con procesamiento simétrico.
- Existe un estándar de Intel (Indeo), diseñado para video basado en LAN y utilizando una velocidad de 1.2 Mbit/segundo.

CONCLUSIONES

La aplicación del Protocolo IP (Internet Protocolo) se está extendiendo a un gran número de elementos, uno de éstos, es el que se utilizó como base de estudio en el presente trabajo que es, poder realizar llamadas telefónicas a través de una red de Internet, permitiendo optimizar los recursos de la red que se encuentran ya en operación y así reducir los gastos de operación y de consumo.

En los primeros capítulos se habló de los modelos que se han utilizado por varios años en la implantación de redes de datos, desde las primeras redes X.25 hasta las redes OSPF para grandes usuarios con técnicas de enlace como Frame Relay, ATM y Protocolo IP, configuradas como redes virtuales VPN (Virtual Private Network). Hoy en día crece más la necesidad de contar con elementos que tengan sistemas operativos que manejen Protocolo IP, desde, teléfonos celulares, aparatos domésticos hasta elementos de redes locales, redes de área abierta, conmutadores digitales, centrales telefónicas y lo más usual que son los Ordenadores.

En el mercado de las telecomunicaciones están disponibles una gran cantidad de productos preparados para trabajar bajo el Protocolo IP, estos elementos forman enlazados entre sí lo que hoy se conoce como Redes Convergentes, que es la integración en una misma red, de voz, datos y video, utilizando un protocolo común entre sí, que en este trabajo se menciona como el H.323. Este Protocolo se utiliza para estandarizar la transmisión y manejo de voz sobre IP. El manejar voz sobre IP está pasando a ser una alternativa en la reducción de costos en llamadas de larga distancia (principalmente) en redes corporativas, que en la actualidad es una carga económica para cualquier empresa.

Los fabricantes que cuentan con equipos que manejen el Protocolo H.323 tienen la oportunidad de competir en el mercado de redes de convergencia, entre estos están, Mitel™, Ericsson™, LucenFM, Cisco Systems Inc. TM, Siemens™, y Alcatel™, entre muchos otros.

H.323 permite utilizar los recursos de una red convencional para instalar elementos que manejen este Protocolo, como son equipos de videoconferencia, aparatos telefónicos y telefonía por ordenador; sin necesidad de utilizar un puerto de red exclusivo o adicional a éste, por ejemplo para un aparato telefónico, ayudando así a los nuevos esquemas dinámicos en las empresas, en las cuales, el personal frecuentemente cambia de área de trabajo; que va desde moverse simplemente de un lugar a otro dentro de la misma área de trabajo, hasta moverse a otro edificio.

El avance tecnológico y el mercado día a día cambian, mejorando y exigiendo a los fabricantes el perfeccionamiento de sus productos para utilizar menos recursos a un menor costo y, con mayores facilidades; esto trae en consecuencia que los organismos (ITU, IETF) que rigen el mercado de las telecomunicaciones, apliquen nuevos protocolos para estandarizar sus productos como es el caso del Protocolo SIP ("Session Initiation Protocol"), que en un tiempo quizá, reemplace al Protocolo actual H.323.

Es importante recalcar que en toda red es imprescindible la seguridad y la optimización de ancho de banda, en la cual se tienen herramientas como codificadores (G.711, G.729, G.723), que permiten utilizar el ancho de banda como mejor se adecue a la red. El

etiquetado de los paquetes y la encriptación de voz, (que es otra parte importante en la seguridad para asignar la prioridad en la red sobre el envío de los paquetes de datos) y así garantizar el envío de paquetes de voz al momento de generar una llamada telefónica.

Tomando en cuenta la investigación realizada en el presente trabajo, permitirá comprender los elementos que componen una Red VPN para el manejo de VoIP (Voz sobre IP), así como los puntos importantes para alcanzar las prestaciones de la red, para así poder reemplazar una red tradicional TDM, a una red virtual VPN.

Desde luego, la creación de redes integradas empleando interfases y protocolos comunes, aunque sin duda resultará benéfica, no es la única meta de estas nuevas tecnologías. Otro objetivo importante es ofrecer más capacidad de rendimiento (en bit/seg) para aplicaciones de usuario y realizar las operaciones de red con mayor rapidez a favor de las aplicaciones.

Esto implica que las tecnologías convergentes se han diseñado para ofrecer alto rendimiento, con velocidades de transmisión muy altas y con retardos muy bajos. Efectivamente, los estándares integrados, con alto rendimiento y bajo retardo, son las piedras angulares de estas tecnologías.

Otra meta importante de estas tecnologías es apoyar cualquier tipo de aplicación, como voz, video, música, facsímil y telemetría. Un término apropiado para este servicio es redes de multiaplicación, aunque casi todo mundo usa el término multimedia. La implantación económica de las redes multimedia está resultando ser uno de los mayores retos que enfrenta la industria.

Desde el punto de vista del proveedor de redes, otro objetivo importante de las tecnologías de telecomunicación que están surgiendo (al menos de algunas de ellas), es proporcionar más y mejores herramientas de gestión de redes. A primera vista, este factor tal vez no signifique mucho para un usuario final, pero dichas herramientas permiten al proveedor de redes, monitorear minuciosamente los recursos de la red y ofrecer un servicio robusto y relativamente libre de errores a las aplicaciones de usuario.

En contraste con los sistemas basados en T1/E1, que tienen funciones de gestión de redes muy limitadas, las nuevas tecnologías de comunicaciones utilizan cerca del 5% del ancho de banda de la red para la administración. Puesto que los canales de comunicaciones son de fibra óptica, se cuenta con suficiente ancho de banda para apoyar esta importante operación.

Por último, otra de las principales metas de las tecnologías de comunicación convergentes es el suministro de interconexiones "sin costuras" entre el "hardware/software" de las redes y entre las redes mismas. Se usa aquí el término "sin costuras" para denotar que un usuario final (incluso un administrador de red), no es consiente de que el tráfico de usuarios se transporta por equipos de diferentes fabricantes y por diferentes redes. Las redes pueden ser locales o remotas, e incluir equipo y programas de un solo fabricante o de muchos. No obstante, las operaciones son transparentes para el usuario (e idealmente, para un administrador de red).

GLOSARIO DE TÉRMINOS.

2B+D	Codificación de línea: 2B1Q. 2B+D.- Canales B, By D.
AC	Control de Acceso, (Access Control)
ACF	Campo de Control de Acceso, (Access Control Field).
ACK	Acuse de Recibo, (Acknowledgement).
ADM	Multiplexor de Agregar-Soltar, (Add-Drop Multiplexer).
ADPCM	Modulación Adaptativa por Código de Pulso Diferencial (Adaptive Differential Pulse Code Modulation).
ARP	Protocolo de Resolución de Dirección, (Address Resolution Protocol).
ARPA	Agencia de Investigación de Proyectos Avanzados, (Advanced Research Projects Agency).
ARQ	Requerimiento de Repetición Automático, (Automatic Repeat Request).
ASCII	Código Estándar Americano para el Intercambio de Información, (American Standard Code for Information Interchange).
ATM	Model de Transferencia Asíncrono, (Asynchronous Trabsfer Mode).
SER	Tasa de Errores de Bit (Bit Error Rate). BOOTP.- Bootstrap Protocol.
BRI	Interfase de Tasa Básica, (Basic Rate Interface).
CSR	Tasa de Bit Constante, (Constant Bit Rate).
CCS	Señalización de Canal Común, (Common Channel Signaling).
CCITT	Comité Consultivo Internacional de Telegrafía y Telefonía, (Committee Consultative Internacional for Telegraphy and Telephony).
CDMA	Acceso Múltiple por División de Código, (Code Oivision Multiple Access).
CIB	Bit Indicador de CRC 32, (CRC 32 Indicator Bit).
CIR	Tasa de Información Comprometida, (Commited Information Rate)
CNM	Gestión de Red de Cliente, (Customer Network Management).
COCF	Función de Convergencia Orientada a Conexiones, (Connection-Oriented Convergente Function).

COM	Continuación del Mensaje (Continuation of the Message).
CPCS	Subcapa de Convergencia de Parte Común, (Common Part Convergente Sublayer).
CPCS-UU	Subcapa de Convergencia de Parte Común-Indicación Usuario a Usuario, (Common Part Convergente Sublayer-User to User Indication).
CRC	Verificación de Redundancia Cíclica (Cyclic Redundancy Check)
CSMA/CD	Acceso Múltiple por Detección de Portadora/Detección de Colisiones, (Carrier Sense Multiple Access/Co/lision Oetect)
CSTA	Aplicaciones Telefónicas Soportadas por Ordenador, (Computer Supported Telephony Applications).
CSU	Unidad de Servicio de Canal, (Channel Service Unit).
DECT	Telecomunicaciones Digitales Europeas sin Cordón, (Digital European Cordless Telecommunications).
DLCI	Identificador de Conexión de Enlace de Datos, (Data Link Connecuonldenufie)·
DNS	Sistema de Nombres de Dominio, (Domain Name System). DP.- Punto de Detección, (Detectionon Point).
DPDU	PDU de Capa de Enlace de Datos, (Data Link Layer PDU). DPSK.- PSK Differential, (Differential PSK).
DSI	Interpolación Digital de Voz, (Digital Speech Interpolation).
DSP	Parte Específica para el Dominio, (Domain Specific Part).
DSU	Unidad de Datos de Servicio, (Data Service Unit).
DTE	Equipo Terminal de Datos, (Data Terminal Equipment).
DTI	Departamento de Comercio e Industria, (Department of Trade and Industry).
DTMF	Tono Dual, Múltiple Frecuencia, (Dual Tone Multiple Frecuency)
DNA	Arquitectura Digital de Red, (Digital Network Architecture).
EC	Comisión Europea, (European Commission).
ECMA	Asociación de Fabricantes de Equipo de Cómputo Europea, (European Computer Manufacturers Association).

ECSA	Asociación de Normas Portadoras de Intercambio, (Exchange Carriers Standards Association).
EOM	Fin del Mensaje, (End of Message).
ETSI	Instituto de Normas de Telecomunicaciones Europeas, (European Telecommunications Standard Institute).
FCC	Comisión Federal de Comunicaciones, (Federal Communicauons Commission).
FDDI	Interfase de Datos Distribuida por Fibra, (Fiber Distribuited Data Interfaz).
FEC	Control de Errores hacia Adelante, (Forward Error Control).
FEC	Corrección de Errores hacia Adelante, (Forward Error Correction).
FECN	Bit de Notificaciones Explícita de Congestionamiento hacia Adelante, (Forward Explicit Congestion Notification Bit).
FRF	Foro de Frame Relay, (Frame Relay Forum).
FTP	Protocolo de Transferencia de Archivos, (File Transfer Protocol).
GSM	Grupo Especial Móvil, (Groupe Speciale Mobile)
GUI	Interfase Gráfica de Usuario, (Graphical User Interface
HCS	Secuencia de Verificación de Encabezado, (Header Check Sequence).
HDCL	Control de Enlace de Datos de Alto Nivel, (High Level Data Link Control).
HDSL	Línea de Suscriptor Digital con Alta Tasa de Bits, (High Bit-Rate Digital Subscriber Line).
HTTP	Protocolo de Transferencia de Hipertexto, (Hyper Texte Transfer Protocol).
ICF	Función de Convergencia Isócrona, (lsochronous Convergence Function).
ICI	Interfase de Portadora de Intercambio, (lnterchange Carrier Interfaz).
ICIP	Protocolo ICI, (lCI Protocol).
IEEE	Instituto de Ingenieros en Electricidad y Electrónica, (Institute of Electrical and Electronic Engineers).

IGMP	Internet Group Multicast Protocol. IKE.- Internet Key Exchange.
IMPDU	Unidad de Datos de Protocolo MAC Inicial, (Inicial MAC Protocol Data Unit).
IP	Protocolo de Internet, (Internet Protocol).
IPv4	Protocolo de Internet Versión 4, (Internet protocol Version 4).
IPv6	Protocolo de Internet Versión 6, (Internet protocol Version 6)
ISDN	Red Digital de Servicios Integrados, (Integrated Services Digital Network).
ISO	Organización Internacional de Normas, (Internacional Standards Organization).
ISP	Internet Service Provider.
ISUP	Parte de Usuario de ISDN, (ISDN User Part).
ITU	Unión Internacional de Telecomunicaciones, (Internacional Telecommunications Union).
LAN	Redes de Área Local, (Local Area Networks).
LAPB	Procedimiento de Acceso a Enlaces Balanceado, (Link Access Procedure Balanced).
LAPD	Procedimiento de Acceso a Enlaces para el Canal O, (Link Access Procedure for the D Channel).
LT	Terminación de Línea, (Line Termination).
MAN	Red de Área Metropolitana, (Metropolitan Area Network).
MIB	Base de Información de Gestión, (Management Information Base)
MID	Identificador de Mensaje, (Message Identifier).
MMDS	Servicio de Distribución Multipunto Multicanal, (Multipoint Multichannel Distribution Service).
MPLS	Mufti Protocol Laber Switching.
MSU	Unidad de Señal de Mensaje, (Message Signal Unit).
MTP	Parte de Transferencia de Mensajes, (Message Transfer Part).
N-ISDN	ISDN de Banda Angosta, (Narrowband ISDN).

NAK	Acuse de Recibo Negativo, (Negative Acknowlegment)
NEI	Identificador de Entidad de Red, (Network Entity Identifier)
NIU	Unidad de Interfase de Red, (Network Interface Unit). MNS.- Network Management System.
NNI	Interfase Red-Nodo (Network-Node Interface). NNI.- Interfase Red-Red, (Network-to-Network Interface). NOC.-Network Operations Center.
OSPF	Abrir Primero el Trayecto más Corto, (Open Shortest Path First).
PABX	Private Automatic Branch Exchange. PBX.- Private Branch Exchange.
PCI	Protocol Control Information.
PCM	Modulación por Código de Pulso, (Pulse Code Modulation)
PCMCIA	Personal Computer Memory Card Internal Associated
PHY	Capa Física, (Phisical Layer).
PPTP	Poin-to-Point Tunneling Protocol.
PRI	Interfase de Tasa primaria, (Primary Rate Interface).
PSK	Modulación por Desplazamiento de Fase, (Phase Shift Key)
PSTN	Public Switched Telephone Network.
PT	Tipo de carga Útil, (Payload Type).
PTT	Protocolo para Telefonía y Telegrafía.
PVC PVN	Circuito Virtual Permanente, (Permanent Virtual Circuit) Red Virtual Permanente, (Private Virtual Network).
QAM	Modulación de Amplitud y Cuadratura, (Quadrature Amplitude Modulation).
QoS	Calidad de Servico, (Quality of Service).
OPSK	Modulación de Cuadratura y Desplazamiento de Fase, (Quadrature Phase Shift Keyed).
RQ	Contador o Temporizador de Solicitudes, (Request Timer).
SAP	Punto de Acceso al Servicio, (Service Access Point).

SAPI	Identificador de Punto de Acceso al Servicio, (Service Access Point Identifier) .
SDDI	Especificación de Par trenzado Blindado
SDH	Jerarquía Digital Síncrona, (Synchronous Digital Hierachy)
SIR	Tasa de Información Sostenida, (Sustained Information Rate).
SNMP	Protocolo Simple de Gestión de Redes, (Simple Network Management Protocol).
SONET	Red Óptica Síncrona, (Synchronous Optical Network).
SPVC	Circuito Virtual Semipermanente, (Semipermanent Virtual Circuit)
SQL	Standard Query Language.
STDM	Multiplexor Estadístico por División en el Tiempo, (Statistical Time Division Multiplexer).
SVC	Circuito Virtual Conmutado, (Switched Virtual Circuit).
TCP	Protocolo de Control de Transmisión, (Transmisión Control Protocol)
TDM	Multiplexión por División en el Tiempo, (Time Division multiplexing)
TDMA	Acceso Múltiple por División del Tiempo, (Time Division Multiple Access).
TELNET	Protocolo TELNET
ToS	Tipo de Servicio, (Type of Service)
TTY	Teletipo
UI	Información no Numerada, (Unnumbered Information). UDP.- User Datagram Protocol.
ULP	Protocolos de Capa Superior, (Upper Layer Protocols)
UTP	Par Trenzado no Blindado, (Unshielded Twisted Pair).
VC	Canal Virtual, (Virtual Channel).
VCC	Conexión de Canal Virtual, (Virtual Channel Connection)
VLAN	Virtual LAN
VPC	Conexión de Trayectoria Virtual, (Virtual Path Connection)

VPN	Red Privada Virtual, (Virtual Private Network).
WAN	Red de Área Amplia o Extensa, (Wide Area Network)
WLAN	Wireless LAN

BIBLIOGRAFÍA

Banke, A. Y Badrinath, B. (1995). **I-TCP: Indirect TCP for Mobile Hosts.** New York: Prentice- Hall.

Barlow, J. P. (1995). **Property and Speech: Who Owns What You Say in Cyberspace.** USA: Commun of the ACM, vol. 38.

Bates, R. J. (1994). **Wireless Networked Communications.** New York: Mc Graw-Hill.

Beltrao, A. (1998). **Redes de Computadoras. Protocolos Y Prestaciones.** México: Mc Graw-Hill. Primera Edición.

Bertsekas D. Y Gallager R. (1997). **Data Networks.** New Jersey: Prentice-Hall, Englewood Cliffs.

Black, U. D. (1994). Emer~in~ **Communication** Technolo~ies. New Jersey: Prentice-Hall, Englewood Cliffs.

Black, U. D. (1995). **TCP/IP and Related Protocols.** New York: Mc Graw-Hill.

Black, Ulysees. (1999). **Redes de Computadoras: Protocolos, Normas e Interfases.** México: Mc Graw-Hill.

Carl-Mitchell, S. y Quarterman, J. S. (2001). **Practical** Internetworkin~ **with TCP/IP and UNIX.** New Jersey: Addisson Wesley.

Clark, D. (1998). **Window and** Acknowled~ement Strate~y **in TCP.** New Jersey: Prentice Hall, Englewood Cliffs.

Comer D. E. (1995). Internetworkin~ **with TCP/IP.** New Jersey: Prentice-Hall, Englewood Cliffs.

Comer, D. (1996). **Redes Globales de Información con Internet Y TCP/IP: Principios Básicos, Protocolos Y Arquitectura.** México: Pearson-Prentice Hall.

Conant, G. E. Y Wecker, S. (1996). DNA: An Architecture for Hetero~eneous Computer Networks. Toranto: ICCC.

De Prycker, M. (1993). Asynchronous Transfer Mode Solution for Broadband ISDN. UK: Ellis Horwood, Second Edition.

De Prycker, M. (1993). Asynchronous Transfer Mode. New York: Ellis Horwood. Second Edition.

Gerla, M. y Kleinrack, 1. (1998). Flow Control: A Comparative Survey. IEEE Transactions on Communications. USA: IEEE.

Giozza, W.; De Araújo, J. y Moura, J. (1996). Redes Locales de Computadores: Aplicaciones y Tecnolo~ías. México: Mc Graw-Hill.

González, Néstor. (1999). Comunicaciones y Redes de Procesamiento de Datos. México: Mc Graw-Hill.

Green, Paul. (1992). **Computer Network Architectures and Protocols.** New York: Plenum Press, Second Edition.

Huitema, C. (1995). Routin~ **in the Internet.** New Jersey: Prentice-Hall, Englewood Cliffs.

International Organization for Standarization. (1987a). Information Processing Systems -Open Systems Interconnection- **Specification of Basic Specification of Abstract Svntax Notation One (ASN.1).** International Standar number 8824, ISO, Switzerland.

International Organization for Standarization. (1987b). Information Processing Systems -Open Systems Interconnection - **Specification of Basic** Encodin~ **Rules for Abstract Svntax Notation One (ASN.1).** International Standard number 8825, ISO, Switzerland.

International Organization for Standarization. (1988a). Information Processing Systems -Open Systems Interconnection- Mana~ement **Information Protocol Definition. Part 2: Common** Mana~ement **Information Protocol.** Draft International Standard number 9596-2.

Latif, A, Rowlance, E. J. Y Adams, R. H. (1992). **The IBM LAN** Brid~e. **IEEE** Network Magazine.

Laudon, K. C. (1995). "Ethical Concepts and Information Technology". **Comun of the AMC,** vol. 38. pp. 33-39, Dec. 1995.

Madrón, A (1997). **Redes de Computadoras.** México: Mc Graw-Hill. Menascé, D. A Y Schwabe, D. (1994). **Redes de Computadoras.** Buenos Aires: Ed. Campus. Milenkovic, Anton. (1998). **Sistemas Operativos.** México: Mc Graw-Hill.

Novel, Inc. (1995). **Introducción a Novel: Manual de Referencia.** México: Novellncorporation.

Perlman, R. (1992). **Interconnections:** Brid~es **and Routers.** New Jersey: Addisson Wesley.

Rase, M. (1993). **The Internet** Messa~e. New Jersey: Prentice Hall, Engewood Cliffs.

Rosenthal, R. (Ed.). **The Selection of Local Area Computer Networks.** USA: National Bureau of Standards Special Publications.

Santifaller, M. (1994). **TCP/IP and ONC/NFS.** New Jersey: Addisson Wesley.

Schwartz, M. y Stern, 1. (1999). **IEEE Transactions on Communications.** USA: COM-28 (4), 539-552.

Sipior, J. C. y Ward, B. 1. (1995). «The Ethical and Legal Quandary of Emails Privacy ». **Comun ofthe** AMC, vol. 38, pp. 48-54, Dec. 1995.

SNA, (1995). **IBM System Network Architecture - General Information.** North Carolina: IBM System Development Division, Publications Center Department.

Stallings, W. (1995a). **ISDN and Broadband ISDN with Frame Relay and A TM.** New Jersey: Prentice Hall.

Stallings, W. (1995b). **Network and Internetwork Security.** New Jersey: Prentice Hall.

Stallings, W. (1995c). **Protect your Privacy: The PGP User's Guide.** New Jersey: Prentice Hall

Stallings, W. (1999). **Data and Computer Communications.** New York: Macmillan Edition

Tanembaum Andrews (1997). **Redes de Computadoras** México:Pearson/Prentice-Hall. Tercera Edición

Tanenbaum, A. (1981). **Computer Networks: Toward Distributed** Processin~ **Svstems.** New Jersey: Prentice-Hall, Englewood Cliffs.

Tanenbaum, A. S. (1991). **Computer Networks.** New Jersey: Prentice Hall, Ebglewood Cliffs.

Villamizan, C. y Song, C. (1995). Hi~h **Performance TCP in ANSNET.** USA: Mc Graw-Hill.

Yeh, H., Hluchyj, M y Acampora, A. (1997). **The Knockout Switch: A Simple, Modular Architecture for** Hi~h-Performance **Packet** Switchin~. USA: IEEE Edition

OBJETIVO GENERAL.

Presentar los conceptos generales de las Redes de Área Local (LAN), así como los elementos referentes a la Transmisión de Datos y de Voz sobre Enrutamiento IP, aplicados en una Red Convergente utilizando protocolos distintos.

OBJETIVOS PARTICULARES.

1.- Presentar y analizar los conceptos básicos de las Redes de Área Local (LAN).

2.- Analizar los conceptos y elementos inherentes a los fundamentos de la Transmisión de Datos sobre Tecnología IP, (DoIP).

3.- Analizar los conceptos y elementos inherentes a los fundamentos de la Transmisión de Voz sobre Tecnología IP, (VoIP).

4.- Analizar los conceptos y elementos inherentes a los fundamentos de la Transmisión de Voz y Datos sobre Enrutamiento IP en una Red Convergente utilizando Protocolos distintos.

JUSTIFICACIÓN.

A manera de Justificación del presente trabajo de Tesis se menciona la tendencia actual a que los Sistemas de Ordenadores, se configuren a modo de Red, para obtener un alto índice de rendimiento y rentabilidad de los equipos así configurados y operados.

Las Redes de Área Local (LAN) están constituidas por ordenadores, tarjetas de interfase de red, medios de red, dispositivos de control del tráfico de la red y dispositivos periféricos. Las LAN permiten a las empresas que emplean tecnología informática compartir de forma eficiente elementos tales como: archivos, impresoras y posibilitar las comunicaciones como el correo electrónico. Unen entre sí datos, comunicaciones, ordenadores, estaciones de trabajo y servidores de archivos. Las LAN están diseñadas para lo siguiente:

- Operar dentro de una zona geográfica limitada.
- Permitir a muchos usuarios acceder a medios de alto ancho de banda
- Proporcionar conectividad, a tiempo completo, a los servicios locales.
- Conectar físicamente dispositivos adyacentes.

Como resultado de estar conectado en red, los ordenadores, las impresoras y otros dispositivos de una Red de Área Amplia (WAN) se pueden comunicar entre sí para compartir información y recursos, así como aceder a Internet. Entre algunas de las tecnologías WAN habituales se incluyen:

- Los Módems analógicos.
- RDSI o ISDN (Red Digital de Servicios Integrados) .
- DSL (Línea de Abonado Digital, Digita! Subscriber Une) . ., Frame Relay .
- ATM (Modo de Transferencia Asíncrona) .
- Las series de portadora T (Estados Unidos de América) y E (Europa): T1, E1, T3, E3, etcétera.
- Sonet (Red Óptica Síncrona): STS-1 (OC-1), STS-3 (OC-3), etcétera.

El almacenamiento y análisis de Información ha sido uno de los grandes problemas a que se ha enfrentado el hombre desde que inventó la Escritura. No fue sino hasta la segunda mitad del Siglo XX que el hombre ha podido resolver en parte este problema gracias a la invención del Ordenador.

En la década de los años cincuenta, el hombre dio un gran salto en este problema al inventar el Ordenador. Ahora la Información podía ser enviada en grandes cantidades a una localidad central donde se realizaba el procesamiento de la misma. El problema era que esta Información (que se encontraba en grandes cajas repletas de tarjetas) tenía que ser acarreada al Departamento de Procesamiento de Datos.

Con la aparición de la Terminales o Estaciones de Trabajo en la década de los sesenta, se logró la comunicación directa entre los Usuarios y la Unidad Central de Proceso, logrando con esto una comunicación más rápida y eficiente, pero se encontró con un problema, entre más terminales y periféricos se agregaban a los Ordenadores, la velocidad de respuesta de las mismas comenzó a decaer.

Hacia la mitad de la década de los años setenta, la refinada Tecnología del Silicón e integración en miniatura permitió a los fabricantes de Ordenadores construir más "Inteligencia" en máquinas más pequeñas.

Estas máquinas llamadas micra-ordenadores, descongestionaron a las viejas máquinas centrales y ahora cada Usuario tenía su propio microordenador en su escritorio.
A principio de la década de los años ochenta, los microordenadores habían revolucionado por completo el concepto de la computación electrónica, así como sus aplicaciones y mercados. Los Gerentes de los Departamentos de Informática fueron perdiendo el Control de la Información ya que ahora el proceso de la Información no estaba centralizada.

Como la mayoría de los Proyectos de Ingeniería; independientemente de la disciplina, las Redes de Ordenadores cuentan con una serie de Estándares o Normas que definen su funcionamiento en todos los aspectos. Por ello se establecen los Modelos de Referencia cuya finalidad se divide en dos puntos básicos:

1.- Flexibilizar la implantación de una Red dividiéndola en Capas ó Niveles de Programas y Paquetes ("Software') interactuando jerárquicamente.
2.- Estandarización de los diversos fabricantes tanto de Arquitectura de Sistemas ("Hardware") como de Programas y Paquetes ("Software") del Modelo de Referencia más utilizado en la actualidad.

Además, el desarrollo de las Redes de Área Local (LAN) a mediados de la década de 1980, ayudo a cambiar la forma de pensar de los Ordenadores. Como ordenadores; a la forma en que nos comunicamos entre ordenadores y usuarios y por que se hace de ese modo (Rosenthal, 1982)

Las Redes de Área Local (LAN) son particularmente importantes, ya que es una Red de Área Local, la que puede ser conectada a muchas Estaciones de Trabajo como la primera fase de un entorno distribuido de Redes y Operaciones de Ordenadores de mayor magnitud.

Así mismo, las Redes de Área Local (LAN) son importantes para muchas Organizaciones de menor tamaño porque son la ruta a seguir hacia un Entorno de Ordenadores Multi-usuarios, distribuido y capaz de comenzar en forma modesta, pero también de extenderse a medida que aumenten las necesidades de la Organización.

Como se puede apreciar, una de las influencias más profundas en el desarrollo de las Redes de Área Local (LAN) ha sido la adopción de "Estándares" Nacionales e Internacionales ("Estándares" que incluso los gigantes de la Industria encuentran difícil de pasar por alto).

Las Redes que transmiten Información pueden organizarse en diversas formas. Al comienzo de la década de 1980, era imposible distinguir entre lo que se ha llamado "Redes Locales" y lo que se denominara "Redes Globales".

En muchas Redes Locales, todos los nodos son Ordenadores; aunque no hay nada inherente en la Tecnología que requiera tal condición, pese a que la existencia de grandes números de Ordenadores ha sido probablemente un factor importante en el desarrollo de las Redes de Área Local (LAN).

Las Redes de Área Local (LAN) fueron estructuradas con el aspecto de la conectividad en mente. Las Redes Locales pueden servir a usuarios locales, se pueden interconectar o bien pueden ser nodos de una Red Global.

Las Redes Locales pueden tener radios que varían de algunos cientos de metros a cerca de 50 kilómetros. Las Redes Globales se pueden extender por todo el mundo, de ser necesario.

Las Redes de Área Local (LAN), se describen a veces, como aquellas que:
"Cubren una área geográfica limitada, donde todo nodo de la Red puede comunicarse con todos los demás y no requiere un nodo Ó procesador central".

Además, una Red de Área Local (LAN) es una Red de Comunicación que puede ofrecer intercambio interno entre Medios de Voz, Datos de Ordenador, Procesamiento de Palabras, Facsímil, Videoconferencias, Transmisión Televisiva de Vídeo, Telemetría y otras formas de Transmisión Electrónica de Mensajes. Una Red de Area Local (LAN) puede clasificarse además como:

1.- Intrainstitucionales, de propiedad privada, administradas por el usuario y no sujetas a la regulación de la FCC. De esta categoría se excluyen a Empresas de servicios comunes, tales como Sistemas Telefónicos Públicos y Sistemas Comerciales de Televisión por Cable.

2.- Integradas a través de la interconexión vía un medio estructural continuo; pueden operar múltiples servicios en un mismo juego de cables.

3.- Capaces de ofrecer conectividad global.

4.- Que soportan Comunicaciones de Datos a baja y alta velocidad. Las Redes de Área Local (LAN) no están sujetas a las limitaciones de velocidad impuestas por Empresas de servicios comunes tradicionales y pueden ser diseñadas para soportar dispositivos cuya velocidad va de 75 Baudios con base en casi cualquier Tecnología, a cerca de 140 Mbaudios en el caso de una Red de Área Local (LAN) de Fibra Óptica disponibles en el Mercado.

5.- Disponibles en el Mercado (al alcance de el Comprador). El Mercado de las Redes de Área Local (LAN) sigue siendo volátil, sin menospreciar los productos que ofrece IBM, muchos sistemas siguen siendo diseñados por pedido. Incluso, los productos ya anunciados pueden encontrarse aún en la fase de prueba.

Como la Red de Área Local (LAN) es más un concepto que un producto, el término "disponibles en el mercado", debe interpretarse de la manera siguiente:

Los componentes de las Redes de Área Local (LAN) que ofrecen conexiones de dispositivos a un medio físico, como un Sistema de Televisión por Cable (CATV), son las que se pueden conseguir realmente en el Mercado.

La Justificación más importante para este trabajo es que las Redes de Área Local (LAN) son únicas porque simplifican procesos sociales. Las Redes Globales se implantan para hacer un uso más efectivo en costo de "Mainframes" o Macroordenadores costosos. Las Redes de Área Local (LAN) se implantan para hacer un uso más efectivo en costo de las personas (Tanenbaum, 1981).

La Conectividad es el concepto impulsor de las Redes de Área Local (LAN) en una forma desconocida para las Redes Globales. Las Redes de Área Local (LAN) son un reconocimiento de la necesidad que tienen las personas de utilizar datos y, como un producto secundario, de transmitir datos de una persona a otra.

Una clave de interés en las Redes de Área Local (LAN), es que aquellos que dirigen grandes organizaciones han reconocido que “organización” implica interacción social.

Los Ordenadores no dirigen Organizaciones, lo hacen las personas. Los Ordenadores no toman decisiones, sino las personas. Los Ordenadores, no importa cuán "Inteligentes" sean; sólo ayudan a las personas a dirigir las Organizaciones.

Como una Organización es principalmente un Proceso Social, operar en forma más eficiente cuando las personas que las constituyen dispongan de herramientas que les ayuden en la 'Toma de Decisiones".

Esto significa que las personas que utilizan Ordenadores en las Organizaciones no lo hacen en forma aislada, sino como seres sociales comprometidos en actividades de comercio y conversación.

En el entorno organizacional, se han introducido muchos recursos de Ordenadores: Ordenadores, Terminales, Copiadoras Inteligentes, y Ordenadores grandes y pequeños. No obstante, un Ordenador vacío, es como una mente también vacía; de poca o ninguna utilidad para nadie, incluyendo a su propietario. Si cada Ordenador debe ser llenado en forma diferente, y a mano, entonces el trabajo se vuelve menos (no más) eficiente.
En el desarrollo de la era de la Informática es importante, que la Tecnología ayude a las personas a reducir la cantidad de información a niveles manejables y a mejorar la calidad de dicha información.

En un contexto Organizacional, las Redes ofrecen el medio para permitir que el poder de Ordenación disponible, sea utilizado a su máximo alcance.

Así mismo, otros aspectos han sido importantes para generar interés en las Redes de Área Local (LAN), incluyendo el deseo de las personas de tener independencia en las operaciones del Ordenador, la necesidad de contar con Ordenadores en todos y cada uno de los Departamentos de una Organización y la economía de las Redes de Área Local (LAN).