4

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES.

CAMPUS ARAGÓN

290080

OPTIMIZACIÓN E INTEGRACIÓN DE SERVICIOS EN UNA RED INFORMÁTICA DE CONCENTRACIÓN A NIVEL NACIONAL.

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO ELECTRICISTA

P R E S E N T A N:

ADRIANA ANZURES LÓPEZ
CRISTINA EUNICE MONTES MONDRAGÓN

ASESOR DE TESIS:
ING. DAVID ESTOPIER BERMUDEZ

MÉXICO, 2001

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
CAMPUS ARAGÓN

SECRETARÍA ACADÉMICA

Ing. IVÁN MUÑOZ SOLÍS
Jefe de la Carrera de Ingeniería Mecánica Eléctrica,
Presente.

En atención a la solicitud de fecha 2 de julio del año en curso, por la que se comunica que las alumnas CRISTINA EUNICE MONTES MONDRAGÓN y ADRIANA ANZURES LÓPEZ, de la carrera de Ingeniero Mecánico Electricista, han concluido su trabajo de investigación intitulado "OPTIMIZACIÓN E INTEGRACIÓN DE SERVICIOS EN UNA RED INFORMÁTICA DE CONCENTRACIÓN A NIVEL NACIONAL", y como el mismo ha sido revisado y aprobado por usted, se autoriza su impresión; así como la iniciación de los trámites correspondientes para la celebración del Examen Profesional.

Sin otro particular, reitero a usted las seguridades de mi atenta consideración.

A t e n t a m e n t e
"POR MI RAZA HABLARÁ EL ESPÍRITU"
San Juan de Aragón, México, 3 de julio del 2001
EL SECRETARIO

Lic. ALBERTO IBARRA ROSAS

C p Asesor de Tesis.
C p Interesado.

AIR/RCC/vr

Agradecimientos

A mis padres Eliezer y Graciela, con su amor y apoyo me llevaron de la mano a descubrir las cosas más bellas de la vida, la motivación que recibí para seguir siempre adelante es un estimulo que me llena de orgullo.

Especialmente a mi hermana; Ely tu tenacidad me ha inspirado a lograr los sueños de nuestra niñez, el compartir mi vida contigo ha sido genial.

A mi asesor David Estopier; su orientación y experiencia hicieron posible este trabajo, especialmente gracias por la paciencia que me has brindado.

A mis maestros, por compartir sus conocimientos y dedicación a la docencia.

A mis amigos, por su inigualable fuente de entusiasmo y amistad.

Cristina

Agradecimientos

A mi Papá Ignacio Anzures:

Este trabajo es el reflejo del agradecimiento a tus enseñanzas, a la educación que me inculcaste, a los valores que me formaste y al amor que me entregaste.

A mi mamá Evelia López de Anzures:

Por darme la vida, y el recuerdo de la humildad, amor y dedicación que siempre tuviste con todos tus hijos...un agradecimiento celestial

A mis hermanos Felix, Lolita, Bebita, Elias, Alfredo, Paty y Lily:

Por compartir conmigo los momentos difíciles y regalarme sonrisas que llenan mi vida de alegría y me llenan de orgullo por pertenecer a esta familia tan unida, los admiro a todos y cada uno de ustedes. Gracias por escucharme y por sus consejos.

A David Estopier, mi asesor:

Aquí está mi oportunidad de agradecerte hoy y siempre el apoyo incondicional y las enseñanzas tan valiosas, gracias también, por tu dedicación, comprensión y confianza en mi y todos tus alumnos.

A Rafael, Estelita, Victor, Carmen, Susy y Miguel:

Por darme la oportunidad de aprender de ustedes, del espíritu de vida y dedicación por salir adelante siempre junto a su familia y por hacerme parte de ella.

A mis sobrinas y sobrinos Alberto, Mario, Diego, Rafael, Miguel, Fernando, Christian, Victor, Daniel y Alfredo.Nadia, Gloria, Erika, Yésica, Angélica, Claudia, Sonia:

Por ser mi inspiración y porque siempre me han regalado una sonrisa y eso es un gran estímulo en mi vida.

A mis amigos tan especiales e incondicionales, Iván, Lucía, Alicia, Marcela, Maribel, Gabriela, Lulú, Mario, Miguel, Mauricio, Laura, Lulú Sotelo, Aída, Fide y Oscar:

Por su amor y sincera amistad, porque en todo momento he contado con ustedes.

Adriana

Agradecimientos

A la ENEP ARAGON:

Por la formación profesional y por la oportunidad de ser alumnas de esta honorable Universidad.

A los sinodales: Por su apoyo en la revisión de esta tesis.

Adriana Anzures L. ***Cristina Montes M.***

INDICE

CAPITULO PRIMERO
AMBIENTE DE RED

CAPITULO SEGUNDO
ARQUITECTURA DE RED

CAPITULO TERCERO
INTERCONECTIVIDAD LAN – WAN

INTERCONECTIVIDAD LAN – WAN

CAPITULO CUARTO
MODELO DE RED

CAPITULO QUINTO
ANALISIS DE LA RED DEL SAT

OBJETIVO

El siguiente trabajo tiene como objetivo, presentar una alternativa con las tecnologías más avanzadas para integrar las redes de voz y de datos, con la finalidad de optimizar su administración e incrementar los beneficios del usuario usando como ejemplo una aplicación real.

JUSTIFICACION

Este trabajo se realiza con el propósito de exponer una herramienta de información que proporcionará una alternativa para la interconectividad y funcionamiento de las redes telemáticas, así como el análisis de una red ya en funcionamiento para mejorar e integrar servicios.

OBJETIVO

El siguiente trabajo tiene como objetivo, presentar una alternativa con las tecnologías más avanzadas para integrar las redes de voz y de datos, con la finalidad de optimizar su administración e incrementar los beneficios del usuario usando como ejemplo una aplicación real.

JUSTIFICACION

Este trabajo se realiza con el propósito de exponer una herramienta de información que proporcionará una alternativa para la interconectividad y funcionamiento de las redes telemáticas, así como el análisis de una red ya en funcionamiento para mejorar e integrar servicios.

INTRODUCCION

En la actualidad, los avances en las telecomunicaciones se presentan de una manera tan rápida que para obtener sus beneficios, debemos actualizarnos a la brevedad posible. La comunicación es una parte esencial en una empresa e inclusive en nuestros hogares, muchas veces depende completamente de ésta el crecimiento y ganancias que nuestros negocios pudieran obtener. De aquí parte la idea de un estudio enfocado a mostrar una de las diferentes opciones que tenemos hoy en día para hacer de las comunicaciones una herramienta flexible, administrable y a los costos más redituables.

La mayoría de las organizaciones establecen sus comunicaciones de voz y datos utilizando redes separadas, sin embargo, ambos servicios se están relacionando cada vez más e integrando en una sola red, con lo que podremos obtener notables mejoras y ahorros económicos en las redes de comunicaciones de las empresas.

Una alternativa que se pretende mostrar en este trabajo de tesis es integrar los servicios de voz utilizando la tecnología Frame Relay explicando sus componentes, ventajas, desventajas, costos, beneficios y aplicaciones.

De cualquier manera, transmitir voz sobre redes Frame Relay y a la vez mantener la calidad y confiabilidad que ofrecen las redes telefónicas tradicionales involucra significativos retos tecnológicos. Por lo tanto, las soluciones de voz sobre Frame Relay deberán ser implementadas en forma transparente sobre los sistemas ya existentes y con posibilidades de crecimiento que permitan adicionar nuevas aplicaciones a futuro.

CAPITULO PRIMERO
AMBIENTE DE RED

1.1 Generalidades

Cada vez con más frecuencia es enorme la cantidad de información a la que estamos expuestos cada uno de nosotros; la productividad y el rendimiento de las organizaciones se basan en el uso de sistemas de comunicación, es decir, una organización es más eficiente, si permite compartir recursos e información por medio de computadoras que pueden comunicarse entre sí de manera flexible; mediante una red de área local (LAN).

Las LAN son en particular importantes porqué es una LAN la que será conectada a muchas estaciones de trabajo como la primera fase de un entorno distribuido de redes y operaciones de computación de mayor magnitud. Así mismo, las LAN son importantes para muchas organizaciones de menor tamaño porque son la ruta a seguir hacia un entorno de computación multiusuarios distribuido capaz de comenzar en forma modesta, pero también de extenderse a medida que aumenten las necesidades de la organización.

Como lo hemos podido apreciar, una de las influencias más profundas en el desarrollo de las LAN ha sido la adopción de estándares nacionales e internacionales (estándares que incluso los gigantes de la industria encuentran difíciles de pasar por alto).

Quizá el desarrollo más penetrante e importante de las redes en la década de 1980 fue el reconocimiento que los dispositivos controlados por computadora son ahora los periféricos de la red, y ya no que la red es un periférico de una computadora. Es importante señalar que se utiliza el término "dispositivos controlados por computadora" ya que ahora debemos de pensar en la conexión de herramientas inteligentes en una planta de manufactura, dispositivos de generación de imágenes incluyendo fax-módem, y otros dispositivos para LAN.

Es cierto que, el término "redes de computadoras", está ya pasado de moda y que incluso, el término "red de comunicación de datos", puede ser demasiado restrictivo en una era en la que deben de reconocerse, no sólo los datos en caracteres, sino también gráficos, imágenes de todos tipos y fragmentos de voz y vídeo como información que deben de manejar las redes. El procesamiento de la información requiere de redes de transmisión de información que ofrezcan servicios superiores a los que caracterizan a las transmisiones de voz y datos tradicionales.

Una definición más completa y actual de una red local sería: Un sistema de comunicaciones capaz de facilitar el intercambio de datos telemáticos, voz, fax, vídeo conferencia, difusión de vídeo, telemetría y cualquier otra forma de comunicación electrónica. Un concepto más restrictivo sería: Un sistema diseñado para compartir datos entre puestos de trabajo.

1.2 Estructura de una red de comunicaciones.

En toda red existe una colección de computadoras destinadas para correr programas de usuario, es decir, aplicaciones tales como programas de contabilidad, de nómina, de inventarios, etc. Dos términos a menudo encontrados en la comunicación son: Equipo de Terminación de Circuitos (DCE Data Circuit Terminating Equipment) y Equipo Terminal de Datos (DTE Data Terminal Equipment). Las terminales y las computadoras son clasificadas como DTE, mientras los módem son ejemplos de DCE.

Un ejemplo de una red de comunicaciones se muestra en la siguiente figura donde:

El sistema involucra una comunicación física y lógica entre computadoras y terminales conectados, las aplicaciones utilizan el canal físico para realizar comunicaciones lógicas, los equipos no necesitan saber nada del proceso de la comunicación en cuanto al aspecto físico y el sistema de comunicación se encarga de enviar la orden a través del canal físico; de tal forma que el ETD designa a la máquina del usuario final (computadora) y se conecta de tal manera que pueda compartir recursos, intercambiar datos y permitir a los usuarios hacer diversas operaciones desde cualquier punto que se encuentren dentro de la red; y el ETCD denominado equipo de comunicación de datos cuya función es conectar los ETD al canal o línea de comunicación, por lo que podemos decir que su función básica es servir de interfaz entre el ETD y la red de comunicaciones, las interfaces se establecen y especifican mediante protocolos.

Por lo tanto, al diseñar una red hay que considerar ciertos aspectos para establecer la topología de la misma:

Proporcionar la máxima fiabilidad a la hora de establecer el tráfico.

Encaminar el tráfico utilizando la vía de coste mínimo entre los ETD transmisor y receptor.

Proporcionar al usuario el rendimiento óptimo y el tiempo de respuesta mínimo.

Al hablar de redes, el concepto de fiabilidad hace referencia a la capacidad de enviar los datos correctamente, (es decir, sin errores) entre los ETD. Involucra la posibilidad de recuperación de errores o de datos perdidos en la red por motivos de fallos en el canal, los ETD, los ETCD y los ECD. La fiabilidad también tienen ver con el mantenimiento del sistema: pruebas diarias, sustitución de componentes defectuosos o en fallo manifiesto, y aislamiento de fallos en caso de aparecer problemas. Si algún componente es causa de problemas, el sistema de diagnóstico de la red debería de buscar rápidamente el fallo, encontrarlo y, si es posible, aislar el componente de la red.

El segundo objetivo es proporcionar el camino de costo mínimo entre los procesos de aplicación que residen en los ETD. Para ello es necesario lo siguiente:

Minimizar la longitud real del canal entre los componentes que se comunican. Para lo cual se debe encaminar el tráfico pasando por el menor número posible de componentes intermedios.

Proporcionar el canal más barato para una aplicación determinada.

El último objetivo es proporcionar el mínimo tiempo de respuesta y el máximo rendimiento, de tal forma que hay que procurar minimizar el retardo entre la transmisión y la recepción de datos entre ETD (importante para sesiones interactivas entre aplicaciones de usuario). El rendimiento tiene que ver con la transmisión de la máxima cantidad de datos en un periodo determinado.

1.2.1 Clases de redes

Podemos clasificar las redes de acuerdo con la tecnología de transmisión y su tamaño.
Tecnología de transmisión es la que se refiere a la utilización de canales para enviar la información y pueden ser:

Broadcast. Un solo canal de comunicación compartido por todas las máquinas. Un *paquete* mandado por alguna máquina es recibido por todas las otras.

Point-to-point. Muchas conexiones entre pares individuales de máquinas. Los paquetes de A a B pueden atravesar máquinas intermedias, para lo cual se necesita el ruteo (*routing*) para dirigirlos.

Si consideramos el tamaño la distancia que cubre la red es lo más importante por lo cual las redes se dividen en:

- ✓ LAN (local Area Network): 10 m a 1 km
- ✓ MAN (Metropolitan Area Network): 10 km
- ✓ WAN (Wide Area Network): 100 km a 1.000 km
- ✓ Internet: 10.000 km.
- ✓ Redes inalámbricas

Las características principales de estas redes considerando los conceptos anteriores son:

LANs
Normalmente usan la tecnología de broadcast: un solo cable con todas las máquinas conectadas. El tamaño es restringido, las velocidades típicas son de 10 a 100 Mbps (Megabits por segundo; un megabit es 1.000.000 bits, no 2^{20}).

WANs
Consisten en una colección de *hosts* (máquinas) o LANs de hosts conectados por una *subred* donde se manda la información o paquetes de un ruteador a otro. Se dice que la red es *packet-switched* (paquetes ruteados) o *store-and-forward* (guardar y reenviar).

Internet
Una *Internet* es una red de redes vinculadas por *gateways,* que son computadoras que pueden traducir los datos entre formatos incompatibles.

Redes inalámbricas
Una red inalámbrica usa radio, microondas, satélites, infrarrojo, u otros mecanismos para comunicarse. Se pueden combinar las redes inalámbricas con las computadoras móviles, pero los dos conceptos son distintos:

Inalámbrico	Móvil	Aplicación
No	No	Workstations estacionarias
No	Sí	Uso de un portable en un hotel
Sí	No	LANs en un edificio antiguo sin cables
Sí	Sí	PDA (Personal Digital Asistant) para inventario

1.2.2 Consideraciones en el diseño de una red

Transferencia de datos:

- ✓ Simplex. Solamente en un sentido.
- ✓ Half-duplex. En ambos, pero uno a la vez.
- ✓ Full-duplex. En ambos a la vez.

Control de errores y detección de recepción.
Orden de mensajes.
Velocidades distintas de transmisión y recepción.
Ruteo.
Servicios
Los servicios se caracterizan por la calidad que prestan. Cada servicio define un conjunto de primitivas (tales como "solicitar" o "acusar recibo"). Por contraste el protocolo es el conjunto de

reglas que controlan el formato y significado de los paquetes intercambiados por entidades de par. Se usan los protocolos para implementar los servicios.
Servicio orientado a la conexión. Como el sistema telefónico. La conexión es como un tubo, y los mensajes llegan en el orden en que fueron mandados.
Servicio sin conexión. Como el sistema de correo. Cada mensaje trae la dirección completa del destino, y el ruteo de cada uno es independiente.
Compara la transferencia de archivos con la comunicación de voz (ambas orientadas a la conexión). Para e-mail un servicio sin conexión y no confiable es suficiente, esto se llama *servicio de datagrama*. Para dar confianza, es posible modificar los servicios de datagrama agregándoles acuses de recibo.

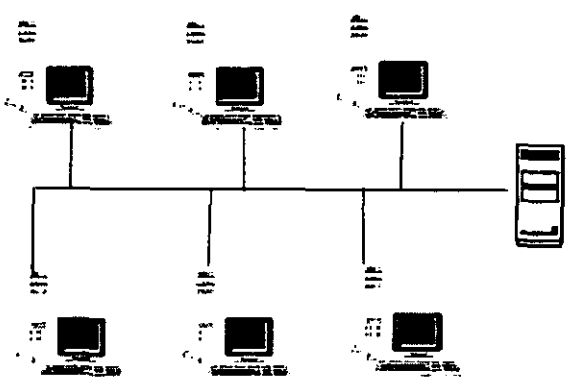
1.3 Redes de Area Local

Existe no obstante una definición oficial, la del Comité IEEE 802, quién define una red local de la siguiente manera: Una Red local es un sistema de comunicaciones que permite que un número de dispositivos independientes se comuniquen entre sí.

Una red local, como su nombre lo indica, debe ser local en cuanto al ámbito geográfico, aunque local puede significar cualquier cosa, desde una simple oficina o un edificio de ocho pisos, hasta un complejo industrial con docenas de edificios de muchos pisos.

El principal atributo de una red local es la conectividad - la capacidad de que un determinado nodo de la red pueda comunicarse con cualquier otro punto alejado de la misma. Otro atributo importante es la capacidad para integrar comunicaciones electrónicas multimedia (datos, vídeo, voz, etc.).

Las redes locales están diseñadas para facilitar la interconexión de una gran variedad de equipo de tratamiento de información dentro de un centro. El término red local incluye tanto el hardware como el software necesario para la conexión, gestión y mantenimiento de los dispositivos y para el tratamiento de la información. Una Red Local (LAN) es un canal de intercomunicación que enlazan dos o más ordenadores, terminales o cualquier otro dispositivo periférico que se encuentren dentro del espacio físico de un mismo centro. figura1.1



Red de área local

figura 1.1 Una LAN básica

Las redes locales se caracterizan por lo siguiente:

- ✓ Un medio de comunicación común a través del cual todos los dispositivos pueden compartir información, programas y equipo, independientemente del lugar físico donde se encuentre el usuario o el dispositivo. En la mayoría de los casos, las redes locales están contenidas dentro de una reducida área física, que puede ser un edificio de oficinas, o una oficina concreta de ese edificio, una empresa, una universidad, etc.

- ✓ Una velocidad de transmisión muy elevada para que pueda adaptarse a las necesidades de los usuarios y del equipo. Normalmente, el equipo de la red local puede transmitir datos a la velocidad máxima a la que pueden comunicarse las "estaciones" de la red (suele ser varios millones de bits por segundo).

- ✓ Una distancia entre "estaciones" relativamente corta, entre unos metros y varios kilómetros (2000 ó 3000 m), aunque la distancia suele ser mucho mayor utilizando dispositivos de transmisión especiales.

- ✓ La posibilidad de cables de transmisión normales.

- ✓ Todos los dispositivos pueden comunicarse con el resto, y algunos de ellos pueden funcionar independientemente.

- ✓ Un sistema confiable, con un índice de errores muy bajo. Las redes locales disponen normalmente de su propio sistema de detección y corrección de errores de transmisión.

- ✓ Flexibilidad, el usuario administra y controla su propio sistema.

Las redes locales se distinguen de los otros tipos de redes (p.e. la red telefónica) en lo siguiente:

- ✓ La zona que cubren (normalmente no suele superar los 3000 metros).

- ✓ La velocidad de transmisión de la información (entre 1 y 5 millones de bits por segundo (MB)).

- ✓ La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica). En los últimos años han tomado gran auge los medios de transmisión inalámbricos.

- ✓ La facilidad con que se pueden efectuar cambios en el hardware y software.

- ✓ La topología (siendo las más populares la de bus, anillo y en estrella) y la facilidad de uso.

1.3.1 Componentes básicos de una LAN

Basándonos en un modelo sencillo de comunicación de datos podemos definir los siguientes componentes como básicos, figura 1.2

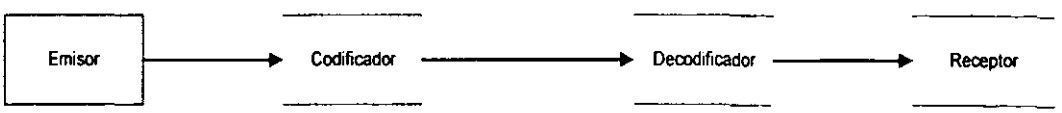


figura 1.2 Componentes básicos de una red

El emisor, en cual se genera, y del que parte la información.

El codificador, el cual convierte los datos que se envían en un mensaje, es decir, transforma la información para que se pueda enviar.

El medio de transmisión, el cual proporciona la vía a través de la cual se va a enviar el mensaje.

El decodificador, el cual convierte los datos recibidos dejándolos de forma que el receptor pueda entenderlos.

El receptor, que es el destinatario de la información enviada, y que en definitiva es quien la va a utilizar.

Como ya mencionamos anteriormente una red de área local (LAN) es un mecanismo de transmisión de datos que está conectado a un medio de comunicación continuo, compuesto por una serie de dispositivos conectados entre sí que desempeñan tareas en forma independiente. Estas redes, están limitadas geográficamente por un perímetro aproximado de 10 kilómetros y son capaces de enviar un gran volumen de información a grandes velocidades.

En una red de ordenadores, estos son al mismo tiempo emisores y receptores de datos. El ordenador sirve también para traducir la información que se encuentra en un formato que es entendible para el usuario y que se pueda transmitir.

1.3.2 Hardware y Software:

Los componentes físicos básicos de una red de área local son:

Interfaces: Conectan los dispositivos a la red y hacen posible la comunicación con otros dispositivos. La interfaz puede ser una tarjeta de red, un módem, o un puerto de comunicaciones de un microordenador.

Topología: La forma física de interconexión entre los dispositivos de la red. Es la forma de poner orden a la conexión indiscriminada de dispositivos.

Medios de transmisión: Proporciona el enlace físico que lleva la información de un punto a otro de la red. A este enlace se le denomina también "canal", "línea", o "circuito".

Protocolo. Son las reglas y convenciones que controlan el intercambio de información.

Los componentes antes mencionados cubren las necesidades funcionales mínimas de una red de ordenadores; pero, además, se necesita el software que controla el sistema:

Un sistema operativo de red.

Aplicaciones que necesita el usuario para realizar su trabajo.

Los programas de las utilidades de la red con los que se llevan a cabo todos los procedimientos rutinarios como copias, backups, etc.

Los componentes más importantes de una red son los nodos o estaciones de trabajo. Nodo es un término que se emplea en el ámbito de los grandes ordenadores y que se refiere al principio, al final, o a la intersección de un enlace de comunicaciones, no a un dispositivo específico. Figura 1.3

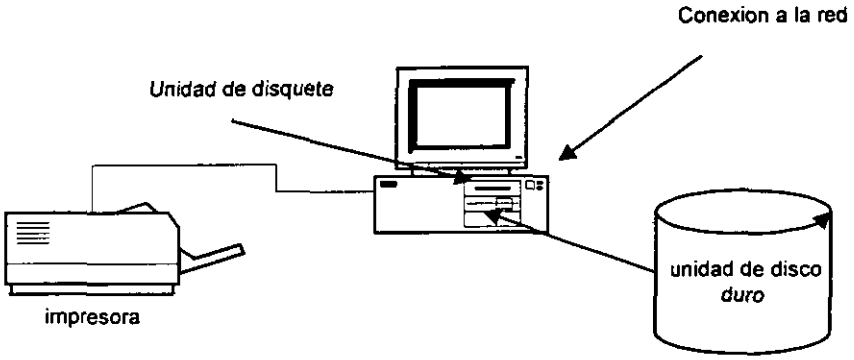


Figura 1.3 Nodo o estación de trabajo

Una estación de trabajo describe cualquier computadora, terminal y todos los periféricos conectados a éstos, o independientes (una impresora, un módem, un escáner, etc.) con una tarjeta de red instalada mediante la cual se puede acceder al servidor a través de los cables (o a través de ondas de radio, como es el caso de las redes inalámbricas).

Para poder comunicarse con el servidor de la red, las estaciones de trabajo deben ejecutar un programa especial de comunicaciones.

Las estaciones de trabajo suelen ser computadoras conectados a la red que por lo general, mantienen su capacidad de trabajar de forma autónoma utilizando su propio software, pero normalmente están conectadas al servidor de la red de modo que pueden acceder a la información contenida en éste. Para poder hacer esto, la estación de trabajo necesita una interfaz especial que se conecta a una de las ranuras de expansión de al estación, y que se conecta un cable que lo enlaza con el servidor.

Interfaces

Los servidores de comunicaciones están diseñados para liberar a la red de las tareas relativas a la transmisión de información. El servidor de comunicaciones funciona igual que una central telefónica, haciendo las mismas funciones que un sistema PABX (central automática privada).

Por medio del servidor de comunicaciones una estación, puede llamar a una red externa o cualquier otro sistema, buscar cierta información y enviarla a la estación que la ha solicitado. El servidor de comunicaciones se puede utilizar también para conectar dispositivos incompatibles a una red.

A pesar de que un servidor de comunicaciones efectúa las funciones de un módem, en particular proporcionando acceso a redes telefónicas de larga distancia, hay bastante diferencia entre ellos. La mayoría de los módem están conectados a una sola estación y sólo se pueden utilizar en esa estación. Los servidores de comunicaciones están conectados a la red y por lo tanto se pueden utilizar todas las estaciones. Los servidores de comunicaciones pueden responder a varias solicitudes a la vez. Además, el servidor de comunicaciones ofrece más funciones, tales como la multiplexión y conmutación, detección de errores, y además es mucho más flexible.

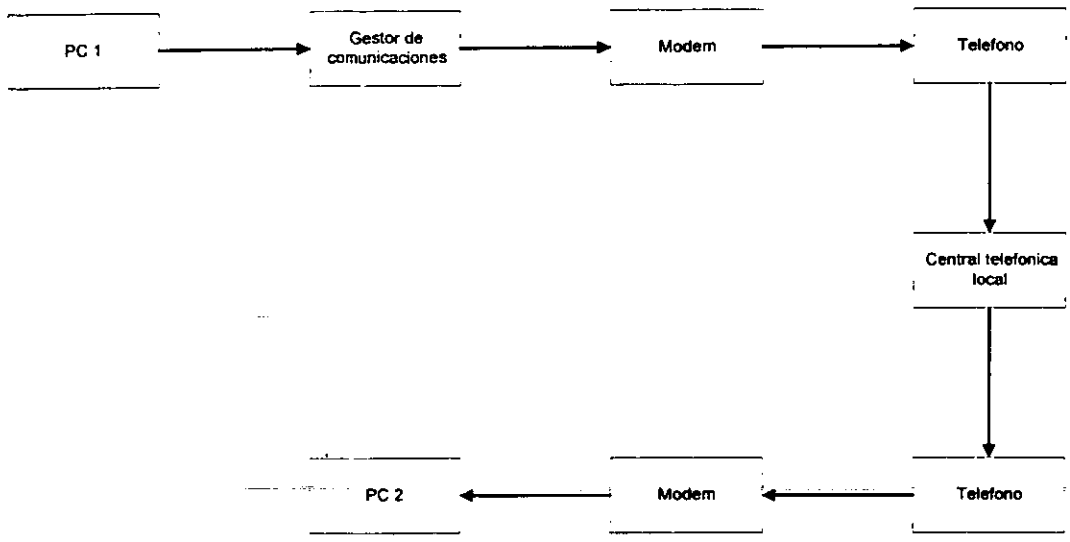


Figura 1.4 Servidor de Comunicaciones

Servidores (clasificación)

Un servidor de red local sirve para acceder a datos y programas que se encuentren en cualquier parte de la red, "charlar con los compañeros de trabajo, compartir impresoras o discos duros, etc. Hemos visto que una red local interconecta ordenadores, y comparte dispositivos, pero para compartir eficientemente periféricos tales como discos duros o impresoras, es necesario configurar uno o más ordenadores como "gestores", es decir, un servidor (server) que es un ordenador que comparte sus periféricos con otros ordenadores. Un servidor de discos permite compartir zonas del disco. Un servidor de impresora es un servidor que pueden utilizar todos los usuarios, y que se encarga de volcar el contenido de ficheros en una impresora.

Servidores de disco

Al principio las redes utilizaban un servidor de disco donde se almacenaba la información que iban a compartir las distintas estaciones de la red. Para estas el servidor es simplemente otra unidad de disco duro donde se almacenan ficheros. En el caso de un PC funcionando bajo DOS la unidad asignada del servidor de ficheros es como un disco normal del que se mantiene una tabla de asignación de ficheros (FAT o file allocation table) propia para poder saber exactamente donde se encuentra un determinado fichero.

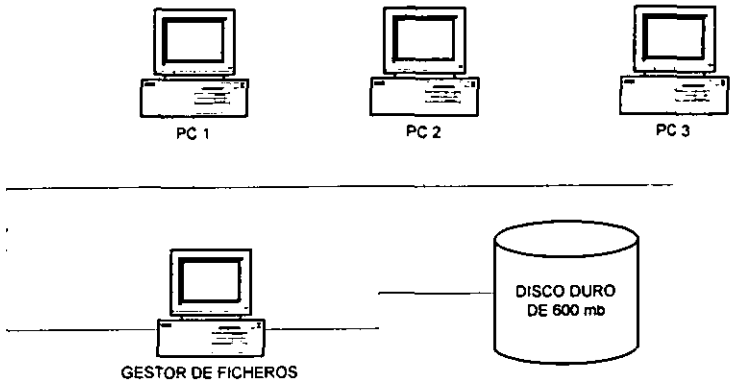


FIGURA 1.5 Servidor de disco de una red

Lo de propia significa que el servidor de ficheros contiene varias particiones, cada una de ellas asignada a un usuario. Esto se hace para cuando el PC necesite leer un fichero, lea la FAT de la partición que le ha sido asignada y busque en ella el fichero que necesita. Una vez modificado lo graba en el disco grabando la FAT en la partición asignada. De no ser así, podría darse el caso de que varios usuarios accediesen a grabar la FAT, que en cada caso sería distinta, produciéndose un complicado galimatías indescifrable y se perderían todos los datos.

Algunas particiones pueden definirse como públicas, pero normalmente suelen definirse como de sólo lectura de modo que no puedan modificarse. Todas las estaciones pueden acceder a esta información pero no pueden cambiarla. Hay dos tipos de servidores de disco: dedicados y no dedicados. Normalmente los servidores dedicados no disponen de monitor ni teclado; para lo único que sirven es para dar servicio a las solicitudes de otros ordenadores de la red. Los servidores no dedicados son ordenadores normales que tienen conectado un disco duro o impresora, y que al igual que los dedicados dan servicio a la red, con la diferencia de que se pueden utilizar como un ordenador normal mientras actúa de servidor.

Servidores de ficheros (file server)

Un servidor de ficheros es mucho más eficiente que un gestor de disco. Contiene software especial que procesa comandos antes de que el sistema operativo los reciba. El servidor de ficheros contiene su propia FAT. Cuando una estación de trabajo pide un determinado fichero, el servidor de ficheros ya sabe donde está el fichero y lo envía directamente a la memoria de la estación de trabajo. Los servidores de ficheros pueden ser de cuatro tipos: Centralizados, distribuidos, dedicados y no dedicados.

Servidores de ficheros centralizados y distribuidos

Para la mayoría de las redes un único servidor de ficheros es más que suficiente y se conoce como servidor central, una unidad se encarga de dar servicio a cada estación de trabajo. En el caso de tener diversas áreas (en el caso de una empresa) y con la necesidad de cada una de estás tener su propio servidor entonces tenemos varios servidores es decir, un servidor distribuido; los cuales reducen tiempos de acceso y además si uno de ellos falla, la red puede seguir funcionando.

Servidores de ficheros dedicados y no dedicados

Un servidor de ficheros dedicado es un ordenador con disco duro que se utiliza exclusivamente como servidor de ficheros. Dedicando toda su capacidad de memoria, procesamiento, y recursos a dar servicio a las estaciones de trabajo por lo que se consigue un aumento de velocidad y eficiencia de la red.

Un servidor no dedicado es aquél que se usa, además de para funciones de servicio de ficheros, como estación de trabajo. Esto implica que la RAM debe estar dividida de forma que puedan ejecutarse programas en la máquina. Cuanto más rápido sea el procesador, más rápido puede el servidor realizar sus tareas, lo que a su vez, implica un costo más elevado.

Servidores de ficheros de una red punto a punto

En una red punto a punto los usuarios toman la decisión de que recursos de su ordenador desean compartir con el resto de los usuarios de la red.

Un usuario puede utilizar su unidad de disco duro como servidor de ficheros para otros usuarios de la red. Una red de este tipo puede constar de varias estaciones que realizan funciones de servidor de fichero no dedicado cuyos propietarios han decidido compartir con el resto de los usuarios de la red. Esta filosofía es aplicable así mismo a las impresoras y otros dispositivos.

Servidor de impresión

Al igual que un servidor de ficheros permite compartir un disco duro, un servidor de impresión hace lo mismo, sólo que en esta ocasión lo que se comparte son impresoras. Para poder compartir impresoras, el servidor de impresión debe disponer del software adecuado y por lo general contiene lo que se conoce con el nombre de spooler de impresión, que es un buffer donde se almacenan los trabajos que cada estación manda a imprimir; los trabajos se van poniendo en cola y se imprimen de forma secuencial en orden de llegada.

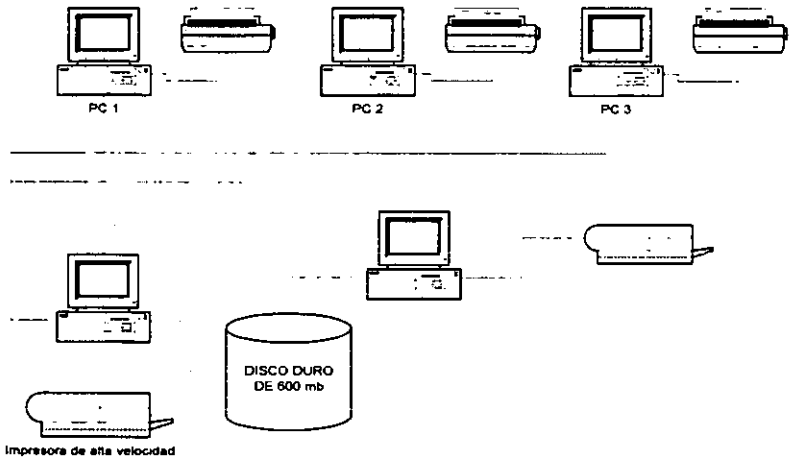


Figura 1.6 Servidor de Impresión

Tarjeta de interfaz de red

(NIC) Es una tarjeta de circuitos que se instala en cada estación de modo que ésta pueda comunicarse con las demás y con el servidor central.

Unidades de almacenamiento

Los administradores de red deben supervisar la integridad de los datos de la red, si falla una unidad requieren estar seguros de que no se pierdan los datos. Una solución cada vez más popular es la agrupación redundante de discos o RAID (Redundant arrays of inexpensive disks). Un sistema

RAID consiste en diversas unidades de disco que funcionan en paralelo, entre los que se distribuyen los datos, de modo que si se produce fallo, pueden recuperarse éstos.

Unidades de almacenamiento de seguridad

Puesto que las redes almacenan por lo general un volumen considerable de datos importante, se hace necesario disponer en cada red de un sistema de almacenamiento de seguridad. Tales como los dispositivos de cinta *dat*.

Microprocesadores

Son los que proporcionan a la red toda la potencia del proceso y los que crean los mensajes. Los microprocesadores son la interfaz entre el usuario y la red en sí, los cuales sirven como dispositivos de comunicación, es decir, son los dispositivos que hacen posible el intercambio de datos entre seres humanos y máquinas.

Cliente

Es la combinación de software y hardware que invoca los servicios de uno o varios servidores, e incluso de otro cliente. El método más común por el cual el cliente solicita los servicios a un servidor es por medio de RPC(Remote Procedure Call, llamada a un procedimiento remoto). Un RPC es un procedimiento que se ejecuta en otra máquina diferente a la que se hizo la invocación del procedimiento; el cliente no ejecuta el procedimiento, sólo lo invoca en el servidor.

1.4 Topología de Red

La topología tiene una gran importancia en el diseño de una red local, puesto que afecta el rendimiento de la misma.

Se denomina topología a la forma geométrica de colocar las estaciones y los cables que las conectan. La topología fue pensada para poner orden al potencial caos que se puede producir al colocar las estaciones de forma indiscriminada. Hay tres formas posibles de conexión:

Punto a punto, en la que sólo se unen dos estaciones adyacentes, sin pasar a través de una estación intermedia.

Multipunto, en la que dos o más estaciones comparten un solo cable.

Lógica, en la cual las estaciones se pueden comunicar entre sí, haya o no-conexión física directa entre ellas.

Las estaciones de una red local se comunican entre sí basándose en una de las conexiones físicas. El objeto de la topología es encontrar la forma más económica y eficaz de conectar a los usuarios a todos los recursos de la red, al mismo tiempo que facilita la capacidad adecuada para satisfacer las demandas de los usuarios, mantiene la fiabilidad del sistema, y mantiene el tiempo de espera en cotas relativamente bajas. El número de parámetros y variables que se pueden emplear para encontrar la solución es muy grande.

El control de la red también afecta la topología, está tan relacionado que a veces se define la topología como el medio de implementar el protocolo de control.

El control puede estar centralizado, en cuyo caso el acceso a la red y la asignación de canal lo determina un nodo. La inteligencia también puede estar concentrada en el nodo "central",

quedando las estaciones como terminales no inteligentes. O puede estar distribuido, en cuyo caso las estaciones pueden acceder independientemente a los canales de la red, dependiendo esto siempre de un conjunto compartido de protocolos. En este caso la "inteligencia" de la red esta distribuida por todas las estaciones conectadas.

1.4.1 Topología Jerárquica

La topología jerárquica o red en árbol proporciona un punto de concentración para control y resolución de errores; el ETD (A) de mayor jerarquía (raíz) es el que controla la red, el flujo de datos entre los DTE lo inicia el ETD . Aunque, el añadir estaciones de trabajo y la forma de control de esta topología es de un modo sencillo, presenta serios problemas de cuellos de botella y fiabilidad debido a que, el ETD (A) es el que controla todo el tráfico entre los ETD y sí el ETD (A) tiene un fallo la red queda completamente fuera de servicio, a no ser que el diseño permita que otro nodo asuma las funciones del nodo averiado.

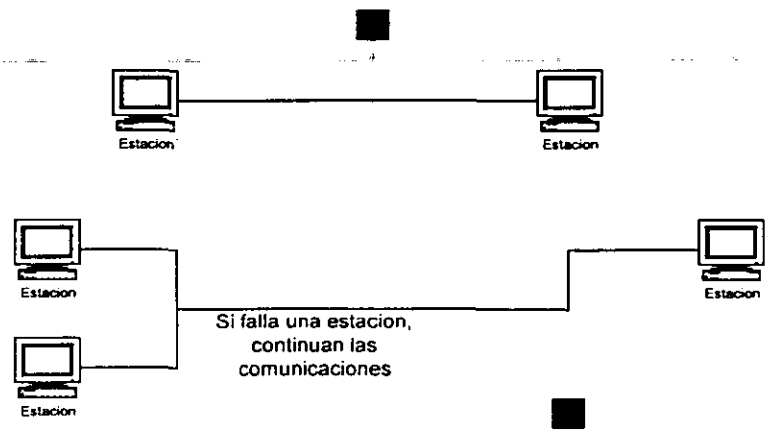


Figura 1.7 Topología en Arbol

1.4.2 Topología en bus

La topología horizontal o en bus es un a de las más utilizada en redes de área local (LAN). El control de tráfico entre los ETD es simple ya que el bus permite que todas las estaciones reciban la transmisión, así cada estación puede difundir la información a todas las demás; uno de los inconvenientes que presenta el más notorio es que sólo existe un único canal de comunicaciones al que se conectan todos los dispositivos de la red y si dicho canal falla, la red deja de funcionar.

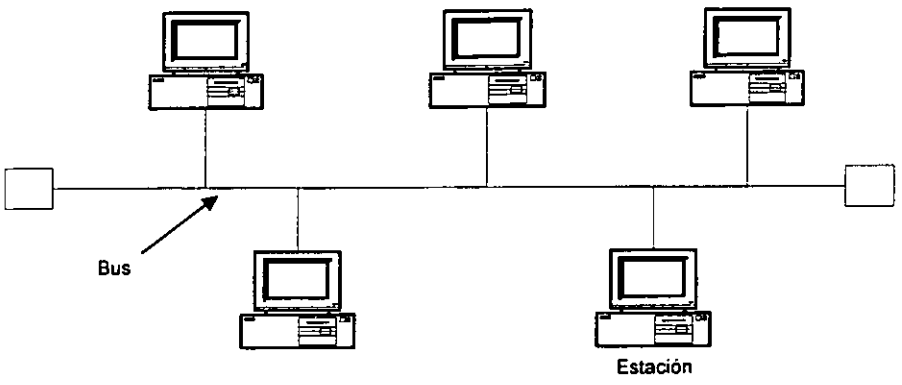


Figura 1.8 Topología en bus

1.4.3 Topología en estrella

Este tipo de topología tiene un software y flujo de tráfico simple, similar a la topología en árbol, tiene un punto que controla todos los ETD y todo el tráfico surge del centro de la estrella (nodo A) hacia los ETD conectados a dicho punto; la diferencia con la topología de árbol es que la estructura en estrella tiene mucho más limitadas las posibilidades de procesamiento distribuido. Esta red sufre los mismos problemas de cuellos de botella y problemas de fallos, debido al nodo central así como problemas de fiabilidad por la centralización distribuida.

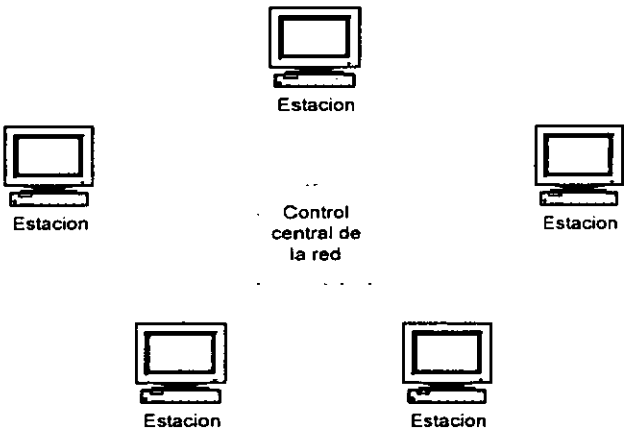


Figura 1.9 Topología Estrella

1.4.4 Topología en anillo

Este tipo de topología forma un círculo de conexiones punto apunto y el flujo de datos va de una estación a otra hasta llegar a la estación adecuada, es decir , las tareas que debe realizar cada componente son aceptar los datos, evitarlos al ETD conectados con él, o bien enviarlos al siguiente componente intermedio en el anillo. Cuando se utiliza una topología en anillo para

distribuir el control en redes locales, el protocolo utilizado ha de evitar situaciones conflictivas a la hora de acceder a un canal compartido. La lógica utilizada es relativamente simple y es raro que presente cuellos de botella, sin embargo, presenta el inconveniente de que un único canal une a todos los componentes del anillo; y si el canal falla entre dos nodos, falla toda la red.

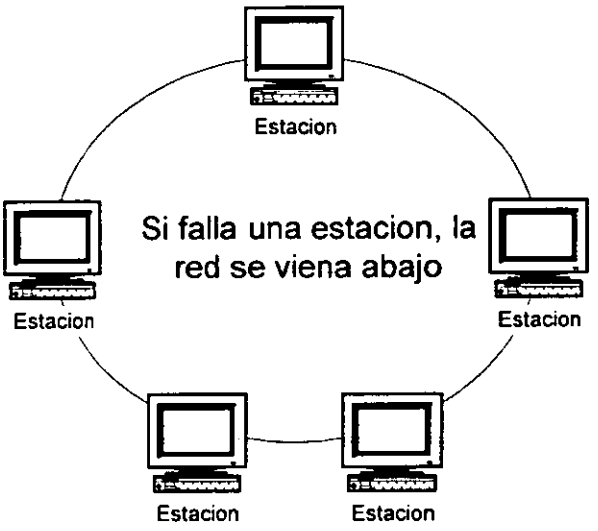


Figura 1.10 Topología en anillo

1.4.5 Topología en malla

Este tipo de topología tiene la posibilidad de encaminar el tráfico por diferentes opciones entre los ETD y ECD evitando componentes que fallen y nodos costos lo cual le da ventaja sobre los anteriores tipos de topología en problemas de fallo y cuellos de botella ya que casi no se presentan; y su diferencia esta en el costo de la red, pero se compensa con la gran fiabilidad que tiene frente a las otras formas de topología.

1.4.6 Factores básicos de evaluación

De acuerdo a las necesidades del usuario, la topología más adecuada será elegida de acuerdo a los factores siguientes:

Aplicación: El tipo de instalación en el que es más apropiada la topología.

Complejidad: Afecta al instalación y mantenimiento de todo el cableado.

Respuesta. El tráfico que puede soportar el sistema.

Vulnerabilidad: lo susceptible que es la topología a fallos o averías.

Expansión: La posibilidad de ampliar la red cuando sea necesario hacerlo, así como la facilidad que hay para añadir los dispositivos necesarios para cubrir distancias más grandes. La tendencia es hacia la señalización digital y sus ventajas:

- ✓ La regeneración de la señal es fácil sobre distancias largas.
- ✓ Se pueden entremezclar la voz y los datos.
- ✓ Los amplificadores son más baratos porque solamente tienen que distinguir entre dos niveles.
- ✓ El mantenimiento es más fácil; es fácil detectar errores.

Un ejemplo sería la red telefónica, que se utiliza para redes más grandes que una LAN.

1.5 Medios de comunicación

Sirven para conectar los dispositivos en una red de área local, proporcionando los medios para que las señales de datos se transporten en los diferentes dispositivos conectados a la red. La capacidad de la transmisión de datos está medido en base a la cantidad de datos que pueden enviar a través del medio y que tan rápido o lejos éstos pueden ser enviados sin interferencias o pérdidas. Los factores que afectan la transmisión son: la interferencia eléctrica y atenuación.

Interferencia eléctrica. El ruido electrónico de las líneas telefónicas, cables de poder y luces fluorescentes pueden causar interferencia en los datos que son transmitidos sobre los cables de la red.

Atenuación. Las señales se van debilitando conforme son transmitidas a lo largo del cable debido a las largas distancias y ruido, provocando que éstas sean mucho más susceptibles a interferencia eléctrica, incrementando la posibilidad de errores.

1.5.1 Medios de Transmisión de Datos utilizados en las Redes.

Cualquier medio físico o no (comunicaciones inalámbricas) que pueda transportar información en forma de señales electromagnéticas se puede utilizar en redes de cómputo como medios de transmisión. Un concepto importante que debemos mencionar es el de ancho de banda el cual significa la capacidad de transmisión de un canal de una computadora, línea o ducto de comunicaciones. El ancho de banda se expresa el ciclos por segundo(Hz). Este representa la diferencia entre las frecuencias transmitidas máxima y mínima. Así un canal se define como un rango de frecuencias disponibles en el ancho de banda por el cual se transmite la información.

Las líneas de transmisión son la espina dorsal (backbone) de la red, por ella se transmite la información entre los distintos nodos. Para efectuar la transmisión de la información se utilizan varias técnicas, pero las más comunes son: la banda base(baseband) y la banda ancha(broadband).

En la transmisión de datos por banda base no es necesario el uso de módem porque la señal se puede transmitir a alta velocidad. Banda base significa que la señal no está modulada y por lo tanto esta técnica no es muy adecuada para transmisiones a larga distancia ni para instalaciones sometidas a un alto nivel de ruidos e interferencias.

La transmisión de datos por banda ancha consiste básicamente en modular la información sobre ondas portadoras analógicas. Cuando se utiliza el sistema de banda ancha para transmitir datos, se requiere de la utilización de modems para modular la información. Los modems utilizados en las redes de banda ancha son dispositivos muy complejos, ya que realizan funciones de modulación/demodulación y de transmisor/receptor.

Existen dos conceptos que se basan en la información anterior y se denominan Técnicas de señalización y métodos de acceso. Las primeras sirven para establecer intercambio de información entre equipos; de tal forma que existen técnicas de transmisión de datos digital en una sola

frecuencia o transmisión de datos análogos en diferentes frecuencias y métodos de acceso que son procedimientos para enviar mensajes a otros nodos de la red a través del ancho de banda. Estos métodos pueden ser clasificados como centralizados o distribuidos.

Algunos ejemplos de estos modelos son:

Red Optica Síncrona (Sonet. Synchronous Optical Network ANSI). Conjunto de estándares para la utilización de redes de transmisión en medios de fibra óptica de alta velocidad.

Red Digital de Servicios Integrados (ISND. Integrated Services Digital Network CCITT). Conjunto de estándares para la utilización de redes de transmisión digital sobre medios de cableado convencional o fibra óptica. Permiten el manejo de canales de voz, vídeo, datos y telefonía.

Arquitectura de Redes de Sistemas (SNA. System Network Architecture IBM). Conjunto de especificaciones establecida para la interconexión de equipos en ambientes IBM. Integra especificaciones completas desde comunicación de medios físicos hasta de aplicaciones.

Existe una gran variedad de medios de transmisión de datos y se clasifican como medio limitado y medio ilimitado.

Medio ilimitado

Transmite los datos llevando la señal a través del espacio, independiente de un cable, por ejemplo:

Microondas. Son ondas electromagnéticas que caen entre ondas de radio y luz.; tienen frecuencias que se extienden dentro del rango de los Gigahertz (100 MHz – 10 GHz). Antes de la fibra formaban el centro del sistema telefónico de larga distancia.
Las microondas se transmiten por LINE-OF-SIGHT (línea visual) y no pueden transmitirse alrededor de la curvatura de la tierra. Estas pueden ser atenuadas o interferidas por fenómenos de la atmósfera tales como la lluvia o rebotar en los obstáculos. El ancho de banda de estas señales es alto y los costos de instalación de los equipos son razonables.

Radio. Consisten en ondas electromagnéticas más bajas que las de microondas. Las frecuencias de radio se extienden en el rango de los Kilohertz (10 KHz – 100 MHz) son fáciles de generar y pueden cruzar distancias largas, y entrar fácilmente en los edificios, son omnidireccionales , lo cual implica que los transmisores y receptores no tiene que ser alineados.
Los equipos para transmitir y recibir ondas de radio son relativamente baratos y son usados raramente para la comunicación de datos; las señales son a menudo afectadas por ruido e interferencia.

Láser. La luz láser posee dos propiedades que la hacen ideal para la comunicación de datos: proporciona un rayo de luz que consiste enteramente de luz de una sola frecuencia. También cada una de las ondas de luz es orientada en paralelo; esta propiedad es conocida como coherencia. La coherencia y pureza de la luz láser hacen posible crear poderosos rayos de luz.
La mayoría de la luz láser usada en las comunicaciones de datos, cae en el rango de la luz infrarroja, y por lo tanto, no visible al ojo humano. Esta luz puede ser transmitida a distancias moderadas y es sensitiva a atenuación de fenómenos atmosféricos. Ofrecen un ancho de banda alto con costo bajo.

Los satélites son básicamente medios de comunicación a través de microondas porque éstos son esencialmente antenas repetidoras de ondas. Un satélite contiene algunos transponedores que reciben las señales de alguna porción del espectro, las amplifican, y las retransmiten en otra

frecuencia. Hay tres bandas principales: C (que tiene problemas de interferencia terrenal), Ku, y Ka (que tienen problemas con la lluvia).
Un satélite tiene 12-20 transponedores, cada uno con un ancho de banda de 36-50 MHz y una velocidad de transmisión de 50 Mbps es típica. Además utilizan la multiplexación de división de tiempo.
La altitud de 36.000 km sobre el ecuador permite la órbita geosíncrona, pero no se pueden ubicar los satélites con espacios de menos de 1 o 2 grados y los tiempos de tránsito de 250-300 milisegundos son típicos.
Los fuertes del medio son la comunicación broadcast, la comunicación móvil, y la comunicación en las áreas con el terreno difícil o la infraestructura débil.

Medio limitado

El Medio limitado[1] transmite los datos llevando la señal a través de una ruta física específica (cables y fibra óptica), por ejemplo:

Cable coaxial. Un alambre dentro de un conductor cilíndrico, tiene un excelente blindaje y puede cruzar distancias mayores con velocidades mayores (por ejemplo 1-2 Gbps) Es altamente resistente a EMI y soporta un alto ancho de banda. Algunos tipos de cable coaxial tienen un pesado blindaje para mejorar sus características de alargar las distancias de las señales para que éstas puedan ser transmitidas confiablemente.
El cable coaxial tiene las siguientes ventajas: es altamente insensible a EMI, soporta ancho de banda alto y es para ambientes rígidos.
Sus desventajas son: vulnerables a EMI en condiciones rigurosas tales como fábricas y son muy voluminosos.

Par trenzado(Twisted Pair). Consiste en dos alambres de cobre enroscados (para reducir interferencia eléctrica); estos cables pueden ser fabricados de múltiples pares de alambres envueltos por un sólo forro y son utilizados en el sistema telefónico.
El trenzado en los pares de cables es una parte importante de las características eléctricas del cable TP. Las trenzas reducen la sensibilidad a EMI y las señales de frecuencia de radio. Es muy fácil de instalar y no es caro, pero es un medio de transmisión lento.

Fibra óptica. Los cables de fibra óptica utilizan ondas de luz para transmitir datos a través de un grupo de fibras de vidrio delgadas o fibras plásticas altamente reflexivas. Estas señales son generadas por diodos que emiten luz (LED´s) y por diodos de inyección láser (ILD´s). La pureza de la luz láser incrementa la velocidad de transmisión en los datos cubriendo mayores distancias(hasta 100 Mb/s). Estas señales son recibidas por fotodiodos que detectan variaciones en la intensidad de la luz.

El diámetro típico exterior de una fibra óptica es de 0.125 mm. Las fibras ópticas son inmunes a interferencias electromagnéticas gracias a su naturaleza dieléctrica y son muy utilizadas para transmisión de información a grandes distancias. Actualmente se encuentran en el mercado sistemas que por medio de una fibra óptica pueden transmitir 2.4 Gbps (billones de bits por segundo), lo que equivale a tener una capacidad aproximada de 33,000 canales telefónicos.

Los cables de fibra óptica ofrecen un alto ancho de banda y la señal no puede ser afectada por interferencia electromagnética. La transmisiones en fibra óptica son extremadamente seguras.
Este tipo de cable no es fácil de instalar y normalmente está limitado a conexiones punto a punto.

1 Puede observar la clasificación de par torcido, coaxial, fibra óptica en el apendice A.

1.5.2 Módem

El término módem proviene de Modulación y Demodulación. La modulación es el proceso para codificar una señal digital sobre un medio analógico. Demodulación es el proceso de recobrar la señal digital original. El módem es capaz de llevar el proceso de transmisión de datos en ambas direcciones.

Un módem es un periférico DCE que conecta un DTE con un medio de transmisión analógica. Este acepta las señales desde su DTE modulándola a un medio analógico. En el receptor final, el módem demodula la señal para extraer la información digital original.

Estos periféricos son clasificados en:

Módem Síncrono. Operan a altas velocidades, transmiten y reciben información en base a ciclos de reloj. Tienen tasa fija de transmisión de datos y típicamente utiliza las modulaciones PSK(codificación de cambio de fase) y QAM(modulación de amplitud en cuadratura).

Módem Asíncrono. Operan a bajas velocidades y no transmiten ni reciben ciclos, tasa variable de transmisión de datos y normalmente utilizan la modulación FSK (modulación por desplazamiento de frecuencia). Son típicamente utilizados para terminales interactivas.

Funcionalidad de los módem[2]

Su función básica es permitir la comunicación entre dos o más estaciones de trabajo, cuando es necesario utilizar la red telefónica. Un módem acepta datos de 0un ordenador transmisor y convierte las señales digitales de este en señales analógicas para transmitirlas mediante la línea telefónica y en el lado receptor el módem decodifica esas señales y las convierte en señales digitales a modo de que el ordenador receptor pueda entenderlas; este proceso se lleva a cabo mediante la modulación/demodulación de señales, su rendimiento y costo tiene que ver con la velocidad de transmisión y él numero de funciones de las que dispone.
La velocidad de transmisión de un módem es el número máximo de bits a que puede transmitir o recibir datos (figura 12.1)

Características de los módem

La mayoría de los módem constan de un microprocesador y de una memoria lo que los hace tener un cierto nivel de inteligencia. Sus características principales son:

Memoria: Almacenan números telefónicos que el usuario pueda requerir en cualquier momento.

Marcador automático de números: Permite al usuario marcar un numero de teléfono por medio del teclado de la estación, en vez de utilizar el aparato telefónico.

Respuesta automática: Proporciona a la estación la posibilidad de responder a una llamada sin que intervenga para nada el usuario.

Llamada automática: Permite al usuario dejar mensajes para que se envíen a una hora y fecha determinada, a un lugar específico.

Devolución de llamada: Cuando el módem contesta una llamada, comprueba la identidad del emisor en una lista de autorizaciones previamente establecida. Si el emisor está autorizado, el

[2] recomendaciones para módem en apéndice b

módem corta la llamada y entonces llama automáticamente al usuario al número de teléfono indicado en la lista

1.6 Sistema telefónico

El sistema telefónico consiste en las oficinas de conmutación, los alambres entres los clientes y las oficinas (local loops), y los alambres de las conexiones de larga distancia entre las oficinas (troncales), en esta parte vamos a considerar conceptos que forman cualquier red de comunicaciones y que pueden explicarse fácilmente utilizando el modelo de la red telefónica.

Local loops

Los local loops son analógicos; las computadoras tienen que usar un módem para convertir una señal digital en una analógica, y en la oficina de compañía de teléfonos un codificador que convierte la señal a digital de nuevo. Existen tres problemas de transmisión que generalmente acompañan a la señal:

- ✓ Atenuación. Los componentes Fourier diferentes de una señal se atenúan por montos distintos.
- ✓ Distorsión de retraso. Los componentes diferentes tienen velocidades diferentes. Dos bits en un cable se pueden entremezclar.
- ✓ Ruido. Tipos: termal, cross talk (inducción entre alambres), e impulsos (de puntos de poder).

Debido a estos problemas no es deseable tener un gran rango de frecuencias en la señal. Por desgracia las ondas cuadradas de la señalización digital tienen un espectro grande. Por lo tanto los módem transmiten un portador de onda sinusoidal y modulan la amplitud, la frecuencia, o la fase. Otro problema es el de los ecos; frecuentemente se refleja una parte de la señal. Una solución para la voz es un supresor de eco, que cambia la línea de full-duplex a half-duplex y cambia el sentido de transmisión rápidamente. Un tono de 2100 Hz puede desactivar los supresores (un ejemplo de la señalización en banda). Una alternativa es un cancelador de eco, que preserva la transmisión full-duplex y resta una estimación del eco a la señal. Al largo plazo hay que convertir los local loops a la fibra, pero es muy caro. Una solución intermedia es instalar la fibra primero solamente en las calles y continuar usar el par trenzado para la conexión al domicilio.

Multiplexación y Troncales

El costo de instalar y mantener una línea troncal es casi lo mismo para una línea de ancho de banda bajo como para una línea de ancho de banda alta. Por lo tanto las compañías de teléfonos multiplexan llamadas múltiples en una sola línea de ancho de banda alto.

Multiplexación de división de frecuencias (MDF). Se usan filtros para restringir cada canal telefónico a solamente 3000 Hz. Para asegurar una buena separación se alocan 4000 Hz para cada canal. Se eleva la frecuencia de cada canal de voz y entonces se combinan; cada canal es independiente de los otros.

Multiplexación de división de longitud de onda. Es la misma idea como MDF, pero con luz y fibras. Ya que cada canal en una fibra no puede tener un ancho de más de unos gigahertz (debido a la velocidad máxima de convertir entre señales ópticas y eléctricas), es una buena manera de usar el ancho de banda de cerca 25.000 GHz de una fibra. En este caso los canales entrantes deben tener frecuencias distintas y se combinan con un prisma.

Multiplexación de división de tiempo (MDT). El problema con MDF es que hay que usar circuitería analógica. Por contraste se puede manejar la MDT completamente con la electrónica digital. En

MDT cada usuario tiene sucesivamente todo el ancho de banda del canal por un momento. Se puede usar MDT solamente con los datos digitales.

MDT en el sistema telefónico.

El primer paso en el uso de MDT es la conversión de las señales analógicas. Debido al teorema de Nyquist, se puede capturar toda la información de una señal de H Hertz con una frecuencia de muestras de 2H. Un codificador (coder-decoder) muestrea el flujo 8000 veces por segundo (125 microsegundos por muestra). Este proceso se llama (en el mundo telefónico) Pulse Code Modulation (PCM).

Un ejemplo de un portador de MDT es una línea T1, que multiplexa 24 canales de voz. Un solo codificador muestrea cada canal sucesivamente; cada uno produce 7 bits de dato y 1 bit de control por muestra. Por tanto hay 7×8000 = 56.000 bps de datos por canal, y 8000 bps de control. Cada marco del T1 tiene 24×8 = 192 bits, más un bit para control de marcos. Tenemos 193 bits cada 125 microsegundos, que es 1,544 Mbps. El bit 193 alterna entre 0 y 1. El receptor lo usa para la sincronización.

Un T2 (6,312 Mbps) consiste en 4 canales T1, un T3 (44,736 Mbps) de 6 T2, y un T4 (274,176 Mbps) de 7 T3. Cada uno agrega bits de control y de marco.
SONET (Synchronous Optical Network) es un sistema de MDT para la fibra. El marco cada 125 microsegundos tiene 810 bytes, que implica 51,84 Mbps.

Conmutación

Los dos tipos principales son la conmutación de circuito y la conmutación de paquetes.

	de circuito	de paquete
Ruta dedicado de "cobre"	Sí	No
Ancho de banda disponible	Fijo	Dinámico
Posibilidad de malgastar ancho de banda	Sí	No
Transmisión de store-and-forward	No	Sí
Cada paquete toma la misma ruta	Sí	No
Inicialización de la ruta	Necesario	No necesario
Puntos donde la congestión puede ocurrir	En inicialización	Con cada paquete
Cobrar	Por minuto	Por paquete

Conmutadores de crossbar (travesaño). Tiene N inputs, N outputs, y N^2 intersecciones. Problema: la escalabilidad. Si N=1000, tenemos 1.000.000 intersecciones.

Conmutadores de división de espacio. Consisten en tres (o más) etapas de conmutadores de crossbar. En la primera etapa hay N/n crossbars con n inputs y k outputs cada uno. En la segunda hay k crossbars de N/n × N/n. La tercera etapa es el revés de la primera.

El número de intersecciones es $2kN + k(N/n)^2$. Si N=2000, n=50, y k=10, hay solamente 24.000. Empero permite solamente 200 conexiones simultáneas.

Con valores de k mayores hay menor probabilidad de bloqueo, pero el costo del conmutador aumenta.

Conmutadores de división de tiempo. Son digitales y la operación tiene las siguientes etapas:

Se examinan los n canales de input sucesivamente para construir un marco de input con n entradas de k bits. (En una línea T1 k=8 y se procesan 8000 marcos por segundo.)

El intercambiador de entradas de tiempo acepta los marcos de input. Ubica las entradas en orden en una tabla de RAM y entonces lee las entradas a un marco de output usando la tabla de mapping.

Se mandan los contenidos del marco de output a los canales de output.

La limitación de conmutadores de división de tiempo es el tiempo de ciclo de la memoria. Si cada acceso requiere T microsegundos, el tiempo para procesar un marco es 2nT, y debe ser menos de 125 microsegundos. Si T es 100 nanosegundos, n=625. Se puede construir conmutadores con etapas múltiples para solucionar este problema.

Velocidad máxima de un canal

Se puede representar cualquiera señal de datos con una serie Fourier. La serie consiste en función de frecuencias distintas, y se suman los términos para reconstruir la señal.

Ningún medio de transmisión puede transmitir señales sin perder algún poder. Normalmente un medio puede transmitir las frecuencias desde 0 hasta algún límite f; las frecuencias mayores se atenúan fuertemente. Cuanto más cambios por segundo de una señal (la razón de baud), tantos más términos de frecuencias altas se necesitan.

El ancho de banda de un canal determina la velocidad de la transmisión de datos, aun cuando el canal sea perfecto. Si tenemos un canal de ancho de banda H (en Hertz) y V niveles discretos de señal, entonces la velocidad máxima en un canal perfecto (en bits por segundo) es

$$v_{max} = 2H \log_2 V$$

Esto es el teorema de Nyquist.

Una línea telefónica tiene un ancho de banda de aproximadamente 3000 Hz. No puede transmitir las señales binarias más rápidamente que 6000 bps. ¿Cómo pueden transmitir los módem modernos a velocidades mayores? En realidad los canales no son perfectos y sufren del ruido aleatorio. Si el poder de la señal es S y el poder de ruido es R, la razón de señal a ruido es S/R. Normalmente se expresa esta razón en los decibeles (dB), que son $10\log_{10}S/R$.

La velocidad máxima en bps de un canal con ancho de banda H Hz y razón de señal a ruido de S/R es

$$v_{max} = H \log_2(1+S/R)$$

Si una línea telefónica tiene un S/R de 30 dB (o 1000), un valor típico, no puede transmitir más de 30.000 bps, independientemente del número de niveles de señal.

1.7 Dispositivos para Redes

A medida que una empresa crece las estaciones de trabajo y usuarios de red aumentan y las necesidades de comunicación con el exterior también aumentan; y antes de proceder a establecer conexión con dispositivos exteriores de la red es necesario resolver los problemas que existen en las comunicaciones entre dos sistemas distintos (tal como direccionamiento, formato de los mensajes, control de errores, método de transmisión, etc.). de tal forma que los dispositivos

utilizados cubran las características del modelo de comunicación para una red considerando las siguientes funciones de comunicación:

Funciones básicas: los servicios de los que se han de disponer en todo momento, incluso cuando las redes que se van a comunicar son del mismo tipo. Aquí se incluyen el desvío de mensajes de una red a otra, y el direccionamiento de mensajes.

Funciones avanzadas: los servicios de que se ha de disponer cuando las redes que han de conectarse no disponen de las mismas funciones, por ejemplo detección de errores, conversión de protocolos, etc.

El tipo de funciones de conexión depende de los servicios que sean necesarios y los dispositivos adecuados deben cubrir las necesidades antes mencionadas. Los siguientes dispositivos permiten que en una red los diferentes recursos establezcan comunicación entre sí ó entre otras redes, proporcionando un óptimo rendimiento de los equipos.

- Hubs
- Gateways (Puertas)
- Routers
- Bridges

Tal como se menciono en las redes locales son los servidores de comunicaciones[3] los encargados de gestionar las comunicaciones con el exterior. Estos han sido diseñados para liberar a la red de las tareas relativas a la transmisión de información con destinos externos. Por medio del servidor de comunicaciones una estación puede llamar a una red externa o cualquier otro sistema, buscar cierta información y enviarla a la a estación que la ha solicitado y esté se puede utilizar también para conectar dispositivos incompatibles a una red.

1.7.1 Gateways

Hemos mencionado que todos los usuarios de una red local pueden compartir datos y dispositivos de la misma red, pero cuando se desea obtener datos de otra red local; es necesario utilizar los dispositivos de hardware y software conocidos como gateways o "puertas", cuya función principal es convertir el protocolo con que se comunica una red al protocolo de comunicación de la otra red.

Un gateway es un dispositivo que interconecta dos redes, pero entre dos redes hay muchas incompatibilidades que nos hacen observar lo siguiente:

Una puede tener un tamaño de paquete mayor que la otra, y por lo tanto será necesario reducir su tamaño, a este proceso se le conoce como fragmentación.

Una de ellas puede tener un complejo método de detección y recuperación de errores y mientras la otra no tenerlo.

Cada red dispone de su propio protocolo de control de acceso a los usuarios y éste puede ser distinto en ambas.

[3] Ver pagina 8
Clasificación de los servidores

Lo que hace el gateway es servir de intermediario entre las comunicaciones de ambas redes, y esta diseñado para reducir problemas de entendimiento entre las redes o los dispositivos. Las redes que enlaza un gateway pueden ser dos redes locales que empleen distintos protocolos, o una red local y una red dedicada de larga distancia. Sus características son las siguientes:

Acepta mensajes procedentes de cualquier dispositivo de la red.

Da a los datos el formato necesario para que la otra red pueda aceptarlos.

Añade la información de control, dirección, y de ruta.

Lleva el mensaje hasta su destino.

Además de las interfaces de hardware y de software, el gateway contiene una cantidad importante de memoria intermedia (buffer). Este buffer es necesario, puesto que cuando el gateway recibe la orden de transmitir un mensaje de una red a otra, tiene que esperar a que se produzca una oportunidad para hacerlo y mientras tanto ha de guardar el mensaje en algún sitio; y se utiliza para otras funciones como regulación de velocidad y conversiones de protocolos. El buffer forma parte importante del proceso de conversión de protocolos, ya en uno solo puede haber hasta cuatro procesos de conversión.

Se pueden distinguir dos tipos de gateways: dedicados y no dedicados. Los gateways dedicados son dispositivos de hardware especializado que se dedican exclusivamente ha hacer de enlace. Un gateway no dedicado puede ser una estación de trabajo que se dedique a otras tareas además de servir de enlace.

1.7.2 Bridges (Puentes)

A medida que aumenta el tamaño y complejidad de las redes, cada vez se va haciendo más necesario un medio que se encargue de la demanda de servicio. En general cuanto mayor es la red, más diversas son las necesidades de los usuarios; y empieza a ser conveniente dividir la red en varias subredes, para conectar estas subredes se emplea un bridge o "puente".

Un bridge conecta dos redes, normalmente una que se encuentra junto a la otra, puesto que las subredes son parte de o que antes era una sola red; las redes conectadas por medio de un puente utilizan los mismos protocolos.

La función principal de un puente es pasar información de una subred a la otra, es decir, envían y filtran paquetes de acuerdo con sus direcciones de destino. Los puentes son dispositivos que trabajan al nivel OSI de Enlace de Datos. Mantienen una tabla que contiene las direcciones de las estaciones de trabajo conectadas a la red local que se utilizan para redireccionar los paquetes al destino final de la red.

Normalmente son muy rápidos porque no necesitan realizar ningún reformateo, simplemente leen una dirección de destino y toman la decisión de filtrar o transferir el paquete. Los puentes aceptan distintos tipos de cableado, por ejemplo, una red Ethernet con cable coaxial de banda ancha puede conectarse mediante un puente a una segunda red Ethernet que utiliza par trenzado.

Igual que los gateways, los puentes tienen dos interfaces, uno para cada subred, una cierta cantidad de memoria intermedia, la lógica y control suficientes para saber que mensajes son los que se han de transmitir a la otra red.

La diferencia principal entre un puente y un gateway es el tipo de redes que conectan. Los puentes conectan redes iguales con el mismo protocolo que a su vez forman parte de una red local mayor, mientras que los gateways conectan redes locales distintas y redes de larga distancia. Otra diferencia importante son los tipos de conexión; un gateway efectúa conversiones de protocolo, mientras que el puente no lo hace. Figura 1.11

Figura 1.11 Representación de un Bridge.

1.7.3 Routers (encaminador)

Un router o "encaminador" es un conjunto de hardware y software que conecta redes con diferentes formatos de comunicación o protocolos. Con algunos sistemas de red, los routers pueden conectar redes con topología diferente, como ARCnet, Ethernet o Token Ring.

Los routers leen en los paquetes la información sobre direccionamiento y añaden más información para transportarlo por la red. Por ejemplo, un router podría tomar un paquete Ethernet con información sobre direccionamiento y transmisión para llevarlo a través de una red de paquetes conmutados X.25; al llegar el paquete al otro extremo de la red X.25 el router receptor interpreta los datos, asigna la dirección apropiada al paquete y lo envía al destino apropiado de la LAN receptora.

Estos dispositivos realizan conexiones inteligentes entre distintos elementos de redes complejas, pueden seleccionar rutas redundantes entre puntos de una LAN y pueden unir segmentos que utilizan empaquetado de datos totalmente diferentes, así como esquemas de acceso al medio diferentes. Sin embargo, debido a su complejidad, los routers transmiten los datos más despacio que los puentes, a diferencia de estos últimos, no conocen la localización exacta de cada nodo, solo tiene información sobre direcciones de otras redes.

El direccionamiento utilizado por los rotures permite dividir la red en varias redes secundarias y por lo tanto se puede utilizar topología diferente.

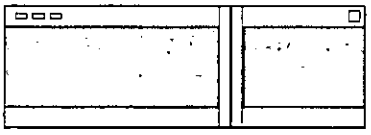


Figura 1.12 Representación de un ruteador

El router decide el camino que va a seguir un paquete, por lo general el camino más corto y con menor numero de vanos conectados entre segmentos. Para ello utiliza una tabla de direcciones creada específicamente para la red; este tipo de router se conoce con el nombre de "router estático".

Otro tipo de router son los "routers dinámicos", que permiten utilizar factores como el costo que supone el envío a través de determinados enlaces y la cantidad de tráfico, para determinar la ruta a

seguir por los paquetes. La compilación de toda esta información, la complejidad de las tablas de direcciones y la toma de decisiones hace que el tiempo de transmisión sea mayor.

1.7.4 Hub de conexiones

Un hub de conexiones, conocido con el nombre de concentrador, es un dispositivo que permite centralizar el cableado de la red y hacer que resulte más sencillo gestionar esta función de la red. El primer tipo de red en ofrecer este método de conexiones fue Token Ring, y después fue posteriormente adoptado por Ethernet y comercializado con el nombre de 10baseT. Una de las principales características del hub es que facilita los cambios e inserción de nuevos usuarios a la red. Si un usuario es transferido de un departamento de la empresa a otro, no es necesario cambiar las conexiones de la red, sólo cambiar la estación de trabajo al nuevo departamento y conectarla al hub en la nueva posición.

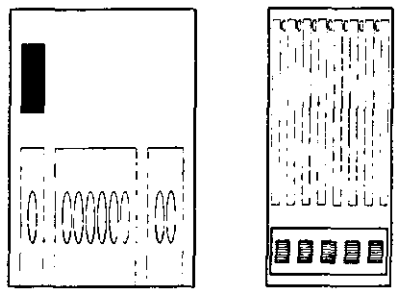


Figura 1.13 representación de un HUB

Hay un tipo de hub que dispone de una determinada inteligencia para transferir información de gestión a un paquete de software, conocido con el nombre de hub inteligente. El software permite al administrador gestionar y controlar todas las funciones del hub. La posibilidad de ver todas las actividades del hub en una pantalla es de gran valor cuando se trata de una red muy grande con cientos de nodos y varias redes locales distintas conectadas.

CAPITULO SEGUNDO
ARQUITECTURA DE RED

2.1 Arquitectura

Dentro del área de comunicaciones, un término que de modo común escuchamos es el de "arquitectura". Mediante la arquitectura se intenta alcanzar un alto nivel de rendimiento a un costo mínimo; viene determinada por el lugar donde se encuentran las estaciones que se van a conectar, la información que se va a transmitir, los medios de que se dispone, etc. Aunque las redes locales no se pueden clasificar sobre la base de su arquitectura, la combinación de los elementos que la forman determinan las características de una red.

Un conjunto de capas y protocolos recibe el nombre de arquitectura de red. La especificación de una arquitectura debe contener información suficiente para que un implementador pueda escribir el programa o construir el hardware para cada capa de manera que cada una obedezca en forma correcta el protocolo apropiado, que a su vez suele asociarse con una topología específica.

Ni los detalles de la implementación, ni la especificación de las interfaces forman parte de la arquitectura porque se encuentran ocultas dentro de las máquinas y no son visibles desde afuera. Ni siquiera es necesario que las interfaces en todas la s máquinas de la red sean iguales, siempre que cada máquina pueda usar correctamente todos los protocolos.

La lista de protocolos empleados por cierto sistema, con un protocolo por capa, se llama pila de protocolos.

Para montar una red, todos los elementos que la componen, (el equipo, la topología, los enlaces de comunicación, el protocolo, etc.) han de formar un sistema compacto y unitario. Los distintos elementos del sistema pueden, (de hecho así suele ser) variar bastante entre sí, no hay ningún componente que se pueda seleccionar o diseñar aisladamente.

Las partes del sistema han de estar compensadas en su totalidad para que pueda tener lugar la comunicación. Si un solo componente del sistema no se comunica correctamente con el resto, no es posible que la comunicación sea eficaz.

Él numera de posibles combinaciones para formar una red es casi infinito, dado que los equipos y tecnologías cambian muy rápidamente, es necesario disponer de algún sistema para coordinar todos los elementos.

Hay varias organizaciones que se encargan de poner un cierto orden en el proceso de diseño e implementación de las redes locales. Entre ellas destacan la International Standards Organization **(ISO)** y el Institute of Electrical and Electronic Engineers **(IEEE)**.

2.2 Modelo OSI

En 1978 la International Standards Organization **(ISO)** propuso un modelo para comunicaciones de redes locales a las que titularon The reference Model of Open System Interconnection (Modelo de Referencia de Interconexión de Sistemas Abiertos).

"Interconexión de Sistemas Abiertos" significa el intercambio de información entre terminales, ordenadores, personas, redes y procesos.

El Modelo de Referencia de Sistemas Abiertos no es por sí mismo un estándar, ni una descripción de las comunicaciones entre ordenadores. El modelo define donde se han de efectuar las tareas, pero no define cómo se han de efectuar. No especifica ni servicios, ni protocolos. El Modelo OSI intenta proporcionar una base común para coordinar el desarrollo de estándares dirigidos a la conexión entre sistemas.

En la actualidad las funciones propias de una red de computadoras pueden ser divididas en las siete capas propuestas por ISO para su modelo de sistemas abiertos (OSI). Sin embargo, la implantación real de una arquitectura puede diferir de este modelo.

Los principios que se aplicaron para llegar a las siete capas son los siguientes:

- ✓ Se debe crear una capa siempre que se necesite un nivel diferente de abstracción.
- ✓ Cada capa debe realizar una función bien definida.
- ✓ La función de cada capa se debe elegir pensando en la definición de protocolos estandarizados internacionalmente.

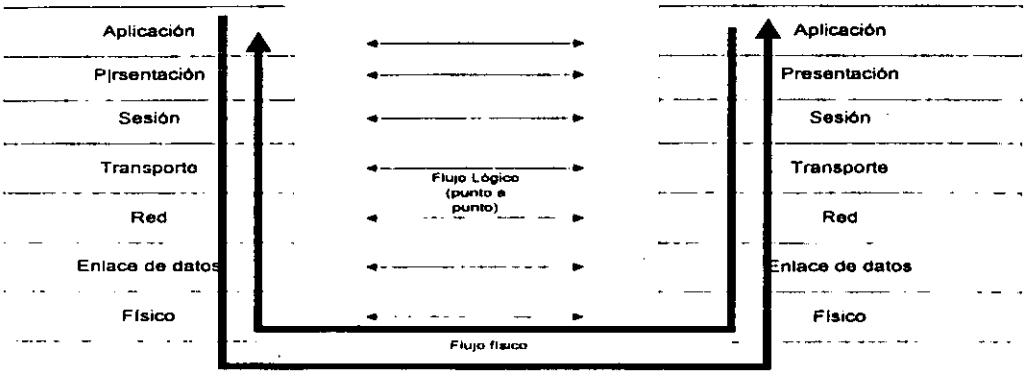


Figura 2.1 Flujo de datos

- ✓ Los límites de las capas deben elegirse a modo de minimizar el flujo de información a través de las interfaces.
- ✓ La cantidad de capas debe ser suficiente para no tener que agrupar funciones distintas en la misma capa y lo bastante pequeña para que la arquitectura no se vuelva inmanejable.

2.2.1 Descripción del Modelo OSI

El modelo se compone de un conjunto ordenado de subsistemas o "niveles" popularmente conocidos como capas. Los niveles del modelo OSI están separados por interfaces. Los niveles adyacentes se comunican entre sí por medio de una interfaz común.

Todos los niveles de la estructura disponen de un conjunto de servicios para el nivel superior que tienen por debajo. La relación entre los distintos niveles y la información que se ha de pasar es definida en cada capa.

Las interfaces se encuentran donde un nivel se comunica con otro, y sirven para separar un nivel del siguiente. Puesto que es fácil esperar que los mecanismos y funciones de los niveles cambien a medida que cambia la tecnología, las funciones de las interfaces están bien definidas, pero el

formato utilizado para transferir datos entre niveles no lo ésta. Esto permite cambiar las características de un nivel sin que afecte al resto del modelo.

Los protocolos asociados con los niveles uno a cuatro son iguales para todos los sistemas. Los niveles cinco a siete dependen del sistema. Para cada dispositivo hay que definir protocolos diferentes. Algunos consideran los cuatro primeros niveles como funciones de comunicación y los tres restantes como funciones de proceso.

CAPA	FUNCIÓN
CAPA 7 APLICACIÓN	Funciones de usuario final y aplicación final, como transferencia de archivos (FATM), servicio a terminales virtuales (VTP) y correo electrónico.
CAPA 6 PRESENTACIÓN	Traducción de datos para ser usados por la capa 7, como conversión de protocolos, descompresión de datos, codificación y expansión de comandos gráficos.
CAPA 5 SESIÓN	Ofrece el establecimiento de una conexión de sesión entre dos entidades de presentación para soportar el intercambio ordenado de datos.
CAPA 4 TRANSPORTE	Transparencia de datos entre entidades de sesiones que liberan a la capa de sesión de la necesidad de preocuparse por la confiabilidad e integridad de los datos.
CAPA 3 RED	Ofrece el medio para establecer, mantener y poner fin a conexiones de redes entre sistemas abiertos, en particular enviando funciones a través de diferentes redes.
CAPA 2 ENLACE DE DATOS	Define la estrategia de acceso para compartir el medio físico, incluyendo los aspectos de enlace de datos y acceso a los medios.
CAPA 1 FÍSICO	Definición de las características eléctricas y mecánicas de la red.

Tabla 2.1 Modelo OSI

Descripción de cada una de las capas

En el modelo OSI, la capa 1, es la base de hardware de la red. Las capas de la 2 a la 7 se implantan en software.

La capa física

El nivel físico define las características eléctricas y mecánicas de las interfaces de la red necesarias para establecer y mantener la conexión física. Este nivel esta pensado para atender a una gran variedad de medios físicos y procedimientos de control, incluye los cables y los conectores, los métodos de transmisión, y los ordenadores y equipos de comunicaciones. Este nivel establece si los bits van a ser enviados half-duplex, (es decir, una terminal envía mientras el otro extremo escucha y cuando el primero ha terminado, el segundo comienza a enviar información) o full-duplex (significa que ambos terminales envían y reciben datos simultáneamente).

Las consideraciones de diseño tienen que ver con la acción de asegurarse de que cuando un lado envíe un bit 1, se reciba en el otro lado como bit 1, no como bit 0; en este nivel se define:

- ✓ Cuantos microsegundos dura un bit.
- ✓ Que cantidad de voltaje deberá utilizarse para representar un 1 y cuanto para un 0.
- ✓ Como se establece la conexión inicial y como se interrumpe cuando ambos lados han terminado.
- ✓ Cuantas puntas tiene el conector de red y para que sirve cada una.
- ✓ Si la transmisión puede efectuarse simultáneamente en ambas direcciones o no.

La capa 1 es el estrato físico (aquel que define las características eléctricas y mecánicas de la red). Las técnicas de modulación, las frecuencias en las que opera la red y los voltajes empleados son todas las características de la capa 1. Como todas las redes deben de implementar los estratos 1 y 2, estos reciben la mayor atención de los fabricantes de redes. Si la atención prestada a esta capa origina componentes compatibles, entonces sabremos si el concepto de los estándares ha sido de utilidad. A menudo, los estándares son más un logro técnico que la ilustración de la posibilidad de algunos fabricantes de procurar la aprobación de un estándar para sobresalir.

La capa de enlace de datos

La función principal de la capa de enlace de datos es tomar un medio de transmisión en bruto y transformarlo en una línea que parezca libre de errores de transmisión no detectados a la capa de red. Esta tarea la cumple al hacer que el emisor divida los datos de entrada en marcos de datos (unos cientos, o miles de bytes normalmente), que transmita los datos en forma secuencial y procese los marcos de acuse de recibo que devuelve al receptor. Puesto que la capa física solamente acepta y transmite una corriente de bits sin preocuparse por su significado o estructura, corresponde a la capa de enlace de datos crear y reconocer los límites de los marcos. Esto se puede lograr añadiendo patrones especiales de bits al principio y al final del marco. Si estos patrones de bits ocurrieran en los datos por accidente, se debe tener cuidado especial para asegurar que estos patrones no se interpretaran incorrectamente como delimitadores de marcos. Una ráfaga de ruido en la línea puede destruir por completo un marco. En este caso, el software de la capa de enlace de datos de la máquina fuente puede retransmitir el marco. Sin embargo las transmisiones retransmitidas del mismo marco introducen la posibilidad de duplicar marcos. Se podría enviar un marco duplicado si se perdiera el marco del acuse de recibo que el receptor devuelve al emisor. Corresponde a esta capa resolver el problema provocado por los marcos dañados, perdidos y duplicados. La capa de enlace de datos puede ofrecer varias clases de servicio distintas a la capa de red, cada una con diferente calidad y precio.

Otra consideración que surge en la capa de enlace de datos es como evitar que un transmisor veloz sature de datos a un receptor lento. Se debe emplear algún mecanismo de regulación de tráfico para que le transmisor sepa cuánto espacio de almacenamiento temporal (buffer) tiene el receptor en ese momento. Con frecuencia esta regulación de flujo y el manejo de errores están integrados.
Si se puede usar la línea para transmitir datos en ambas direcciones, esto introduce una nueva complicación que el software de la capa de enlace de datos debe considerar. El problema es que los marcos de acuse de recibo para el tráfico de A a B compiten por el uso de la línea con marcos de datos para el tráfico de B a A.

Las redes de difusión tienen una consideración adicional en la capa de enlace de datos: cómo controlar el acceso al canal compartido. Una subcapa especial de la capa de enlace de datos se encarga de este problema a la subcapa de enlace al medio.

La capa de enlace de datos (capa 2) define la estrategia de acceso para compartir el medio físico (el cable de la variedad que sea). Entre las técnicas más comunes para las redes de área local se encuentran sistemas Carrier Sense Multiple Access/Collision Detection (CSMA/CD, o Acceso múltiple con detección del portador/Detección de colisión) y de transmisión de señales codificadas. Las

técnicas de transmisión de información específica de la red en paquetes de datos, como la dirección de un nodo son funciones de la capa 2.

La capa de red

Se ocupa de controlar el funcionamiento de la subred. Una consideración clave de diseño es determinar como se encaminan los paquetes de la fuente a su destino. Las rutas se pueden basar en tablas estáticas que se alambran en la red y rara vez cambian. También se pueden determinar al inicio de cada conversación, por ejemplo en una sesión de terminal. Por último pueden ser altamente dinámicas, determinándose de nuevo con cada paquete para reflejar la carga actual de la red.

Si en la subred se encuentran presentes demasiados paquetes a la vez, se estorbarán mutuamente, formando cuellos de botella. El control de tal congestión pertenece también a la capa de red. Cuando menos, el software debe contar cuantos paquetes o caracteres o bits envía cada cliente para producir información. Cuando un paquete cruza una frontera, con sistema diferente de cada lado, a la situación se puede complicar.

Cuando un paquete debe viajar de una red a otra para alcanzar su destino, pueden surgir muchos problemas. El tipo de direcciones que usa la segunda red puede ser diferente del de la primera; puede ser que la segunda no acepte en absoluto el paquete por ser demasiado grande; los protocolos pueden diferir y otras cosas. La capa de red debe resolver todos estos problemas para lograr que se interconecten redes heterogéneas.

En las redes de difusión el problema del ruteo es simple y la capa de red con frecuencia es delgada o incluso inexistente.

En muchas de las redes de área local no se necesita una capa 3 (capa de la red) funcional. Las redes que requieren mecanismos de envío entre nodos si requieren de la capa 3. Sin embargo, las LAN, en alguna implantación, transmiten datos a todos y cada uno de los nodos, y una conexión especifica recolecta esos paquetes adecuadamente direccionados a ella.

Las LAN de banda base, como Ethernet, transmiten en general en un solo canal y no requieren de dispositivos de envío. No obstante, los sistemas de banda ancha se diseñan frecuentemente con agilidad de frecuencia (la posibilidad de usar únicamente un solo canal); y, por lo tanto, requieren de algún mecanismo de enlace por puente (ese mecanismo requiere a su vez alguna técnica de envío). Pese a ello, cuando las LAN se conectan entre sí a través de vías de acceso se requiere de un estrato 3 funcional.

La capa de transporte

El objetivo de la capa de transporte (capa 4) es proporcionar un nivel adicional, aunque de nivel inferior, de conexión que la capa de sesión. Dentro de la capa de transporte se confrontan aspectos relacionados con un nivel de confiabilidad fundamental en la transferencia de datos. Estos aspectos incluyen control del flujo, manejo de errores y problemas que se presentan con la transmisión y recepción de paquetes.

Su función básica es aceptar datos de la capa de sesión, dividirlos en unidades más pequeñas, si es necesario, pasarlos a la capa de red y asegurar que todos los pedazos lleguen al otro extremo correctamente, y todo esto se debe de hacer de manera eficiente y en forma que aísle a las capas superiores de los cambios inevitables en la tecnología del hardware. En condiciones normales la capa de transporte crea una conexión de red distinta para cada conexión de transporte que requiera la capa de sesión. Sin embargo si la conexión de transporte requiere un volumen de

transmisión alto, la capa de transporte podría crear múltiples conexiones de red, dividiendo los datos entre las conexiones para aumentar el volumen. Por otro lado, si es costoso crear o mantener una conexión de red, la capa de transporte puede multiplexar varias conexiones de transporte en la misma conexión de red para reducir el costo. En ambos casos, la capa de transporte debe lograr que la multiplexión sea transparente para la capa de sesión.

Determina también que tipo de servicio proporcionará a la capa de sesión y, finalmente, a los usuarios de la red. El tipo más popular de conexión de transporte es un canal de punto a punto libre de errores que entrega mensajes o bytes en el orden en que se enviaron. Sin embargo, otras posibles clases de servicio de transporte son el transporte de mensajes aislados sin garantía respecto al orden de entrega y la difusión de mensajes a múltiples destinos. El tipo de sesión se determina al establecer la sesión.

La capa de transporte es una verdadera capa de extremo a extremo, del origen al destino. En otras palabras, un programa en la máquina fuente sostiene una conversación con un programa similar en la máquina de destino, haciendo uso de los encabezados de mensaje y de los mensajes de control.

En las capas bajas, los protocolos se usan entre cada máquina y sus vecinas inmediatas, y no entre las máquinas de origen y destino, que pueden estar separadas por muchos enrutadores, Las diferencias entre las capas 1 a la 3, que están encadenadas, y las capas 4 a la 7, que son de extremo a extremo, figura 2-1. Muchos modos están multiprogramados, lo que implica que múltiples conexiones entran y salen de cada nodo. En este caso se necesita una manera de saber cual mensaje pertenece a cual conexión. El encabezado de transporte es una opción para colocar esta información. Además de multiplexar varias corrientes de mensajes por un canal, la capa de transporte debe cuidar de establecer y liberar conexiones a través de la red. Esto requiere alguna clase de mecanismo de asignación de nombres de modo que un proceso en una máquina pueda describir con quien quiera conversar. También debe haber un mecanismo para regular el flujo de información, a fin de que un nodo rápido no pueda saturar a uno lento; tal mecanismo se llama control de flujo y desempeña un papel clave en la capa de transporte (también en otras capas). El control de flujo entre nodos es distinto del control de flujo entre enrutadores, aunque después veremos que se aplican principios similares a ambos.

La capa de sesión

De particular importancia para las redes de área local es la capa 5 (capa de sesión). Recuerde que una razón importante para implantar una red de área local es obtener conectividad (la posibilidad de que dos o más dispositivos se conecten entre sí). Cuando se hace un enlace entre dos dispositivos se establece una sesión. En un sentido un tanto más técnico, la capa de sesión facilita el establecimiento y terminación de torrentes de datos de dos o más conexiones de LAN o nodos. Cuando una red mapea direcciones en conexiones especificas se lleva a cabo una función de nivel 5.
La capa de sesión permite a los usuarios de máquinas diferentes establecer sesiones entre ellos. Una sesión permite el transporte ordinario de datos como lo hace la capa de transporte, pero también proporciona servicios que son útiles en algunas aplicaciones. Se podría usar una conexión para que el usuario se conecte a un sistema remoto de tiempo compartido o para transferir un archivo entre dos máquinas. Uno de los servicios de la capa de sesión es manejar el control de diálogo. Las sesiones pueden permitir que el tráfico vaya en ambas direcciones al mismo tiempo, o solo en una dirección a la vez. Si el tráfico puede ir únicamente en un sentido a la vez, la capa de sesión puede ayudar a llevar el control de los turnos.

Un servicio de sesión relacionado es le manejo de fichas. Para algunos protocolos, es esencial que ambos lados no intenten la misma operación al mismo tiempo. A fin de controlar estas actividades,

la capa de sesión proporciona fichas que se pueden intercambiar; solamente el lado que posea la ficha podrá efectuar la operación crítica.

Otro servicio de sesión es la sincronización. Considere los problemas que puedan ocurrir cuando se trata de efectuar una transferencia de archivos de 2 horas de duración entre dos máquinas que tienen un tiempo medio entre rupturas de 1 hora. Cada transferencia, después de abortar, tendrá que empezar de nuevo desde el principio y probablemente fallaría también la siguiente vez. Para eliminar este problema, la capa de sesión ofrece una forma de insertar puntos de verificación en la corriente de datos, de modo que después de cada interrupción solo se deban repetir los datos que se transfirieron después del último punto de verificación.

La capa de presentación

La traducción de la información que será utilizada por la capa 7 se lleva a cabo en la capa de presentación (capa 6). Servicios tales como conversión de protocolo, descompresión de datos traducción, codificación, cambios o conversiones de conjuntos de caracteres, y la expansión de comandos gráficos se efectúan en la capa 6.

Esta capa realiza ciertas funciones que se piden con suficiente frecuencia para justificar la búsqueda de una solución general, en lugar de dejar que cada usuario resuelva los problemas. En particular, y a diferencia de todas las capas inferiores que se interesan solo en mover bits de manera confiable de acá para allá, la capa de presentación se ocupa de la sintaxis y a la semántica de la información que se transmite.

Un ejemplo típico de servicio de presentación es la codificación de datos en una forma estándar acordada. La mayor parte de los programas de usuario no intercambian cadenas de bits al azar; intercambian cosas como nombres de personas, fechas, cantidades de dinero y cuentas.

Estos elementos se representan como cadenas de caracteres, enteros, punto flotante y estructuras de datos compuestas de varios elementos más simples. Las diferentes computadoras tienen códigos diferentes para representar cadenas de caracteres, enteros, y con el fin de hacer posible la comunicación entre computadoras con representaciones diferentes, las estructuras de datos por intercambiar se pueden definir en forma abstracta, junto con un código estándar que se usa en el cable. La capa de presentación maneja estas estructuras de datos abstractas y las convierte de la representación que se usa dentro de la computadora a la representación estándar de la red y viceversa.

La capa de aplicación

La capa de aplicación (capa 7) ofrece servicios a usuarios de la red. La responsabilidad de la iniciación y confiabilidad de las transferencias de datos se realiza en la capa 7. El acceso general a la red, el control del flujo y la recuperación de errores son, en parte, función de esta capa. Las tareas se realizan al nivel de la capa 7 y todos los niveles inferiores están diseñados para dar soporte a las aplicaciones. Los sistemas de mensajes electrónicos, recursos de emulación de terminales y la expansión de comandos gráficos son ilustrativos del software que opera en la capa 7.

Contiene varios protocolos que se necesitan con frecuencia. Por ejemplo considere que existen cientos de tipos de terminales incompatibles en el mundo. Considera la situación de un editor de pantalla completa que deba trabajar en una red con muchos tipos diferentes de terminal, cada uno con formatos diferentes de pantalla, secuencias de escape para insertar y eliminar texto, mover el cursos, etc. Una forma de resolver este problema es definir una terminal virtual de red abstracta que los editores y otros programas pueden manejar. Para cada tipo de terminal se debe escribir un

programa para establecer al correspondencia entre funciones de la termina virtual de red y las de la terminal real. Por ejemplo cuando el editor mueva el cursos de la terminal virtual a la esquina superior izquierda de la pantalla, este software debe emitir la secuencia apropiada de órdenes a la terminal real para poner su cursos en su lugar. Todo el software de terminal virtual esta en la capa de aplicación.

Otra función de la capa de aplicación es la transferencia de archivos. Los diferentes sistemas de archivos tienen convenciones diferentes para nombrar los archivos, formas diferentes de representar líneas de texto, etc. la transferencia de un archivo entre dos sistemas diferentes requiere la resolución de estas y otras incompatibilidades. Este trabajo también pertenece a la capa de aplicación, lo mismo que el correo electrónico, la carga remota de trabajos, la búsqueda en directorios y otros recursos de uso general y especial.

En el modelo OSI la capa 1 es la base de hardware de la red, pero no incluye los medios físicos de la comunicación. Las capas de la 2 a la 7 se implantan en software.

2.3 Datagrama, servicio de conexiones y orientado a conexiones

Ahora que hemos mencionado el conjunto de estándares es necesario definir dos conceptos importantes: *servicios sin conexiones y orientados a conexiones*. Estos se conocen también como servicios de *datagramas* y de *circuitos virtuales*, respectivamente. En términos generales, un datagrama puede definirse como un paquete de longitud finita con información suficiente para ser enviado en forma independiente de la fuente al destino sin recurrir a transmisiones anteriores. En general, la transmisión de datagramas no implica el establecimiento de sesiones bipartitas y puede o no causar reconocimiento de la confirmación de la entrega.

Un servicio orientado a conexiones establece una conexión virtual que da el aspecto al usuario de ser un circuito bipartito real. La conexión virtual contrasta con un circuito físico en que es una conexión dinámicamente variable donde paquetes de datos de usuarios secuenciales pueden ser enviados en forma diferente durante el curso de una conexión virtual.

Un servicio sin conexiones no forma una conexión virtual o lógica entre sistemas anfitriones y no garantiza que todas las unidades de datos serán entregadas o bien que se entregaran en el orden adecuado. Las ventajas del servicio sin conexiones son su flexibilidad robustez y soporte de aplicaciones sin conexiones. Las aplicaciones sin conexiones son aquellas que requieren de servicios de envío pero que no requieren de servicios orientados a conexiones.

Un servicio de datagramas, como el que proporciona el Internet Protocol (IP); del Departamento de Defensa de los Estados Unidos (DOD) es un servicio sin conexiones. De la misma forma, en el contexto del modelo OSI, algunos protocolos proporcionan servicios orientados a conexiones, en tanto que otros ofrecen servicios sin conexiones. Además, estos dos tipos de servicios pueden existir en varios niveles. Por ejemplo, el estándar ISO 8473 es un protocolo sin conexiones para la capa de la red y funciona en forma análoga al IP; en tanto que el estándar ISO 8073 es un protocolo orientado a conexiones en la capa de transporte.

El estándar de control de enlace lógico 802.2 del IEEE (ISO 8802/2) puede ser implantado como un servicio sin conexiones u orientado a conexiones en la capa de enlace de datos. En general, si una red se configura para manejar servicios orientados a conexiones en, por ejemplo, la capa de transporte, los protocolos en la capa de red y enlace de datos se implementarán probablemente como servicios sin conexiones.

Ya antes se menciono el estándar de Internet (IP). La DOD ha definido también a TCP: Transmission Control Protocol (o protocolo de control de la transmisión). Cuando menos en Estados

Unidos se escriben obras importantes concernientes a la relación que existe entre TCP/IP y OSI. La razón de ser de esto es que muchas de las operaciones de enlace entre redes en los Estados Unidos se realizan actualmente a través de uso de TCP/IP.

2.4 TCP/IP

La familia de protocolos TCP/IP, surge a mediados de los 70´s con la finalidad de establecer la comunicación entre los diferentes equipos, independientemente de la tecnología de transporte y la arquitectura de la red.

TCP/IP da la posibilidad de que un usuario final se comunique a través de una maquina local con alguna maquina o usuario final distante, lo cual cubre la necesidad de contar con servicios de enlace en redes.

TCP/IP es una familia de protocolos que se basa en software utilizado en redes LAN y WAN, su nombre es una combinación de dos protocolos el Protocolo de Control de Transmisión (Transmisión Control Protocol) y el Protocolo Internet (Internet Protocol) ***TCP/IP***, este término se refiere a un conjunto de programas de software que proporciona servicios de red como registros remotos, transferencia de archivos remotas y correo electrónico, de tal modo que proporciona un método para transferir información de una máquina a otra. El protocolo TCP/IP cubre los requisitos de un protocolo de comunicaciones es decir, maneja los errores de la transmisión, administra el enrutamiento y envío de datos y controla la transmisión real del uso de señales de estado predeterminadas. TCP/IP tiene las siguientes características básicas:

- ✓ Un conjunto común de aplicaciones
- ✓ Enrutamiento dinámico
- ✓ Protocolos sin conexión en le nivel de red
- ✓ Conectividad Universal
- ✓ Intercambio de paquetes
- ✓ Definición del termino cliente/servidor[1]

El protocolo TCP/IP está compuestos de capas.

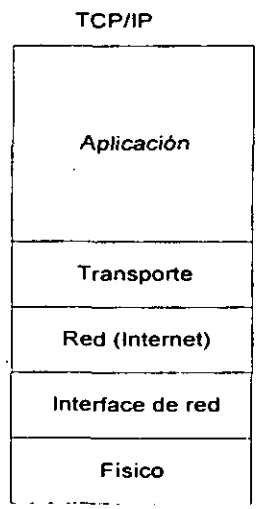


Figura 2.2 Capas TCP/IP

[1] Cualquier dispositivo que inicie comunicaciones se denomina cliente y el dispositivo que responde, se llama servidor.

2.4.1 Diferencias entre OSI y TCP/IP

Las diferencias entre la arquitectura OSI y el TCP/IP se relacionan con las capas encima del nivel de transporte y aquellas del nivel de red. OSI tiene una capa de sesión y una de presentación, en tanto que TCP/IP combina ambas en una capa de aplicación. El requerimiento de un protocolo sin conexión, también requirió que el TCP/IP incluyera además, las capas de sesión y de presentación del Modelo OSI en la capa de aplicación del TCP/IP. El siguiente esquema compara la estructura de OSI (siete capas) con TCP/IP (que llama subredes a los elementos diferentes del nivel de red).

El modelo OSI combina los niveles físico y de vinculación en un controlador inteligente (como una tarjeta de red); lo que permite que se diseñe una subred independiente de cualquier protocolo de red, por lo tanto TCP/IP no considera los detalles, por lo que se hace útil para establecer una conectividad externa es decir, fuera de sistemas cerrados.

Este enfoque en capas dio origen al nombre TCP/IP; sin embargo sólo existe un protocolo para el nivel de red: el Internet Protocol (IP) esto es lo que asegura la conectividad universal del sistema, uno de los objetivos primarios del diseño.

TCP/IP Y ETHERNET

Hasta el momento se ha mencionado la relación del modelo OSI con el TCP/IP, sin embargo es importante mencionar una tecnología llamada Ethernet la cual nos ayudara a comprender términos que definiremos más adelante (direccionamiento, tipos de direcciones, empaquetado de datos, etc.) y en este momento podemos decir, que Ethernet proporciona el cableado físico (capas uno y dos) y TCP/IP el protocolo de comunicaciones (capas tres y cuatro) que se transmite por el cable; por lo que está combinación permite un óptimo funcionamiento entre Ethernet y TCP/IP.

2.5 Tecnología Ethernet

Ethernet es el nombre que se le ha dado a una popular tecnología LAN de conmutación de paquetes (IEEE liberó una versión compatible del estándar utilizando el número 802.3). Existen muchas variantes de Ethernet; analizaremos brevemente el diseño original y posteriormente el diseño actual.

Diseño original

Cada cable Ethernet tiene aproximadamente ½ pulgada de diámetro y mide hasta 500 m de largo. Se añade una resistencia entre el centro del cable y el blindaje en cada extremo del cable para prevenir l a reflexión de señales eléctricas.

El diseño original de Ethernet utilizaba un cable coaxial, llamado Ether, el cable por si mismo es completamente pasivo; todos los componentes electrónicos activos que hacen que la red funcione están asociados con las computadoras que se comunican a la red.

La conexión entre una computadora y un cable coaxial Ethernet requiere de un dispositivo de hardware llamado transceptor. Físicamente la conexión entre un transceptor y un cable Ethernet requiere de una pequeña perforación en la capa exterior del cable.

Los técnicos con frecuencia utilizan él termino TAB para describir la conexión entre un transceptor Ethernet y el cable. Por lo general, una pequeña aguja de metal montada en el transceptor atraviesa la perforación y proporciona el contacto eléctrico con el centro del cable y el blindaje trenzado, algunos fabricantes de conectores hacen que el cable se corte y se inserte una T cada conexión a una red Ethernet tiene dos componentes electrónicos mayores. Un transceptor es

conectado al centro del cable y al blindaje trenzado del cable, por medio del cual recibe y envía señales por el cable Ether. Una interfaz anfitrión ó adaptador anfitrión se conecta dentro del bus de la computadora, (por ejemplo, en una tarjeta madre).

Un transceptor es una pequeña de hardware que pro lo común se encuentra físicamente junto al cable Ether. Además del hardware análogo que envía y controla las señales eléctricas en el cable Ether, un transceptor contiene circuitos digitales que le permiten la comunicación con una computadora digital. El tranceptor, cuando el cable Ether esta en uso puede recibir y traducir señales eléctricas analógicas hacia o desde un formato digital en el cable Ether. Un cable llamado Atachment Unit interfaz (AUI) conecta el transceptor con la tarjeta del adaptador en una computadora anfitrión.

Informalmente llamado cable transceptor el cable AUI contiene muchos cables. Los cables transportan la potencia eléctrica necesaria para operar el tranceptor, las señales de control para la operación del transceptor y el contenido de los paquetes que se están enviando o recibiendo. Cada interfaz de anfitrión controla la operación de un transceptor de acuerdo a las instrucciones que recibe el software de la computadora. Para el software del sistema operativo al interfaz aparece como un dispositivo de entrada/salida que acepta instrucciones de transferencia de datos básicas desde la computadora, controla la transferencia del transceptor e interrumpe el proceso cuando este ha concluido, finalmente reporta la información de estado. Aun cuando el transceptor es un simple dispositivo de hardware, la interfaz de anfitrión puede ser compleja (ej. Puede contener un microprocesador utilizado para controlar la transferencia entre la memoria de la computadora y el cable Ether).

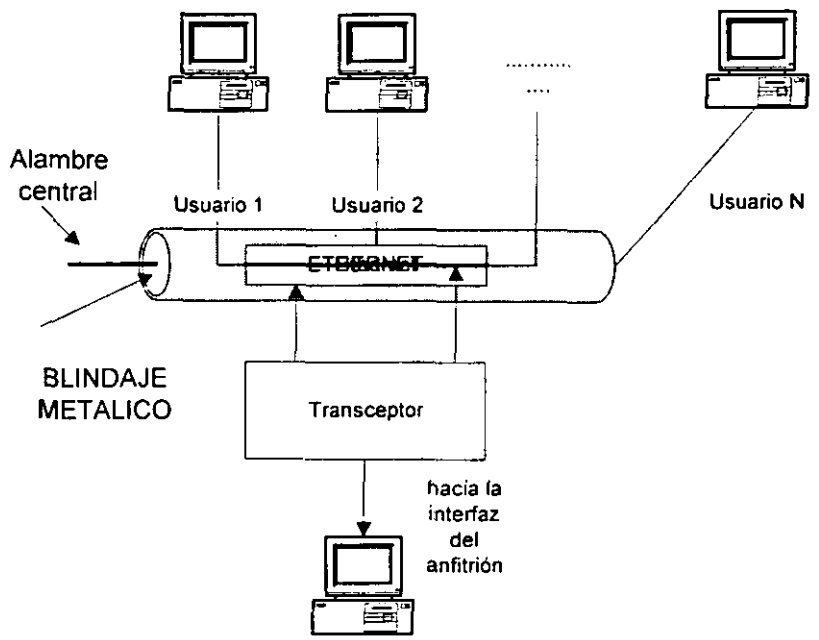


Figura 2.3 El cable Ethernet y disposición de las máquinas

2.5.1 Propiedades de una red Ethernet

La red Ethernet es una tecnología de bus de difusión[2] de 10 Mps que se conoce como " entrega con el mejor esfuerzo" y un control de acceso distribuido. Las redes Ethernet cuentan con un mecanismo llamado entrega con el mejor esfuerzo debido a que el hardware no proporciona información al emisor acerca de sí el paquete ha sido recibido (no distingue las transmisiones-transfiere todos los paquetes del cable a la interfaz anfitrión, la cual selecciona los paquetes que la computadora debe recibir y filtra todos los demás); ej. Si la máquina de destino es apagada los paquetes enviados se perderán y el emisor no será notificado. El control de acceso en las redes Ethernet es distribuido, porque a diferencia de algunas tecnologías de red, Ethernet no tiene una autoridad central para garantizar el acceso; este esquema es conocido como Carrier Sense multiple access con collision detect (CSMA/CD). Es un CSMA debido a que varias maquinas pueden accesar la red Ethernet de manera simultanea y cada maquina determina sí el cable Ether esta disponible; y sí esta presente una onda portadora. Cuando un interfaz anfitrión tiene un paquete para transmitir verifica el cable Ether para comprobar si el mensaje sé esta transmitiendo.

Cuando no se comprueba la presencia de una transmisión, la interfaz de anfitrión comienza a transmitir; cada transmisión esta limitada en duración (dado que hay un tamaño máximo para los paquetes). Además, el hardware debe respetar un tiempo mínimo de inactividad entre transmisiones, esto significa que no se dará el caso de que un par de computadoras que se comuniquen puedan utilizar la red sin que otras máquinas tengan la oportunidad de accesarla.

Recuperación y detección de colisiones

Cuando un transceptor comienza a transmitir, la señal no alcanza todas las partes de la red de manera simultanea. En lugar de ello, la señal viaja a lo largo del cable a una velocidad aproximada al 80 % de la velocidad de la luz. De esta forma, es posible que dos tranceptores perciban que la red esta desocupada y comiencen a transmitir en forma simultanea. Cuando las dos señales eléctricas se cruzan, se produce una perturbación y ninguna de las dos señales será significativa. Este tipo de incidentes se conocen como colisiones.

El manejo de las colisiones en Ethernet se resuelve de la siguiente manera; cada transceptor monitorea el cable mientras esta transmitiendo para explorar si hay laguna señal eléctrica exterior que interfiera con su transmisión. Técnicamente, el monitoreo se conoce como detección de colisiones (CD) esto hace de Ethernet una red CSMA/CD. Cuando se detecta una colisión, la interfaz de anfitrión aborta la transmisión y espera que la actividad disminuya, luego intenta de nuevo transmitir se debe tener mucho cuidado pues de otra forma la red podría caer en una situación en la que todos los tranceptores se ocuparían de intentar transmitir y todas las transmisiones producirían colisiones para ayudara evitar este tipo de situaciones las redes Ethernet utilizan un procedimiento de retroceso exponencial binario mediante el cual e el emisor espera un lapso de tiempo aleatorio, después de la primera colisión esperara el doble de tiempo para intentar transmitir de nuevo si de nuevo a produce una colisión esperar cuatro veces el lapso de tiempo inicial antes de hacer un tercer intento y así sucesivamente. El retroceso exponencial evita que se pueda producir un congestionamiento intenso, cuando estaciones diferentes tratan de transmitir en forma simultanea.

Capacidad de las redes Ethernet

El estándar Ethernet se define en 10Mps, lo cual significa que los datos pueden transmitirse por el cable a razón de 10 millones de bits por segundo; sin embargo esta no es la velocidad a la que transmiten las computadoras aunque es posible, debemos considerar la velocidad de red como una

[2] Bus de difusión porque todos los tranceptores reciben todas las transmisiones

medida de la capacidad del tráfico total en la red. Un ancho de banda alto hace posible transferir cargas de trafico pesadas, mientras que un ancho de banda bajo significa que la carretera no puede transporta mucho trafico. Una red Ethernet puede soportar unas cuantas computadoras con carga pesada o muchas computadoras con carga ligera.

2.5.2 Direccionamiento de Ethernet

Las redes Ethernet definen un esquema de direccionamiento de 48 bits. Cada computadora conectada a una red Ethernet es asignada a un número único de 48 bits conocido como dirección Ethernet. Para asignar una dirección, los fabricantes de hardware de Ethernet adquieren bloques de direcciones Ethernet [3] y las asigna en secuencia conforme fabrican el hardware de interfaz Ethernet. Generalmente las direcciones Ethernet se fijan en las máquinas en el hardware de interfaz de anfitrión de forma que se puedan leer; Ethernet se da en dispositivos de hardware, a esto se le llama a veces direccionamiento o direcciones físicas, de tal modo que, las direcciones físicas están asociadas con el hardware de interfaz Ethernet; cambiar el hardware de interfaz a una máquina nueva o reemplazar el hardware de interfaz que ha fallado provocará cambios en la dirección física de la máquina. Tiene la facilidad de que conociendo la dirección física Ethernet se pueden hacer cambios con facilidad porque los niveles superiores del software de red están diseñados para adaptarse a estos cambios.

El hardware de interfaz anfitrión examina los paquetes y determina qué paquetes deben enviarse al anfitrión. La interfaz de anfitrión utiliza el campo de dirección de destino de un paquete como filtro. La interfaz ignora los paquetes que están direccionados hacia otras máquinas y selecciona sólo los paquetes direccionados hacia el anfitrión. El mecanismo de direccionamiento y filtrado de hardware en necesario para prevenir que una computadora s ea abrumada con la entrada de datos.

Una dirección Ethernet de 48 bits puede hacer más que especificar una sola computadora destino y puede ser de alguno de los tres tipos siguientes:

- La dirección física de una interfaz de red (dirección de unidifusión)
- Dirección de publidifusión de la red
- Una dirección de multidifusión.

La dirección de difusión se reserva para envíos simultáneos a todas las estaciones. Las direcciones de multidifusión proporcionan una forma limitada de difusión en la cual un subconjunto de computadoras en una red acuerda recibir una dirección de multidifusión dada. Cuando el sistema operativo comienza a trabajar, este inicia la interfaz Ethernet, haciendo que se reconozca a un conjunto de direcciones. La interfaz entonces examina el campo de direcciones de destino en cada paquete, pasado hacia el anfitrión sólo las transmisiones destinadas a una de las direcciones especificas.

2.5.3 Encapsulamiento De Datos En Un Paquete Ethernet

El contenido del paquete de Ethernet muestra información típica de control para el envío de un paquete en un medio de red.

- Preámbulo: 64 bits de 0s y 1s alternando, usado para sincronizar en el nodo receptor.
- Dirección Destino: Dirección Ethernet de 48 bits del nodo que recibirá el paquete.

[3] El IEEE maneja el espacio de direcciones Ethernet

- Dirección origen: dirección Ethernet del nodo que envía el paquete.
- Tipo de paquete: un entero de 16 bits que identifica el tipo de los datos que contiene el paquete, TCP/IP emplea este campo para distinguir entre los protocolos.
- Datos: Los datos que se transporta. El MTU (unidad máxima de transmisión) del medio es de 1500, que es la cantidad máxima de datos que pueden ser transportados por Ethernet.
- CRC: una verificación de los datos se calcula en 32 bits en función del contenido con el fin de detectar errores en la transmisión.

Preámbulo 64 bits	Dirección de Destino 48 bits	Dirección de Origen 48 bits	Datos de la trama (paquete)	Tipo de trama (datos) 368-12000 bits	CRC 32 bits
8 octetos	6 octetos	6 octetos	2 octetos	64-1500 octetos	4 octetos

Figura 2.4 Trama de Ethernet.

Dado que cada medio físico tiene su propio esquema de direccionamiento y formato de paquete, es difícil escribir un protocolo que sirva a cada tipo de hardware. Al manejar capas de protocolos, se resuelve este problema, asilando los específicos del medio y los detalles en las capas bajas. Esto permite a los protocolos superiores ver a las redes diversas inferiores como una sola red lógica grande.

Para comunicar al nivel de red lógica en vez del físico, se requiere un esquema independiente del hardware para direccionar a los nodos, para esto sirve el direccionamiento Internet o Interred en TCP/IP.

2.6 Direccionamiento

Toda comunicación ocurre en el ámbito físico o de hardware; un dispositivo transmite bits a otra a través de un medio de comunicación. Cada medio es diferente y tiene su propio esquema de direccionamiento de los nodos que se conectan. Las direcciones físicas se pueden dividir en dos:

- Fijas, grandes y únicos
- Variables, pequeños y programables.

El primero en le caso de Ethernet, que emplea 48 bits (6 bytes) de direccionamiento. La dirección de Ethernet es única en el ámbito mundial.

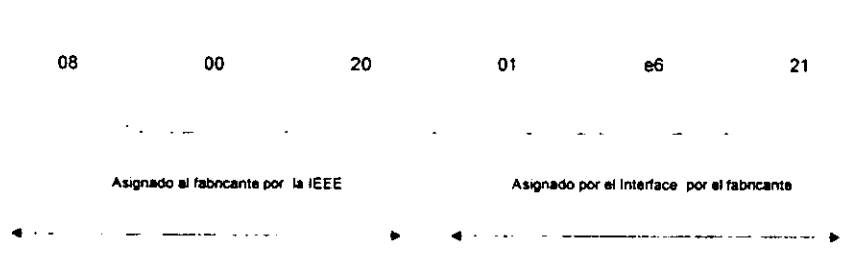


Figura 2.5 Direcciones físicas.

El segundo es el caso de algunos ruteadores o equipos dedicados que es único localmente, pero no en el ámbito mundial.

El encapsulamiento de datos es el proceso de agregar datos de control necesarios para enviar los datos a su destino. Generalmente, los datos son encapsulados en un paquete, con información de direcciones agregadas en forma de encabezados (headers) y colas (trailers). Los encabezados y colas pueden ser considerados como un sobre. Ellos encierran a los datos (carta) y contiene información de direccionamiento y las instrucciones de envío, en la cual la interface de red (cartero) usa para entregar.

Los protocolos que más adelante se verán, usan las técnicas de encapsulamiento para agregar información específica del protocolo a los datos para su interpretación en el destino.

2.6.1 Dirección física.

Cada dispositivo en una red que se comunica con otros tiene una dirección física única, aveces llamada dirección de hardware. En cualquier red dada, solo hay una ocurrencia de cada dirección; de otra manera, el servidor de nombre no tiene forma de identificar sin ambigüedad al dispositivo que es su meta. Para el hardware, las direcciones por lo general se codifican en una tarjeta de interfaz de red, establecidas ya sea por medio de interruptores o con software. Con respecto al modelo OSI, la dirección se localiza en la capa física.

En la capa física se ejecuta el análisis de cada datagrama que llega (o unidades de datos de protocolo). Si la dirección del receptor concuerda con la dirección física del dispositivo, el datagrama puede pasarse hacia arriba de la s capas. Si las direcciones no concuerdan, el datagrama se ignora. Mantener este análisis en la capan inferior del modelo OSI previene demoras innecesarias, debido a que de otra manera el datagrama tendría que pasarse hacia arriba a las otras capas para su análisis.

La longitud de la dirección física varía, dependiendo del sistema de la red, pero Ethernet y varias otras usan 48 bits en cada dirección. Para que ocurra la comunicación se requieren dos direcciones una para cada uno de los dispositivos transmisor y receptor.

El IEEE ahora está manejando la tarea de asignar direcciones físicas universales para subredes. Para cada subred, el IEEE asigna un identificador único de organización (Organization Unique Identifier, OUI), que tiene una longitud de 24 bits, permitiendo a la organización asignar los otros 24 bits de cualquier manera que desee. (En realidad dos de los 24 bits asignados como un OUI son bits de control, así, que sólo 22 bits identifican a la subred). Debido a que esto proporciona 2^{22} combinaciones.

La siguiente figura representa el formato de los OUI, el bit menos significativo de la dirección (el número de bit más bajo) es el bit de dirección individual o de grupo. Si el bit se fija en 0, la dirección se refiere a una dirección individual; si se fija en 1 significa que el resto de campo de dirección identifica una dirección de grupo que necesita mayor definición. Si el OUI entero se fija en 1, la dirección tiene un significado especial de que todas la s estaciones en la red se suponen como el destino.

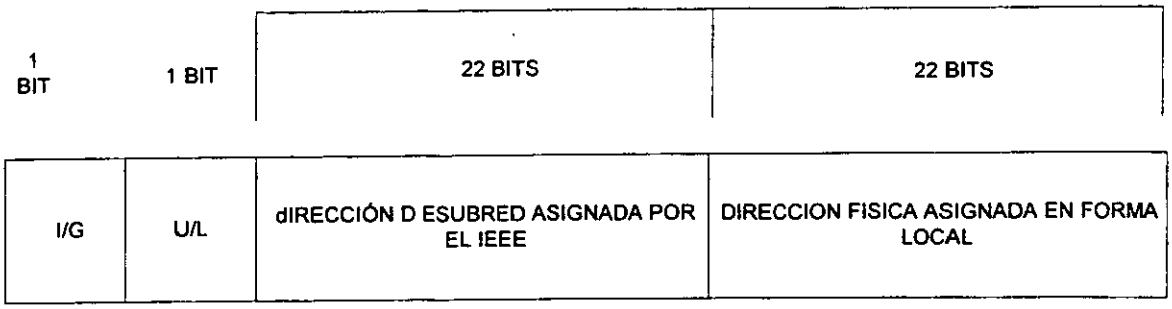


Figura 2.6 Formato de los OUI

2.6.2 Dirección lógica (IP)

Construcción lógica en software.

Dada la independencia del hardware se diseña el esquema según necesidades.

Dirección de 32 bits (4 bytes).

Selección para buscar eficiencia en los algoritmos de ruteo.

Se representan por una secuencia de 4 números decimales separados por puntos (ej.132.248.23.1)

La dirección Internet identifica únicamente a una interfaz de nodo de la red.

Un nodo o host con más de una interfaz de red requiere de igual número de direcciones Internet.

Las direcciones de red son análogas a las direcciones postales en el sentido de que le dicen aun sistema a donde enviar el datagrama. Tres términos usados comúnmente en el Internet se relacionan con el direccionamiento: nombre, dirección y ruta.

El nombre es la identificación especifica de una máquina, un usuario o una aplicación. Por lo general es único y proporciona un objetivo absoluto para el datagrama. Una dirección de manera característica identifica dónde se localiza el objetivo, por lo general su ubicación física o lógica en una red.

Una ruta le dice al sistema cómo hacer llegar un datagrama a la dirección. A menudo se usa el nombre de receptor, ya sea especificando un nombre de usuario o un nombre de máquina y una aplicación hace lo mismo para uno pero en forma transparente.

Con el nombre, un paquete de software de red llamado *servidor de nombre* intenta resolver la dirección y la ruta, haciendo que ese aspecto carezca de importancia para uno. Cuando se envía correo electrónico, tan solo se indica el nombre del receptor, confiando en que el servidor de nombre averiguará como hacer que el mensaje de correo llegue a él.

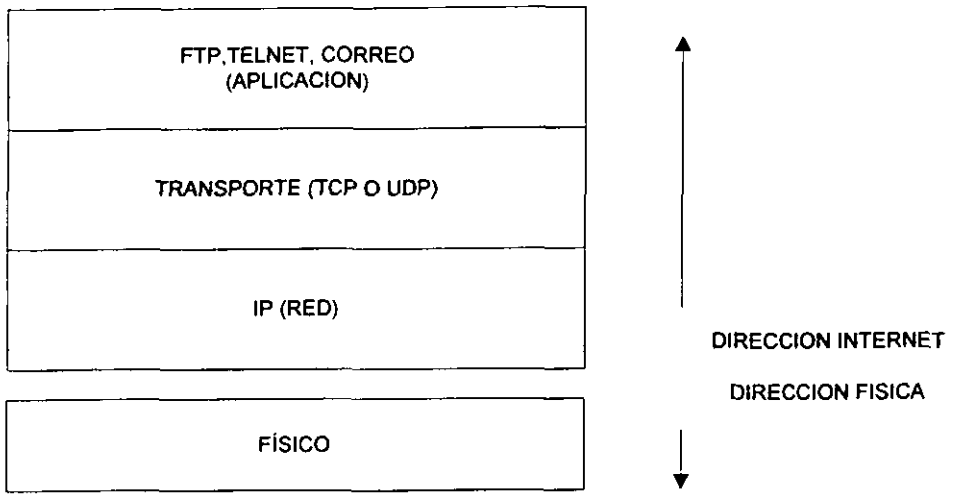


Figura 2.7 Direccionamiento Internet

Usar un servidor de nombre tiene como ventaja principal además de hacer que carezca de importancia para el usuario final el direccionamiento y enrutamiento: da al administrador del sistema o red plena libertad para cambia la red como se requiera, sin tener que informarle a cada máquina de los usuarios de cualquier cambio. En tanto que una aplicación pueda tener acceso al servidor de nombre, cualquier cambio en el enrutamiento puede ignorarlo la aplicación y los usuarios.

2.6.3 Direccionamiento de subredes.

En una red única son necesarias varias partes de información para asegurar el envío correcto de los datos. Los componentes primarios son la dirección física y la vinculación de datos.

Clases de direcciones IP

La dirección IP no identifica por sí misma a una máquina, sino más bien la conexión de una máquina con su red. Las direcciones IP se clasifican por sus formatos y cuentan con las siguientes características:

- ✓ Se dividen en cinco clases
- ✓ El valor de los bits de mayor valor de la dirección determina la clase.
- ✓ La clase determina el tamaño de la red (en número de nodos).
- ✓ Seleccionado para buscar eficiencia en los algoritmos de ruteo.
- ✓ La dirección Internet indica a la red en que se conecta el nodo y únicamente identifica la nodo sobre la red.
- ✓ La dirección Internet se puede pensar como un pareja de un identificador de red y un identificador de nodo (idred, idnodo).

Están permitidos cuatro formatos: Clase A, Clase B, Clase C y Clase D. Los primeros bits de la dirección especifican el formato del resto del campo de direcciones en relación con los subcampos de red y máquina. La dirección de la máquina se denomina también dirección local (o campo **REST**).

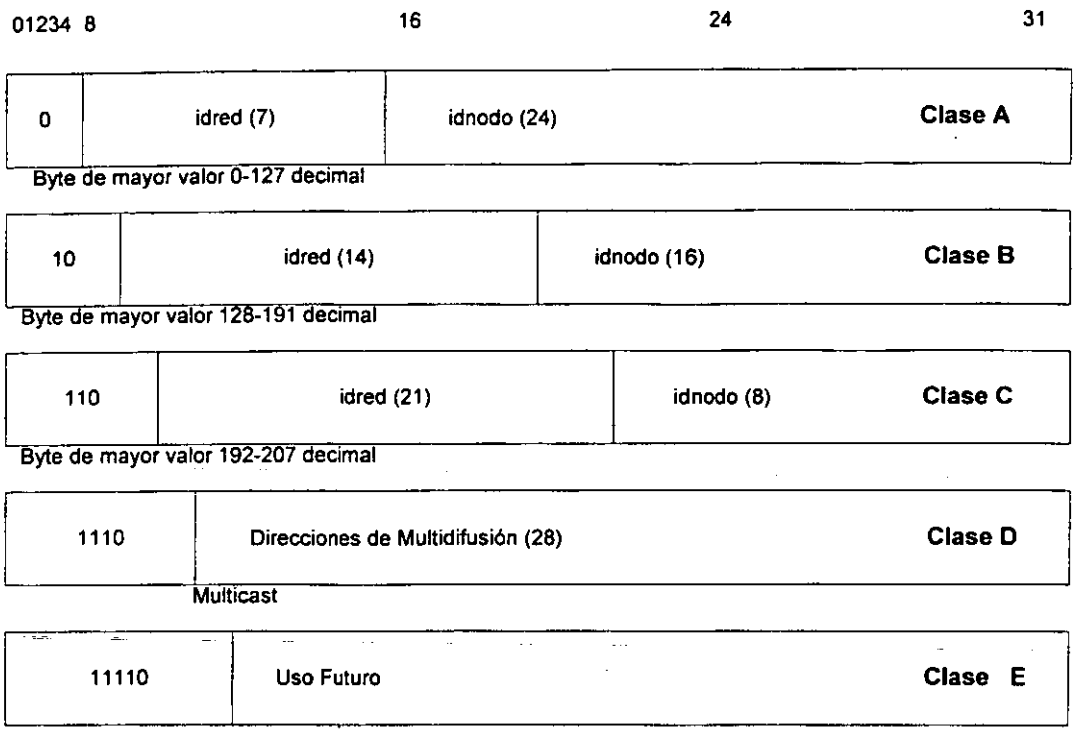


Figura 2.8 Clases de direcciones Internet

Las direcciones A se utilizan para redes con un gran número de ordenadores conectados. El campo identificado de ordenador tiene 24 bits, se podrían identificar, por tanto, hasta 2^{24} ordenadores (cada red puede contener 16,777,215 nodos). El identificador de red puede ocupar siete bits, con lo que se podrían identificar hasta 127 redes (con los valores de 1 a 27). Esta clase A se distingue por tener 0 en el primer bit del primer byte, identifica al numero de red (idred), los tres bytes siguientes identifican la interfaz del nodo (idnodo).

Las direcciones clase B se utilizan para redes de tamaño intermedio. El identificador de red utiliza 14 bits y el identificador de ordenador 16 bits. Los 2 primeros identifican al número de red (idred). Los 2 bytes siguientes identifican al nodo (idnodo). La clase B se distingue por tener 10 en los dos primeros bits, del primer byte (numerado de 128.1 al 191.254), cada red puede contener 65535 nodos.

Las direcciones clase C contienen menos de 256 ordenadores (2^8). Los 3 primeros bytes identifican al número de red (idred), el identificador de red utiliza 21 bits y el byte siguiente identifica al nodo (idnodo). La clase C se distingue por tener 110 en los tres primeros bits del primer byte (numerado del 192.0.1 al 223.255.254). Cada red puede contener un máximo de 254 nodos.

Las direcciones de clase D se reservan para multidifusión (multicast), que es una forma de difusión en un área limitada. El multicast permite la transmisión de datagramas IP a un conjunto de nodos. La clase D se distingue por tener 1110 en los 3 primeros bits del primer byte.

La clase E se distingue por tener 11110 en los 3 primeros bits del primer byte.

Direcciones Internet especiales (reservados)	
127.idnodo llamado "localhost" o "loopback"	
Idred.255 dirección del broadcast	
Clase A	89.255.255.255
Clase B	128.62.255.255
Clase C	192.129.32.255
No se usa 0 y 255 en idred y idnodo	

Tabla 2.2 Clases de direcciones IP

El 127.idnodo es conocido como "localhost", definido en cada nodo para indicar un bucle interno. Los datos no se envían por la red, pero si bajan por la pila de protocolos y sube de nuevo. Toda la red 127 es reservada y generalmente es 127.0.0.1 ó 127.1.

La Idred.255 es una dirección Internet que contiene a la parte de idnodo en 1s es llamado broadcast, los datos con esta dirección se envían a todos los nodos sobre la red.
La idred.0 en algunas implantaciones viejas, el 0 en todos los bits de idnodo significaba el broadcast, hoy en día esto ya no sucede, pero se reserva por seguridad.

Mapeo de direcciones

El mapeo es necesario porque el medio físico requiere direcciones físicas, mientras que los protocolos superiores requieren direcciones lógicas. Muchos archivos están para hacer la vida más fácil en el manejo de los protocolos, aplicaciones y personas. Se presentan dos tipos:

- Mapeo de dirección física a dirección Internet
- Mapeo de dirección Internet a nombre de nodo

La idea principal es el mapeo de una dirección física a una dirección Internet y después una dirección Internet a un nombre de nodo. Las direcciones Internet son difíciles de recordar por eso si nosotros trabajamos con nombre, hace más fácil nuestro direccionamiento. En este ejemplo se muestra que Gabriela corresponde a una dirección Internet 132.247.2.3 y que esta dirección corresponde a la dirección física de 08:00:c0:12:34:56.

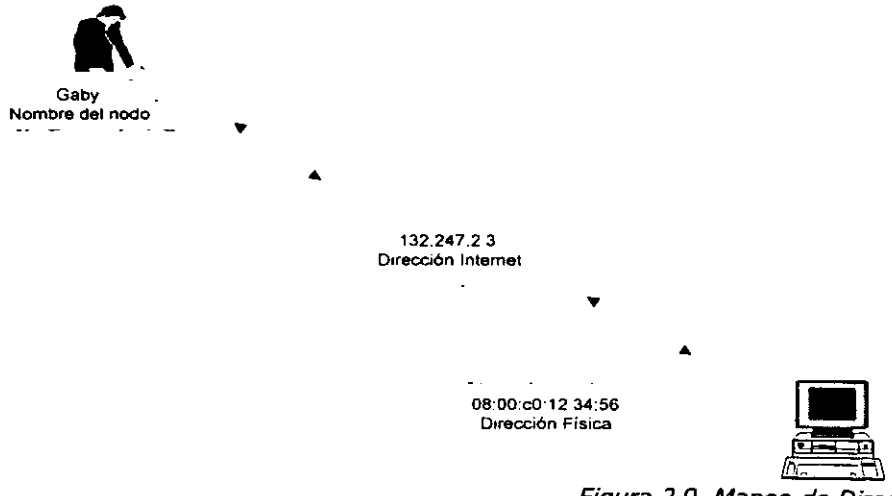


Figura 2.9 Mapeo de Direcciones

Si dos nodos están en la misma red, cada nodo tiene una dirección Internet que TCP/IP emplea para enviar paquetes. Cómo toda comunicación ocurre a nivel físico ¿cómo es que los nodos se comunican sin saber la dirección física del otro? Sencillamente no lo saben, la resolución de direcciones es un problema que requiere ser resuelto, antes que los protocolos de más alto nivel puedan comunicarse.

Existen 3 maneras de realizar esta tarea:

- Mapeo directo: se codifica directamente la dirección física con la dirección lógica. Este metido es directo; debe ser una red pequeña y direcciones localmente asignadas, su implementación es fácil de entender, pero no es flexible dado que las direcciones lógicas son dependientes de las direcciones físicas.

- Tabla estática: esta es una forma más flexible de resolver direcciones, se crea una tabla conteniendo pares de direcciones Internet con direcciones físicas, usualmente es un proceso manual.

- "Binding dinámico": con este método dejamos a la computadora trabajar. Es el más flexible y automático de los métodos; un protocolo de bajo nivel llamado ARP (Address Resolution Protocol) ha sido diseñado para relacionar direcciones físicas con direcciones Internet dinámicamente.

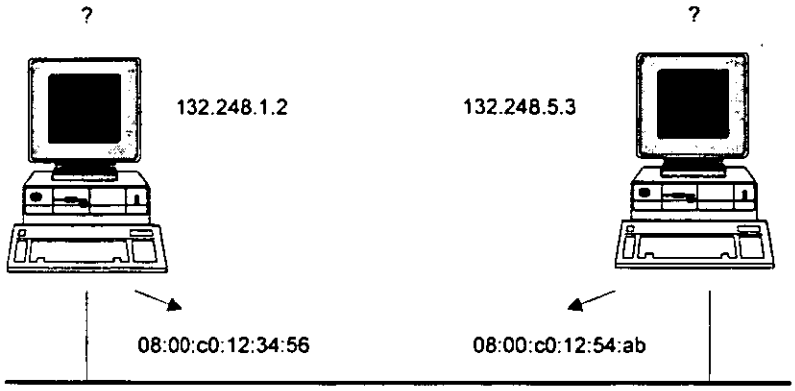


Figura 2.10 Mapeo de Dirección IP a Dirección Física

2.7 ARP (Protocolo de Resolución de direcciones)

El protocolo de Resolución de Direcciones (ARP) tiene el trabajo de convertir las direcciones IP a direcciones físicas (de red y locales) y, al hacerlo, elimina la necesidad de que las aplicaciones conozcan las direcciones físicas.
La idea básica es la siguiente:

Juan:" Oye, alguno conoce el teléfono de Pedro"
Pedro: " seguro, mi teléfono es 345-2345"

Se envía un broadcast pidiendo al dirección física de un nodo.
El destinatario Internet contesta indicando su dirección física.

En esencia, el ARP es una tabla con una lista de las direcciones IP y sus correspondientes direcciones físicas. La tabla se llama caché ARP; al disposición de un caché ARP se muestra en la

Tabla 2.3 . Cada fila corresponde a un dispositivo, con cuatro piezas de información para cada dispositivo:

	Indice FI	Dirección Física	Dirección IP	Tipo
Registro 1	El puerto físico (interfaz)			
Registro 2		la dirección física del dispositivo		
Registro 3			la dirección IP correspondiente a la dirección física	
Registro 4				el tipo de registro en él caché ARP

Tabla 2.3 de direcciones caché ARP

Cuándo un nodo desea, enviar un paquete a otro nodo, un paquete ARP es enviado a la red diciendo "tengo una dirección Internet xx.xx.xx.xx, ¿alguien puede dar la dirección física correspondiente?. El nodo destino lleva la información en el paquete y lo regresa. Ahora el nodo original tiene la dirección física de nodo con el que se quiere comunicar y puede enviar el paquete que originalmente comenzó a enviar.

Las solicitudes de ARP son broadcast, que cada vez que se realiza una comunicación, causarían una saturación del medio. Para eliminar estas ineficiencias, cada host se acuerda con quien se ha comunicado recientemente, haciendo un caché, y guardándolo en una tabla dinámica.

El tipo de mapeo es uno de cuatro valores posibles indicando el estado del registro en él caché ARP. Un valor de 2 significa que el registro es no válido; un valor de 3 significa que el mapeo es dinámico (el registro puede cambiar); un valor 4 significa estático (el registro no cambia), y un valor de 1 significa que no es ninguno de los anteriores.

Cuando el ARP recibe una dirección IP del dispositivo receptor, busca en él caché ARP para realizar una comparación. Si encuentra una igual, regresa la dirección física. Si él caché ARP no encuentra una igual para una dirección IP, envía un mensaje fuera de red. El mensaje, llamado solicitud ARP es una emisión que reciben todos los dispositivos en la red local (debe recordarse que una emisión sólo tiene unos en la dirección). La solicitud ARP contiene la dirección IP del dispositivo receptor pretendido. Si un dispositivo reconoce la dirección IP como perteneciente a éste, el dispositivo envía un mensaje de respuesta que contiene su dirección física de regresó a la máquina que generó la solicitud ARP, la cual coloca la información en su caché ARP para uso futuro. De esta manera, él caché ARP puede determinar la dirección física para cualquier máquina con base en su dirección IP.

Siempre que recibe una solicitud ARP, un caché ARP, éste usa la información de la solicitud para actualizar su propia tabla. Por tanto, el sistema puede acomodar las direcciones físicas cambiantes y las adiciones a la red de forma dinámica, sin tener que generar una solicitud ARP propia. Sin el uso de un caché ARP, todas las solicitudes y respuestas ARP generarían mucho tráfico en la red, el

cual tendría un impacto serio en el desempeño de la red. Algunos esquemas de red más sencillos no utilizan él caché y tan sólo usan mensajes de emisión cada vez; esto es factible sólo cuando el número de dispositivos es lo bastante bajo como para evitar problemas de tráfico en la red.

Cuando se envía una solicitud ARP se usan todos los campos en la disposición excepto la dirección del Hardware receptor, a la cual está tratando de identificar la solicitud; en una respuesta ARP, se usan todos los campos. La disposición de las solicitudes ARP se muestra a continuación

Tipo de hardware (16 bits)	
Tipo de protocolo (16 bits)	
Longitud de la dirección de hardware	Longitud de la dirección de protocolo
Dirección IP del receptor	Código de operación (16 bits)
Dirección de hardware Receptor	Dirección del hardware transmisor
Dirección IP del transmisor	
Dirección del hardware receptor	
Dirección IP del receptor	

Tabla 2.4 Disposición de la solicitud ARP y de la respuesta RARP

2.7.1 Disposición de los campos ARP

Esta disposición, la cual esta combinada con los protocolos del sistema de red en una unidad de datos de protocolo (PDU), tiene varios campos. Los campos y su propósito son los siguientes:

- Tipo de hardware: el tipo de interfaz del hardware (ej. Ethernet=1)
- Tipo de protocolo: el tipo de protocolo que está usando el dispositivo transmisor (ej. Dirección Internet IP=0800 (16))
- Longitud de dirección de hardware: la longitud de cada dirección de hardware en el datagrama, dado en bytes (ej. Ethernet=6)
- Longitud de dirección del protocolo: la longitud de la dirección de protocolo en el datagrama, dada en bytes (ej. Internet=4)
- Código de operación(Opcode): el Opcode indica si el datagrama es una solicitud ARP o una respuesta ARP. Si el datagrama es una solicitud, el valor se fija en 1. Si es una respuesta, el valor se fija en 2.
- Dirección de hardware transmisor: la dirección de hardware (dirección física) del dispositivo transmisor.
- Dirección IP del transmisor: la dirección IP (dirección lógica) del dispositivo transmisor.
- Dirección IP del receptor: la dirección IP del receptor (nodo destino)
- Dirección del hardware receptor: la dirección del hardware del dispositivo receptor (nodo destino).

Los dos primeros campos tienen valores ya establecidos los cuales se describen a continuación:

Campo de tipo hardware

El tipo de hardware identifica, el tipo de interfaz del hardware. Los valores válidos son los siguientes:

Tipo	Descripción
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET (Token Ring)
5	Chaos
6	IEEE 802.X
7	ARCnet

Campo de tipo de protocolo

El tipo de protocolo identifica el tipo que esta usando el dispositivo transmisor. Por lo general con TCP/IP estos protocolos son un EtherType, por lo cual los valores válidos son como siguen:

Decimal	Descripción
512	XEROX PUP
513	PUP Address Translation
1536	XEROX NS IDP
2048	Internet Protocol (IP)
2049	X.75
2050	NBS
2051	ECMA
2052	Chaosnet
2053	X.25 level 3
2054	Address Resolution Protocol (ARP)
2055	XNS
4096	Berkeley Trailer
21000	BBN Simnet
24577	DEC MOP Dump/Load
24578	DEC MOP Remote Console
24579	DEC DECnet Phase IV
24580	DEC LAT
24582	DEC
24583	DEC
32773	HP Probe
33784	Excelan
32821	Reverse ARP
32824	DEC LAN Bridge
32823	Apple Talk

Si el protocolo no es Ether Type se permiten otros valores.

2.7.2 Proxy ARP

Dos redes (o más) conectadas por un gateway pueden tener la misma dirección de red. El gateway tiene que determinar a cuál red corresponde la dirección física o la dirección IP. El gateway puede hacer eso con un ARP modificado, llamado Proxy ARP (en ocasiones llamado ARP Promiscuo). Un Proxy ARP crea un caché ARP consistente en registros de ambas redes, con el gateway capaz de transferir datagramas de una red a la otra. El gateway tiene que administrar las solicitudes y respuestas ARP que cruzan las dos redes.

Un defecto que presenta el sistema ARP es que si el dispositivo no conoce su propia dirección IP no hay manera de generar solicitudes y respuestas. La única dirección de la que se percata el dispositivo es la dirección física establecida, ya sea con interruptores en la interfaz de la red o por medio de software. El Protocolo Inverso de Definición Direcciones (Reverse Address Resolution Protocol, RARP), el cual funciona a la inversa que el ARP, enviando al dirección física afuera y esperando que regrese una dirección IP; proporciona una. La respuesta que contiene la dirección IP se envía mediante un servidor RARP, una máquina que puede administrar la información (muchas redes asignan más de un servidor RARP, tanto para extender la carga de procesamiento como para actuar como un respaldo en caso de problemas). Aunque el dispositivo origen envía el mensaje como una emisión, las reglas RARP estipulan que solo el servidor RARP puede generar una respuesta.

2.8 RARP (Protocolo de Resolución de Direcciones en Reversa)

Como ya antes mencionamos algunos equipos no conocen su dirección lógica cuando sé inicializan, por lo que requieren solicitar a un servidor en la red su dirección lógica, en base de su dirección física. Un paquete RARP es enviado a la red diciendo "tengo una dirección física XX.XX.XX.XX.XX.XX, ¿Alguien puede dar la dirección lógica correspondiente?". El nodo destino llena la información en el paquete y lo regresa.

Cuando el sistema recibe su dirección lógica, lo almacena en memoria, RARP no se emplea de nuevo; solamente en la inicialización del equipo.

La idea básica en la Resolución de direcciones por RARP es:

Juan: "Oye, alguien se acuerda de mi teléfono"
Pedro: "Seguro, tu teléfono es 345-2345"

Se envía un broadcast pidiendo la dirección lógica del mismo nodo en la base de la dirección física.

Algún nodo del servidor (con el programa de direcciones) contesta la solicitud.

Al igual que un mensaje ARP, un mensaje RARP se envía de una máquina a otra, encapsulado en la porción de datos de una trama de red. Por ejemplo, una trama Ethernet que transporta una solicitud RARP tiene el preámbulo usual, las direcciones Ethernet tanto fuente destino y campos de tipo paquete al comienzo de la trama. El tipo de trama contiene el valor 8035_{16} para identificar que el contenido de la trama contiene un mensaje RARP. La porción de datos de la trama contiene el mensaje RARP de 28 octetos. El que envía transmite por difusión una solicitud RARP especificada como máquina transmisora y receptora, y proporciona su dirección física de red en el campo de dirección de hardware objetivo. Todas las máquinas en la red reciben la solicitud, pero solo las autorizadas para proporcionar el servicio RARP la procesan y envían la respuesta; dichas máquinas se conocen de manera informal como servidores RARP. Una vez llenado el campo de dirección de protocolo objetivo, los servidores contestan las solicitudes, cambian el tipo de

mensaje de solicitud a respuesta y envían está de vuelta directamente a la máquina que la solicito. La máquina original recibe respuesta de todos los servidores RARP, aunque sólo se necesite una contestación.

En general RARP se utiliza solo en redes de área local, como Ethernet, en las que la probabilidad de falla es muy baja. La principal ventaja de que se tengan funcionando varias máquinas como servidores RARP es que se obtiene un sistema más confiable.

2.9 IP Datagrama del Protocolo de Internet

El **datagrama** es la unidad de transferencia usada por el IP, también conocido como datagrama Internet o IP. Las especificaciones que definen al IP tienen encabezados y colas en términos de palabras, donde una palabra es de 32 bits (algunos sistemas utilizan hasta de 64 bits).

2.9.1 Encabezado del IP

El encabezado IP tiene una longitud de seis palabras de 32 bits (24 bytes) cuando en el encabezado se incluyen todos los campos opcionales; y el más corto en IP usa cinco palabras (20 bytes). Para entender todos los campos en el encabezado es útil recordar que el IP depende del hardware, pero debe considerar todas las versiones de software de IP que pueda encontrar. En la siguiente figura 2.11 se muestra de manera esquemática el diseño del encabezado IP.

<table>
<tr><td>Versión</td><td>Longitud</td><td>Tipo de servicio</td><td colspan="4">Longitud del paquete</td></tr>
<tr><td colspan="3">Identificación</td><td></td><td>DM</td><td>MF</td><td>Compensasión de fragmentos</td></tr>
<tr><td colspan="2">TTL</td><td>Transporte</td><td colspan="4">Suma de verificación del encabezado</td></tr>
<tr><td colspan="7">Dirección Transmisora</td></tr>
<tr><td colspan="7">Dirección de Destino</td></tr>
<tr><td colspan="5">Opciones</td><td colspan="2">Relleno</td></tr>
</table>

Figura 2.11 Diseño del Datagrama IP

2.9.2 Descripción de los campos en el datagrama IP

Número de versión

Es un campo de 4 bits que contiene le número de versión IP qu8e esta usando el software de protocolo. El número de versión se necesita para que el software receptor IP sepa como descifrar el resto del encabezado, el cual cambia con cada publicación nueva de las normas IP, en la actualidad la mayoría están utilizando la versión 4 (la mayor parte de Internet y LAN's no soportan al IP versión 6).

Parte de la definición del protocolo estipula que el software receptor primero debe verificar él numero de la aversión de los datagramas que llegan, antes de proceder a analizar el resto del encabezado y los datos encapsulados, si el software no puede manejar la versión usada para crear el datagrama, la capa IP de la máquina receptora rechaza el datagrama e ignora el contenido por completo.

Longitud del encabezado

Este campo de cuatro bits refleja la longitud total del encabezado IP creado por la máquina transmisora; se especifica en palabras de 32 bits (el encabezado más corto es de cinco palabras), pero el uso de campos opcionales puede incrementar el tamaño del encabezado hasta su máximo de seis palabras (24 bytes)

Para descifrar de manera apropiada el encabezado, el IP debe saber donde termina el encabezado y comienzan los datos, razón por la cual se incluye este campo; la longitud del encabezado se usa para calcular la compensación desde el inicio del encabezado IP para dar el inicio del bloque de datos.

Tipo de servicio

El campo de tipo de servicio de 8 bits (1 byte) instruye al IP acerca de cómo procesar el datagrama de manera apropiada. Los 8 bits del campo se leen y asignan en el campo de tipo de servicio dentro del encabezado IP mostrado en la figura anterior. Los primeros 3 bits indican la procedencia del datagrama, con un valor de 0 (normal) a 7 (control de red). Entre más alto es el número, más importante el datagrama, de tal forma que el datagrama sé enrutará más rápido hacia su destino.

Los siguientes tres bits son banderas de 1 bit que controlan la demora, el paso a través y la confiabilidad del datagrama, si el bit fija en 0, el parámetro es normal. Un bit fijado en 1 implica una demora lenta, un paso a través alto y una confiabilidad alta para las banderas respectivas. Los últimos dos bits del campo no se utilizan.

La mayoría de las veces; los valores de los bits en el campo del tipo de servicio se fijan en 0, debido a que las diferencias en la precedencia, la demora, el paso a través y la confiabilidad entre máquinas son casi inexistentes, a menos que se haya establecido una red especial. Aunque estas banderas deberían ser útiles para establecer el mejor método de enrutamiento para un datagrama.

Longitud del datagrama (longitud del paquete)

Este campo da la longitud total del datagrama, incluyendo el encabezado en bytes. La longitud de datos misma puede calcularse, restándole a este valor la longitud del encabezado; el tamaño del campo de longitud del datagrama es de 16 bits, de aquí la longitud máxima de 65,535 bytes de un datagrama incluyendo el encabezado. Este campo se usa para determinar el valor de la longitud que se va a pasar al protocolo de transporte para establecer la longitud total del marco.

Identificación

Este campo contiene un número que es un identificador único creado por el nodo transmisor. Este numero se requiere cuando sé reensamblan mensajes fragmentados, asegurando que los fragmentos de un mensaje no estén entremezclados con otros. A cada arte de datos recibida por la capa IP de una capa de protocolo más alta, cuando legan los datos s ele asignan uno de estos números de identificación. Si un datagrama esta fragmentado tiene le mismo número de identificación.

Banderas

El campo de banderas es un campo de tres bits, el primer bit de los cuales no se usa. Los dos bits restantes están dedicados a banderas llamadas DF (Don't fragment) y MF (More Fragments), los cuales controlan el manejo de los datagrama cuando la fragmentación es conveniente.

Si la bandera DF se fija en 1, bajo ninguna circunstancia puede fragmentarse el datagrama. Si el software de la capa IP actual no puede enviar el datagrama a otra máquina sin fragmentarlo y este bit, esta fijado en 1, el datagrama se desecha y se envía un mensaje de error de regreso al dispositivo transmisor.

Si la bandera MF se fija en 1, al datagrama actual le siguen más paquetes, los cuales deben reensamblarse para volver a crear el mensaje completo. El último fragmento que se envía como parte de un mensaje más grande tiene su bandera MF fijada en 0, de modo que el dispositivo receptor sabe cuando ya no esperar mas datagrama. Debido a que el orden de llegada de los fragmentos podría no corresponder al orden en el que le fueron enviados, la bandera FM se usa junto con el campo compensación de fragmentos (el campo siguiente en él encabezado IP) para indicar a la máquina receptora la extensión total del mensaje.

Compensación de fragmentos

Si el bit d él abandera MF (mas fragmentos) se fija en 1 (indicando fragmentación de un datagrama más grande), el de compensación de fragmentos contiene la posición en el mensaje completo del submensaje contenido dentro del datagrama actual. Esto permite a IP reensamblar los paquetes fragmentados en le orden apropiado. Las compensaciones siempre se dan en relación con el comienzo del mensaje. Este es un campo de 13 bits, de modo que las compensaciones se calculan en unidades de 8 bits, correspondiendo a la longitud máxima del paquete de 65535 bytes. Si usa él numero de identificación para indicar a cual mensaje pertenece un datagrama recibido, la capa IP en una máquina receptora puede usarla compensación de fragmentos para reensamblar el mensaje completo.

Tiempo de vida TTL

Este fragmento de campo da el tiempo en segundos que un datagrama puede permanecer en la red antes de que se deseche. Esto lo establece el nodo transmisor cuando se ensambla el datagrama. Por lo general el campo TTL se fija en 15 o 30 segundos.

Las normas TCP/IP estipulan que el campo TTL debe disminuirse al menos en un segundo por cada nodo que procesa el paquete, aun si el tiempo de procesamiento es menor que un segundo. Además, cuando un datagrama lo recibe un gateway, el tiempo de llegada se agrega dé modo que si el datagrama debe esperar para ser procesado, este tiempo cuenta en contra de su TTL. Por consiguiente, si un gateway esta muy sobrecargado y no puede atender la datagrama en un lapso breve, el temporizador del TTL puede expirar mientras espera el procesamiento y abandona el datagrama.

Si el campo TTL alcanza 0, el datagrama debe desecharlo al nodo actual, pero se envía de regreso un mensaje a la máquina transmisora cuando el paquete es abandonado. La máquina transmisora puede volver a enviar el datagrama. Las reglas que gobiernan al campo TTL están diseñadas para impedir que los paquetes IP circulen interminablemente a través de las redes.
Protocolo de transporte

Este campo contiene el número de identificación del protocolo de transporte al que fue entregado el paquete. Los números los define el Centro de Información de Redes (Network Information Center), el cual regula Internet. En la actualidad existen alrededor de 50 protocolos que se han definido y a los que se les ha asignado un numero de protocolo de transporte. Los dos protocolos más importantes son el ICMP (Protocolo Internet de mensajes de Control), el cual tiene le numero 1 y el TCP, que tiene el número 6, los cuales son los más utilizados.

Suma de verificación de encabezado

El número en este campo en el encabezado IP es una suma de verificación para el campo de encabezado del protocolo, pero no para los campos de datos, para permitir un procesamiento más rápido. Debido a que el campo tiempo de vida TTL disminuye en cada nodo, la suma de verificación también cambia con cada máquina por la que pasa el datagrama. El algoritmo de la suma de verificación toma el complemento de unos de la suma de 16 bits de todas las palabras de 16 bits. Que solo contiene 0. Sin embargo, debido a que la suma de verificación de datos usadas tanto para el TCP como por él UD. cubren el paquete completo, estos tipos de errores por lo general pueden detectarse conforme el marco lo ensambla al transporte de red.

Dirección de envío y de destino

Este campo contiene las direcciones IP de 32 bits de los dispositivos de envío y de destino. Estos campos se establecen cuando se crea el datagrama y no se alteran durante el enrutamiento.

Opciones

Es un campo opcional compuesto de varios códigos de longitud variable, si se usa más de una opción en el datagrama, las opciones aparecen en forma consecutiva en el encabezado IP. Todas las opciones están controladas por un byte, que por lo general esta dividido en tres campos: una bandera de copia de 1 bit, una clase de opción de 2 bits y un numero de opción de 5 bits. La bandera de copia se usa para estipular como se maneja la opción cuando es necesitarla fragmentación en un gateway. Cuando el bit se fija en 0, la opción debe copiarse en le primer datagrama, peor no en los subsecuentes. Si el bit se fija en 1, la opción se copia en todo s los datagramas.

Hoy en día existen dos clases de opciones, cuando el valor es 0, la opción se aplica al datagrama o control de red. Un valor de 2 significa que la opción es para propósitos de eliminación de errores o administración. Los valores 1 y 3 no se usan, en el siguiente cuadro se dan valores soportados para la clase y número de opción.

Clase de Opción	Número de Opción	Descripción
0	0	Marca el final de la lista de opciones
0	1	Ninguna opción (usada para relleno)
0	2	Opciones de seguridad(propósitos militares
0	3	Enrutamiento de fuentes holgadas
0	7	Activa el registro de enrutamiento
0	9	Enrutamiento de fuente estricta
2	4	Activa el marcador de tiempo(agrega campos)

Tabla 2.5 Opciones del datagrama

De mayor interés son las opciones que permiten se registre el enrutamiento y el marcador de tiempo. Estas se usan para proporcionar un registro del paso de un datagrama a lo largo de la interred, lo cual puede ser útil para propósitos de diagnóstico. Ambas opciones agregan información a una lista contenida dentro del datagrama.

Existen dos tipos de enrutamiento indicados dentro del campo Opciones: holgado y estricto. El enrutamiento holgado proporciona una serie de direcciones IP que la máquina debe de atravesar, pero permite que se utilice cualquier ruta para llegar a cada una de estas direcciones (por lo general gateways). El enrutamiento estricto no permite desviaciones de la ruta especificada; si no puede seguir la ruta el datagrama es abandonado. El enrutamiento estricto se usa con frecuencia para probar rutas, pero rara vez para la transmisión de datagramas de usuario, debido a las probabilidades elevadas de que el datagrama se pierda o se abandone.

Relleno

El contenido del área de relleno depende de las opciones seleccionadas. Por lo general, el relleno se usa para asegurar que el encabezado del datagrama es un número redondeado de bytes.

2.9.3 Finalidad del datagrama

De acuerdo a la especificación del datagrama, podemos explicar cual es la ruta que sigue un datagrama característico. Cuando una aplicación debe enviar un datagrama por la red realiza unos cuantos pasos. Primero crea el datagrama IP dentro de la **longitud legal** estipulada por la realización IP local; la suma de verificación para los datos se calcula y luego, se crea el **encabezado IP**. A continuación, el primer paso (máquina) de la ruta hacia el destino debe determinarse para dirigir el datagrama en forma directa a la máquina de destino a través de la red local o hacia un **gateway**, si se va a usar la interred. Si el enrutamiento es importante, esta información se agrega al encabezado usando una opción. Por último el datagrama se pasa a la red para la manipulación del datagrama.

Conforme un datagrama pasa a lo largo de una interred, cada gateway realiza una serie de pruebas. Después de que la capa de red ha quitado su propio encabezado, la capa IP del gateway calcula la suma de verificación y comprueba la integridad del datagrama. Si la suma de verificación no concuerda, el datagrama se desecha y se regresa un mensaje de error al dispositivo transmisor. A continuación, **el campo TTL** se disminuye y verifica; si ha expirado el datagrama sé desecha y se envía un mensaje de regreso un mensaje error a la maquina transmisora. Después de determinar el siguiente salto de la ruta, ya sea por análisis de la dirección de destino o mediante una instrucción de enrutamiento especificada dentro del **campo de Opciones** del encabezado IP, el datagrama reconstruye con el valor TTL nuevo y una suma de verificación nueva.

Si la **fragmentación** es necesaria debido aun incremento en la longitud del datagrama o a una limitación en el software, el datagrama se divide y ensambla nuevos datagramas con la información de encabezado correcta. Si se requiere **un enrutamiento o un marcador de tiempo**, también se agrega; por ultimo el datagrama se pasa de vuelta a la capa de red.

Cuando finalmente se recibe el datagrama en el dispositivo de destino, el sistema realiza él calculo de la suma de verificación y, suponiendo que las dos sumas concuerdan, verifica para ver si hay otros fragmentos. Si se requieren más datagramas para reensamblar el mensaje completo, el sistema espera, mientras corre un temporizador para asegurar que los datagramas legan dentro de un tiempo razonable. Si todas las partes del mensaje más grande han llegado, pero el dispositivo no puede reensamblarlas antes de que el temporizador llegue a cero, el datagrama se desecha y regresa un mensaje de error al transmisor. Por ultimo el encabezado IP se retira, el mensaje

original se reconstruye si fue fragmentado y el mensaje se pasa hacia arriba a través de las capas hasta la aplicación de la capa superior (sí se requiere de una respuesta se genera y envía de regreso al dispositivo transmisor).

Cuando se añade información extra al datagrama para registro del enrutamiento o del marcador de tiempo, la longitud del datagrama puede aumentar. Parte de la fuerza del IP es manejar todas estas condiciones, por lo que casi cualquier problema tiene un sistema de resolución.

2.10 ICMP Protocolo de Internet mensajes de Error y de Control

En los sistemas que hemos explicado anteriormente, cada ruteador opera de manera autónoma, ruteando o entregando los datagramas que llegan sin coordinarse con el transmisor original. El sistema trabaja bien si todas la s máquinas funcionan de manera correcta y si están de acuerdo respecto a las rutas. Por desgracia, ningún sistema funciona bien todo el tiempo; además de las fallas en las líneas de comunicación y en los procesadores, el IP tiene fallas en la entrega de datagramas cuando la máquina de destino está desconectada temporal o permanentemente de la red, cuando el contador de vida expira, o cuando los ruteadores intermedios se congestionan tanto que no pueden procesar el tráfico entrante. La más importante diferencia entre tener una sola red implantada con hardware dedicado y tener una red implantada con software, es que en el primer caso, el diseñador puede añadir hardware especial para informar a los anfitriones conectados cuando surge un problema. En una red de redes, que no tiene un mecanismo de hardware como el anterior, un transmisor no puede indicar sí ocurrió una falla en la entrega, originada por un mal funcionamiento local o uno remoto. La depuración se vuelve difícil. El protocolo IP, por si mismo, no contiene nada para ayudar al transmisor a comprobar la conectividad ni para ayudarle a aprender sobre dichas fallas.

Para permitir que los ruteadores en una red de redes reporten los errores o proporcionen información sobre circunstancias inesperadas, los diseñadores agregaron a los protocolos TCP/IP un mensaje de protocolos de propósito especial. El mecanismo, conocido como Protocolo de Mensajes de Control Internet (ICMP), se considera como parte obligatoria del IP y se debe incluir en todas las implantaciones IP.

Al igual que el resto de tráfico, los mensajes ICMP viajan a través de la red de redes en la porción de datos de los datagramas IP. Sin embargo, el destino final de un mensaje ICMP no es un programa de aplicación ni un usuario en la máquina de destino, sino el software de Protocolo Internet en dicha máquina. Esto es, cuando llega un mensaje de error ICMP, el módulo de software ICMP lo maneja; por supuesto si el ICMP determina que un protocolo de un nivel más alto o un programa de aplicación causaron un problema, notificara al módulo apropiado.

En principio el ICMP estaba diseñado para permitir que los ruteadores reporten a los anfitriones las causas de los errores en la entrega, el ICMP no esta restringido solo a los ruteadores; aunque las normas y reglas limitan el uso de algunos mensajes ICMP, cualquier máquina puede enviar un mensaje ICMP a cualquier otra. Por lo tanto, un anfitrión puede utilizar el ICMP para comunicarse con un ruteador o con otro anfitrión. La mayor ventaja de permitir que los anfitriones utilicen el ICMP es que proporciona un solo mecanismo que se utiliza para todos los mensajes de información y de control.

Reporte de errores

Técnicamente el ICMP es un mecanismo de reporte de errores. Proporciona una forma para que los ruteadores que encuentren un error lo reporten a la fuente original. Aunque la especificación del protocolo subraya los usos deseables del ICMP y sugiere acciones posibles para responde a los

reportes de error, el ICMP no especifica del todo la acción que debe tomarse para cada posible error.

La mayor parte de los errores proviene de la fuente original, pero otros no, sin embargo debido a que el ICMP, reporta los problemas a la fuente original no se puede utilizar para informar los problemas a los ruteadores intermedios. Supongamos que un datagrama sigue un camino a través de una secuencia de ruteadores, R_1, R_2, . R_K. Si R_K tiene información de ruteo incorrecta y por error, rutea el datagrama hacia el ruteador R_E, éste no podrá utilizar el ICMP para reportar el error a R_K, el ICMP sólo puede enviar un informe a la fuente original. Sin embargo la fuente original no tiene ninguna responsabilidad sobre el problema ni sobre el control del ruteador que se equivocó, de hecho no es capaz de determinar que ruteador causo el problema.

El ICMP está restringido solo para comunicarse con la fuente original porque, un datagrama solo contiene campos que especifican la fuente original y el último destino; no contiene un registro completo de su viaje a través de la red de redes(a excepción de casos especiales en que se utiliza la opción de registro de ruta) y como los ruteadores pueden establecer y cambiar sus propias tablas de ruteo, no existe un conocimiento global de las rutas; por lo tanto cuando un datagrama llega a un ruteador, es imposible conocer el camino que siguió para llegar hasta ahí. Si el ruteador detecta un problema, no puede saber que grupo de máquinas intermedias procesó el datagrama, así que no puede informarles del problema; en vez de descartar discretamente el datagrama, el ruteador utiliza el ICMP para informar a la fuente original que ocurrió un problema, y confía en que los administradores del anfitrión cooperarán con los administradores de red para localizarlo y corregirlo.

2.10.1 Entrega de mensajes ICMP

Los mensajes ICMP requieren dos niveles de encapsulación, como se muestra en la figura 2.12; cada mensaje ICMP viaja a través de la red de redes en la porción de datos de un datagrama IP, el cual viaja a través de cada red física en la porción de datos de una trama. Los datagramas que llevan mensajes ICMP sé rutean exactamente como los que llevan información de usuario; no existe ni una confiabilidad ni una prioridad adicionales; por lo tanto, los mensajes de error se pueden descartar o perder. Hay una excepción en los procedimientos de manejo de errores si un datagrama IP que lleva un mensaje ICMP causa un error, es decir, especifica que los mensajes ICMP no se generan por errores resultantes de datagramas que llevan mensajes de error ICMP.

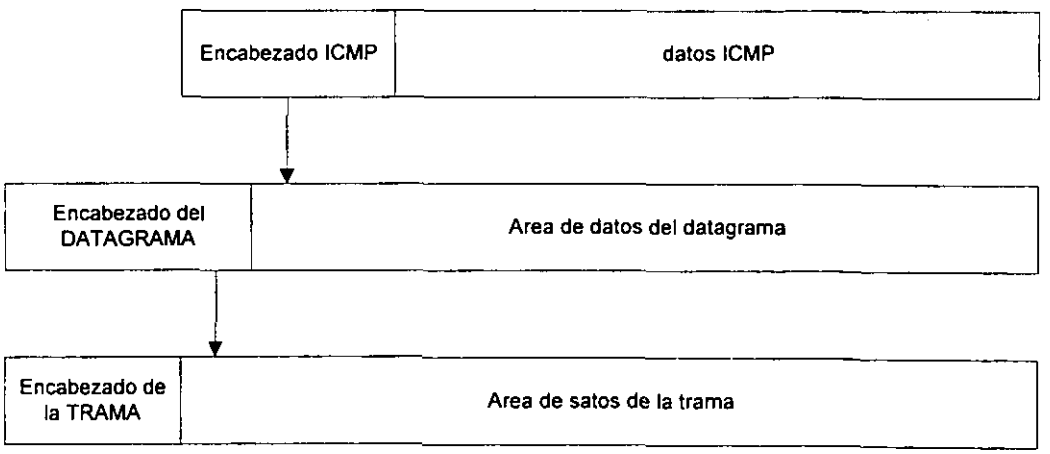


Figura 2.12 Los dos pasos de encapsulación del ICMP

Es importante tener en mente que aunque los mensajes ICMP se encapsulan y envían mediante el IP, el ICMP no se considera como un protocolo de nivel más alto sino como una parte obligatoria de IP. La razón de utilizar IP para entregar mensajes ICMP es que quizás necesiten viajar a través de muchas redes físicas para alcanzar su destino final; por lo tanto no se puede entregar solo por medio de transporte físico.

2.10.2 Formato de los mensajes ICMP

Aunque cada mensaje ICMP tiene su propio formato, todos comienzan con los mismos tres campos; un campo TYPE (tipo) de mensaje de 8 bits y números enteros, que identifican el mensaje; una campo CODE (código) de 8 bits, que proporciona más información sobre el tipo de mensaje, y un campo CHECKSUM (suma de verificación), de 16 bits (el ICMP utiliza el mismo algoritmo aditivo de suma de verificación que el IP, pero la suma de verificación del ICMP sólo abarca el mensaje ICMP). Además los mensajes ICMP que reportan errores siempre incluyen el encabezado y los primeros 64 bits de datos del datagrama que causó el problema.

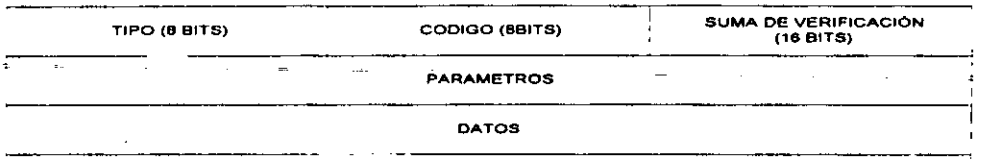


Figura 2.13 Formato de los mensajes ICMP

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

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

Campo de Tipo	Tipo de mensaje ICMP
0	Respuesta de eco
3	Destino inaccesible
4	Disminución de origen
5	redireccionar (cambiar una ruta)
8	Solicitud de eco
11	Tiempo excedido par aun datagrama
12	Problema de parámetros en un datagrama
13	Solicitud de timestamp
14	Respuesta de timestamp
15	Solicitud de información (obsoleto)
16	Respuesta de Información (obsoleto)
17	Solicitud de mascara de dirección
18	Respuesta de mascara de dirección

Tabla 2.6 Tipo de campos en los mensajesICMP

2.10.3 Pruebas de accesibilidad y destino (Ping)

Para que los administradores de red puedan identificar los problemas que ocurran en la red, los protocolos TCP/IP proporcionan funciones y herramientas de depuración; una de las más utilizadas incluye los mensajes ICMP de *echo request* (solicitud de eco) y *echo reply* (respuesta de eco). Un anfitrión o un ruteador envía un mensaje de ICMP de solicitud de eco hacia un destino específico.

Cualquier máquina que recibe una solicitud de eco, formula una respuesta y la regresa al transmisor original. La solicitud contiene un área opcional de datos: la respuesta contiene una copia de los datos enviados en la solicitud. La solicitud de eco y su respuesta asociada se pueden utilizar para comprobar si un destino es alcanzable y si responde. Debido a que la solicitud y respuesta viajan en datagramas IP, la recepción exitosa de una respuesta verifica que las piezas principales del transporte estén funcionando bien. Primero, el software IP en la computadora de origen debe rutear el datagrama; segundo los ruteadores intermedios entre el origen y el destino deben funcionar bien y rutear correctamente el datagrama; tercero, la máquina de destino debe estar funcionando (al menos debe responder a las interrupciones), y tanto el software ICMP como el IP deben estar funcionando; Por último, todos los ruteadores a lo largo del camino de regreso deben tener rutas correctas.

En muchos sistemas el comando que manda el usuario para enviar solicitudes de eco ICMP se conoce como **PING.** Las versiones más sofisticadas de ping envían una serie de solicitudes de eco ICMP, capturan las respuestas y proporcionan estadísticas sobre la pérdida de datagramas. Permiten que el usuario especifique la longitud de los datos que se envían así como el intervalo entre solicitudes. Las versiones menos sofisticadas sólo envían una solicitud de eco ICMP y esperan la respuesta.

Formato de los mensajes de solicitud de eco y respuesta.

El campo indicado como OPTIONAL DATA (datos opcionales) es un campo de longitud variable que contiene los datos que se regresarán al transmisor. Una respuesta de eco siempre regresa exactamente los mismos datos que se recibieron en la solicitud. Los campos IDENTIFIER (identificador) y SEQUENCE NUMBER (número de secuencia) los utiliza el transmisor para responder a las solicitudes. El valor del campo TYPE (tipo) especifica si el mensaje es una solicitud (8) o una respuesta (0).

Reporte de destinos no accesibles

Cuando un ruteador no puede direccionar o entregar un datagrama IP, envía un mensaje de destino *no accesible* a la fuente original, utilizando el formato que se muestra a continuación

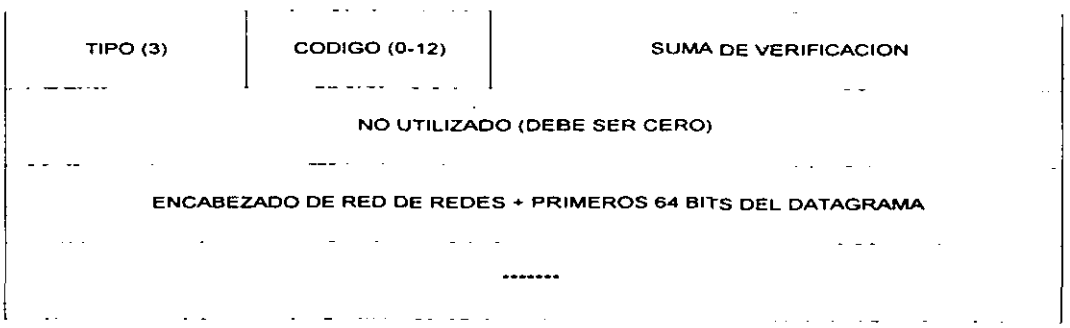


Figura 2.14 Formato del mensaje ICMP destino no accesible

El campo CODE (código) de un mensaje de destino no accesible contiene un número entero que describe con más detalle el problema. Los valores posibles son:

Valor del código	Significado
0	Red inaccesible
1	Anfitrión inaccesible
2	Protocolo inaccesible puerto inaccesible
3	Puerto inaccesible
4	Se necesitan fragmentación y configuración DF
5	Falla en la ruta de origen
6	Red de destino desconocida
7	Anfitrión de destino desconocido
8	Anfitrión de origen aislado
9	Comunicación con la red de destino administrativamente prohibida
10	Comunicación con el anfitrión de destino administrativamente prohibida
11	Red inaccesible por el tipo de servicio
12	Anfitrión inaccesible por el tipo de servicio

Tabla 2.7 Significado del código del campo CODE en ICMP

Aunque el IP es un mecanismo de entrega con el mejor esfuerzo, el descarte de datagramas no se debe tomar a la ligera. Siempre que un error evite que un ruteador direccione o entregue un datagrama, el ruteador envía al origen un mensaje de destino no accesible y luego salta (descarta) el datagrama. Los errores de red no accesible por lo general implican fallas en ele ruteo nota pie. Debido a que los mensajes ICMP contienen un prefijo del datagrama que causó el problema, la fuente sabrá exactamente que dirección no es accesible.

Los destinos pueden no ser accesibles ya sea porque el hardware esté temporalmente fuera de servicio, porque el transmisor haya especificado una dirección de destino no existente porque el ruteador no tenga una ruta para la red de destino. Notesé que aunque los ruteadores reportan las fallas que encuentran, quizás no tengan conocimiento de todas las fallas de entrega. Por ejemplo, si la máquina de destino se conecta a una red Ethernet, el hardware de red no proporcionara acuses de recibo; por lo tanto, un ruteador puede seguir enviando paquetes hacia un destino cuando éste se encuentre apagado, sin recibir ninguna indicación de que los paquetes no se están entregando.

El significado de los mensajes de protocolo y puerto no accesibles se aclarará cuando analicemos los protocolos de niveles superiores. La mayor parte de los mensajes restantes se explican por si mismos, si el datagrama contiene una opción de ruta de origen con una ruta incorrecta, activará un mensaje de falla en la ruta de origen. Si un ruteador necesita fragmentar un datagrama pero está activado el bit de "no fragmentar", el ruteador enviará un mensaje de necesidad de fragmentación hacia la fuente.

2.10.4 Control de Congestionamiento y de flujo de datagramas.

Debido a que el IP funciona sin conexión, un ruteador no puede reservar memoria o recursos de comunicación antes de recibir datagramas; los ruteadores se pueden saturar con el tráfico, condición conocida como congestionamiento. El congestionamiento puede ser por dos razones:

- Primero, una computadora de alta velocidad puede ser capaz de generar tráfico de forma más rápido de lo que una red lo puede transferir. Por ejemplo, imagínese una supercomputadora que genera tráfico para la red de redes. Los datagramas pueden necesitar pasar a través de una red de área amplia(Wan) más lenta, aunque la supercomputadora se conecte a una red de área local de alta velocidad. El congestionamiento ocurrirá en el ruteador que conecta a la LAN con la WAN, ya que los datagramas llegan más rápido de lo que se pueden enviar.

- Segundo, si muchas computadoras necesitan enviar datagramas al mismo tiempo a través de un solo ruteador, esté se puede congestionar, aunque ningún origen por sí mismo cause el problema.

Cuando los datagramas llegan demasiado rápido para que un ruteador los procese, los pone temporalmente en una cola de espera de memoria, pero si la memoria se satura en el ruteador descartar los demás datagramas que lleguen. Una máquina utiliza mensajes ICMP de distribución de tasa al origen (source quench) para reportar el congestionamiento a la fuente original.

Un mensaje de disminución de tasa al origen es una solicitud para que la fuente reduzca la velocidad de transmisión de datagramas. Por lo general, los ruteadores congestionados envían un mensaje de disminución de tasa al origen por cada datagrama que descartan. Los ruteadores también pueden utilizar técnicas más sofisticadas para el control de congestionamientos, algunos monitorean el tráfico entrante y reducen las fuentes que tienen las velocidades más altas de transmisión de datagramas. Otros intentan evitar los congestionamientos al enviar solicitudes de disminución cuando sus colas de espera crecen, pero antes de que se saturen.

No existe ningún mensaje ICMP para revertir el efecto de una disminución de tasa al origen; en vez de eso un anfitrión que reciba mensajes de disminución para un destino D, baja la velocidad de envío de datagramas hacia D, hasta que deja de recibir los mensajes de disminución de tasa al origen: luego aumenta de manera gradual la velocidad en tanto no reciba más solicitudes de disminución de tasa al origen.

Formato de disminución de tasa al origen

Además de los campos normales ICMP, como TYPE, CODE, CHECKSUM, y un campo no utilizado de 32 bits, los mensajes de disminución de tasa al origen tienen un campo que contienen un prefijo de datagrama, como sucede en la mayor parte de los mensajes ICMP que reportan un error, el campo antes mencionado contiene un prefijo del datagrama que activo la solicitud de disminución de origen.

Solicitudes para cambio de ruta desde los ruteadores.

Generalmente, las tablas de ruteo de una red de redes se mantienen sin cambios por grandes periodos de tiempo; los ruteadores intercambian en forma periódica información de ruteo para incorporar los cambios en la red y para mantener actualizadas sus rutas; por lo tanto, se asume que los ruteadores conocen rutas correctas; los anfitriones comienzan con información mínima de ruteo y aprenden nuevas rutas de los ruteadores.

Para ayudar a que sigan esta ruta y para evitar la duplicación de información de ruteo en el archivo de configuración de cada anfitrión, esta configuración especifica la menor información posible de ruteo necesaria para comunicarse (por ejemplo, la dirección de un solo ruteador); por lo tanto el anfitrión arranca con información mínima y confía en los ruteadores para actualizar su tabla de ruteo. En un caso especial, cuando un ruteador detecta un anfitrión que utiliza una ruta no óptima, le envía al anfitrión un mensaje ICMP llamado redireccionar (redirect), solicitándole que cambie sus rutas y el ruteador también direcciona al datagrama original hacia su destino.

La ventaja del esquema de redireccionamiento ICMP es la simplicidad: permite que un anfitrión inicie conociendo solamente un ruteador en la red local: El ruteador inicial genera mensajes de redireccionamiento siempre que un anfitrión envía un datagrama para el que existe una ruta mejor. La tabla de ruteo del anfitrión permanece reducida, y aun así, contiene rutas óptimas para todos los destinos en uso.

Además de los campos obligatorios, cada mensaje de redireccionamiento llamado ROUTER INTERNET ADDRESS (dirección de red de redes del ruteador) y un campo HEADER (encabezado).

El campo router Internet Address contiene la dirección de un ruteador que el anfitrión utilizará para alcanzar el destino mencionado en el encabezado del datagrama. El campo Internet header contiene el encabezado IP, más los siguientes 64 bits del datagrama que activó el mensaje. Por lo tanto, un anfitrión que recibe un redireccionamiento ICMP examina el prefijo del datagrama para determinar la dirección de destino El campo Code de un mensaje ICMP de redireccionamiento especifica con mayor detalle como interpretar la dirección de destino. Como regla general, los ruteadores envían solicitudes ICMP de redireccionamiento solo a los anfitriones y no a otros ruteadores.

Detección de rutas circulares o excesivamente largas

Debido a que los ruteadores en una red de redes computan un salto al siguiente ruteador, utilizando tablas locales, los errores en dichas tablas pueden producir un ciclo de ruteo para algún destino D. Un ciclo de ruteo puede consistir en muchos ruteadores, cada uno, ruteando al otro un datagrama para el destino D y hacia el siguiente ruteador dentro del ciclo. Si un datagrama entre un ciclo de ruteo, recorrerá indefinidamente y de manera circular todos los ruteadores. Como se menciono con anterioridad, para evitar que los datagramas circulen indefinidamente en una red de redes TCP/IP, cada datagrama IP contiene un contador de tiempo de vida, conocido como conteo de saltos. Un ruteador disminuye el contador de tiempo de vida siempre que procese el datagrama y lo descarta cuando el conteo llega a cero.

Siempre que un ruteador descarta un datagrama ya sea porque su conteo de saltos llega acero o porque ocurre una terminación de tiempo mientras espera fragmentos de un datagrama, envía un mensaje ICMP de tiempo excedido a la fuente del datagrama, utilizando el siguiente formato.

En el campo CODE se explica la naturaleza de la terminación de tiempo. El reensamblado de fragmentos se refiere a la tarea de recolectar todos los fragmentos de un datagrama. Cuando llega el primer fragmento de un datagrama, el anfitrión que lo recibe arranca un temporizador y considera como error que dicho temporizador expire antes de que lleguen todas las piezas del datagrama. El valor 1 para el campo Code se utiliza para informar dichos errores al transmisor, se envía un mensaje por cada error y el valor 0 indica el tiempo de vida excedido

Reporte de otros problemas

Cuando un ruteador o un anfitrión encuentran problemas que no se han cubierto con los mensajes ICMP de errores anteriores (un datagrama con un encabezado incorrecto), envía un mensaje de problema de parámetros a la fuente original. Una causa posible de dichos problemas ocurre cuando los argumentos para una opción son incorrectos. Solo se envía cuando el problema es tan severo que se tiene que descartar el datagrama.

Para lograr que el mensaje no sea ambiguo, el transmisor utiliza el campo pointer en el encabezado del mensaje para identificar el octeto del datagrama que causo el problema. El código 1 se utiliza para informar que falta la opción requerida.

Sincronización de relojes y estimación del tiempo de tránsito

El grupo de protocolos TCP/IP, incluye muchos protocolos que se pueden utilizar para sincronizar los relojes de las máquinas, (cada máquina tiene su propio reloj). Una de las técnicas más sencillas se vale de un mensaje ICMP para obtener la hora de la otra máquina. Una máquina solicitante envía un mensaje ICMP de solicitud de TIMESTAMP (marca de hora) a otra, solicitándole que informe su valor actual para la hora del día. La máquina receptora envía una respuesta de TIMESTAMP (marca de hora) a quien la solicito.

El campo TYPE identifica el mensaje como solicitud (13) o como respuesta (14); los campos IDENTIFIER Y SEQUENCE NUMBER los utiliza la fuente para asociar las solicitudes con las respuestas. Los campos restantes especifican la hora, en milisegundos. El campo ORIGINATE TIMESTAMP es llenado por la fuente original justo antes de transmitir el paquete, el campo RECEIVE TIMESTAMP se llena inmediatamente al recibir una solicitud y el campo TRANSMIT TIMESTAMP se llena justo antes de transmitir la respuesta.

Solicitud de información y mensajes de respuesta

Los mensajes ICMP de solicitud de información y respuesta de información (tipos 15 y 16) actualmente se consideran como obsoletos y no se deben de utilizar. Originalmente se permitía que los anfitriones descubrieran su dirección de red en el arranque del sistema. Los protocolos de direcciones RARP y BOOTP son los que actualmente se utilizan.

2.11 AMBIENTE TCP/IP

TCP/IP es una arquitectura de protocolos. Podemos decir que es un sistema abierto que permite a cualquiera desarrollar y modificar los servicios que ofrece, además crea niveles de abstracción que separa en capas a los medios físicos y los de programación, como mencionamos anteriormente tiene similitud con el Modelo OSI; en consecuencia todos los servicios están descritos por protocolos.

El diseño de capas permite dividir las tareas y servicios tal que la arquitectura tiene que realizarlo en módulos. Los protocolos interactuan entre sí en forma de pila. La capa superior interactua con el nivel inferior, y este a su vez interactua con su siguiente nivel inferior. El flujo de datos físico es como sigue:

- ✓ Bajan a través de la pila de protocolos para enviar los datos.
- ✓ Cruzan la red física.
- ✓ Suben la pila de protocolos en el host destino para recibir datos

TCP/IP se ha implantado frecuentemente en LAN estándar 802.3, sin embargo cabe aclarar que TCP/IP es un conjunto de protocolos no relacionados con las capas física y de enlace de datos, según se describe en el modelo de referencia OSI. TCP/IP se puede implantar en casi cualquier medio físico de comunicaciones de datos y protocolos de las capas física y de enlace de datos relacionados.

TCP puede residir en una misma red integrada y no requerir a IP. Es decir, si el nodo A de la red Y desea comunicarse con el nodo B de la red Y, en general no se requieren de funciones de envío existentes en IP. Por ejemplo, si la red Y es una LAN 802.3 del IEEE la implantación del estándar 802.3 se encargara de llevar un cuadro del nodo A al B. Sin embargo, si el nodo A de la red Y desea enviar un mensaje al nodo C de la red X, y la red X es quizá una red X.25 entonces se requiere a IP.

TCP ofrece una secuencia en los paquetes, control de errores y otros servicios que se requieren para generar comunicaciones confiables, en tanto que IP tomara el paquete de TCP y lo pasará a través de las vías de acceso que sean necesarias para enviarlo a la capa TCP remoto a través de la capa IP distante. De hecho, algunas redes pueden utilizar a IP, pero no a TCP, optando por utilizar en cambio algún protocolo alternativo en la capa de transporte.

Aunque hemos venido utilizando y seguiremos utilizando, el término híbrido TCP/IP para referirnos a varios protocolos diferentes, el conjunto de protocolos se denomina a menudo "conjunto de protocolos Internet" o pila de protocolos Internet. La pila Internet consta, como se mencionó antes, no solo de TCP e IP, sino también de algunos protocolos de la capa de aplicación. También seguiremos empleando "TCP/IP" para referirnos a toda la pila o conjunto Internet.

Los servicios tradicionales de TCP/IP son soportados por los protocolos adecuados que se describirán como sigue:

El protocolo de transferencia de archivos (FTP), que hace posible la transferencia de archivos de una computadora en Internet a cualquier otra computadora también en Internet.

El protocolo de terminales de red (Telnet) ofrece un medio para permitir a un usuario en Internet ingresar a cualquier otra computadora de la red.

El protocolo simple de transferencia de correspondencia (SMTP) permite a los usuarios enviar mensajes entre sí en Internet.

Cada uno de los servicios implícitos en estos protocolos deben de estar presentes en general en cualquier implantación de TCP/IP. Un sistema servidor ofrece servicios específicos a usuarios de redes, en tanto que un sistema cliente es usuario de esos servicios. El servidor y el cliente pueden estar en la misma computadora, o en computadoras diferentes. Otros servicios que ofrecen dentro del campo de acción de TCP/IP son:

Sistemas de archivos para redes
Impresión distante
Ejecución distante
Servidores de nombres
Servidores de terminales
Sistemas de ventanas orientados a redes

Sin embargo, no todos los protocolos que soportan estos dispositivos son parte de la pila de protocolos de TCP/IP oficial.

TCP se comunica con aplicaciones a través de "puertos" específicos y cada uno de ellos tiene un numero o dirección local propio. Si un proceso en el nodo A, asociado con el puerto 1, debe enviar un mensaje al puerto 2, nodo B, ese proceso transmite el mensaje del TCP de la capa de servicio con instrucciones adecuadas para dirigirlo a su destino (nodo y puerto) buscado. TCP envía el mensaje a IP con instrucciones para llevar el mensaje a IP con instrucciones para llevar el mensaje a la vía de acceso, que es el primer *lúpulo* del nodo B. Esta secuencia de eventos es regulada anexando información de control de datos del usuario en las diversas capas.

Aplicación ----------> Datos del usuario
Datos del usuario + Encabezado TCP ----------> segmento TCP
segmento TCP + Encabezado IP ----------> datagrama IP
datagrama IP + Encabezado NAP ----------> paquete

TCP segmenta los datos del usuario en unidades manejables; luego anexa un encabezado TCP que incluye el *puerto destino, numero de secuencia del segmento y suma de verificación* para probar si existen errores en la transmisión. Esta unidad recibe el nombre de *segmento* TCP.

Una vez que se ha ensamblado el segmento TCP se pasa a IP, donde se le anexa un encabezado IP. Un elemento importante almacenado en el encabezado IP es la dirección anfitrión/nodo destino; la unidad resultante es un *datagrama* IP. En general, un datagrama puede definirse como un paquete de longitud finita con información suficiente para ser enviado en forma independiente de la fuente al destino sin apoyarse en transmisiones anteriores. La transmisión de datagramas no implica en general el establecimiento de sesiones biparciales y puede o no acarrear reconocimiento de confirmación de la entrega.

Después el datagrama IP es entregado a la capa física donde el protocolo de acceso a la red anexa su información de control, creando así un *paquete*. El paquete es enviado después por el medio físico. El encabezado del paquete contiene información suficiente para llevar el paquete completo del nodo A cuando menos a la vía de acceso, y quizá más lejos. Por ejemplo, en el caso de una red 802.3 del IEEE, el paquete seria un cuadro 802.3 que encapsula los datos de TCP/IP e información de control.

Obsérvese que es probable que la corrección de errores se lleve a cabo en varios niveles. El encabezado IP contiene también una suma de verificación, al igual que el encabezado TCP. En el extremo receptor se efectúa el proceso opuesto.

La capa rotulada como "física" tiene la asignación de contener las funciones de las capas de enlace de datos y físico de OSI. Todos los nodos de una red TCP/IP podrían residir en una misma LAN, como una Ethernet. En tal caso, TCP/IP operaria como un NOS dé redes de área local. Sin embargo, el concepto fundamental que respaldo a TCP/IP fue que ofrecería un estándar común para enlazar a muchas maquinas distantes; y, más recientemente, a muchas redes distantes o remotas. En consecuencia, se debe utilizar alguna clase de sistema de dispositivo de envío /vía de acceso/puente.

2.11.1 Documentos sobre TCP/IP

La definición de los protocolos de TCP/IP se encuentran en una serie de documentos conocidos como:

"Request for Comments" (RFC)

Los RFCs son un conjunto de documentos que describen los protocolos de TCP/IP, pero no la forma de implementación.
Algunos ejemplos son:

Transmisión Control Protocol	RFC 793
Internet Protocol	RFC 791
User Datagram Protocol	RFC 768
Remote Procedure Call	RFC 1050 y 1057
TELNET	RFC 854, 764 y otros
eXternal Data Representation (XDR)	RFC 1014
Internet Subnets	RFC 917

Son de dominio público y se pueden obtener electrónicamente o por correo al NIC (Network Information Center) del Departamento de Defensa de los Estados Unidos.

Para obtenerlos por FTP se emplea la cuenta "anonymous" y password "guest". Se encuentra en el directorio /pubs/rfcs al NIC.DDN.MIL.

2.11.2 INTERNET aplicación de TCP/IP

El término de Internet se refiere a un conjunto de redes que se comunican entre sí a través de gateways y que lo único que tienen en común todas es el TCP/IP como un protocolo de comunicaciones, a menudo este conjunto de redes se llama subred, debido a que son una parte menor de la red global. Esto no implica que una subred es pequeña o dependiente de la red grande. Las subredes son redes completas, pero están conectadas por medio de un gateway como parte de una interred más grande o, en este caso, de Internet.

Con el TCP/IP, todas las interconexiones entre las redes físicas se hacen por medio de gateways. Se supone que los gateways son transparentes para el usuario, lo cual libera al gateway manejar aplicaciones de usuario, la única tarea del gateway es recibir un Protocol Data Unit (PDU; Unidad de Datos de Protocolo) proveniente de la interred local y dirigirla hacia el siguiente gateway o pasarla a la red local para su enrutamiento al usuario apropiado. Los gateways funcionan con cualquier clase de hardware y sistema operativo, siempre que estén diseñados para comunicarse con los otros gateways con los que están conectados (lo que en este caso significa que usa TCP/IP).
Pensemos en Internet formada por cuatro capas, esta arquitectura en capas de Internet se muestra en la siguiente figura 2.15:

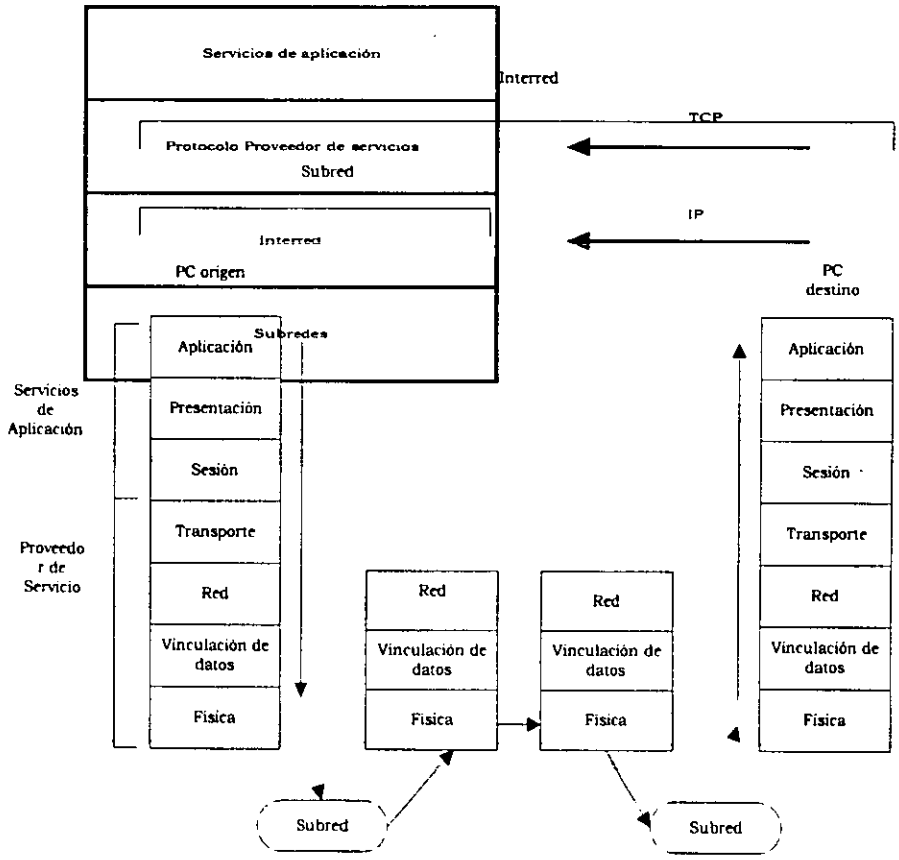


Figura 2.15 Arquitectura de Internet.

Encima de la capa de subred está la capa de interred, la cual proporciona la funcionalidad para las comunicaciones entre redes a través de gateways. Cada subred usa gateways para conectarse con las otras subredes en la interred. La capa de interred es donde se transfieren los datos de gateway a gateway hasta que alcanzan su destino y, luego, pasan a la capa de subred. La capa de interred ejecuta el Protocolo Internet (IP).

La capa del protocolo proveedor de servicios es responsable de las comunicaciones globales de extremo a extremo de la red. Esta es la capa que ejecuta el Transmission Control Protocol (TCP) y otros protocolos. Maneja el flujo de tráfico de datos en sí y asegura la confiabilidad para la transferencia de mensajes.

La capa superior es la capa de servicios de aplicación, la cual soporta las interfaces para las aplicaciones del usuario. Esta capa ofrece interfaces para correo electrónico, transferencias de archivos remotos y acceso remoto.

Suponga que una aplicación en una máquina desea transferir un datagrama a una aplicación en otra máquina, en una subred diferente el proceso se muestra en la siguiente figura 2.18. Las capas en la s máquinas transmisoras y receptora son las capas OSI, que indican las capas de la arquitectura Internet equivalentes.

Para ver como funciona el modelo de arquitectura de Internet es útil el siguiente ejemplo:

Los datos se envían hacia abajo por las capas de la maquina transmisora, ensamblando el datagrama con el Protocol Control Information (PCI; Información de Control de protocolo) mientras lo hace. Desde la capa física, el datagrama (que se llama *marco* después de que la capa de vinculación de datos ha añadido su información de encabezado y cola) se envía fuera de la red de área local. La LAN enruta la información hasta el gateway para que salga a la interred. Durante este proceso, a la LAN no le interesa el mensaje contenido en le datagrama. Sin embargo algunas redes alteran la información del encabezado para mostrar la máquina por la que ha pasado, entre otras cosas.

Desde el gateway; el marco pasa de gateway en gateway a lo largo de la interred hasta que llega a la subred de destino. En cada paso el gateway analiza el encabezado del datagrama para determinar si es a la subred que conduce ese gateway. Si no enruta el datagrama de vuelta por la interred. Este análisis se realiza en la capa física, eliminando la necesidad de pasar el marco de arriba hacia abajo a través de capas diferentes en cada gateway. El encabezado puede alterarse en cada gateway para reflejar su vía de enrutamiento.

Cuando el datagrama por fin se recibe en le gateway de la subred de destino, el gateway reconoce que el datagrama está en la subred correcta y lo enruta hacia dentro de la LAN, y por ultimo hasta la maquina que es su objetivo. El enrutamiento se logra leyendo la información del encabezado, cuando alcanza la maquina de destino, pasa hacia arriba a través de las capas, con cada capa retirando su encabezado PCI y luego pasando el resultado hacia arriba. Al final la capa de aplicación en la maquina de destino procesa el encabezado final y pasa el mensaje hasta la aplicación correcta.

Si el datagrama no tenía datos para procesar sino una solicitud de servicio, como una transferencia de archivo remota, la capa correcta en la maquina de destino descifrará la solicitud y enrutará el archivo de regreso por la interred hasta la maquina original.

CAPITULO TERCERO
INTERCONECTIVIDAD LAN – WAN

3.1 UDP Protocolo de Datagrama de Usuario.

En el grupo de protocolos TCP/IP, el Protocolo de Datagrama de Usuario o UDP proporciona el mecanismo primario que utilizan los programas de aplicación para enviar datagramas a otros programas de aplicación. Él UDP proporciona puertos de protocolo utilizados para distinguir entre muchos programas que se ejecutan en la misma maquina. Esto es, además de los datos, cada mensaje UDP contiene tanto él numero de puerto de destino como el numero de puerto de origen, haciendo posible que el software UDP en el destino entregue el mensaje al receptor correcto y que este envíe una respuesta.

El UDP utiliza Protocolo Internet subyacente para transportar un mensaje de una maquina a otra y proporciona la misma semántica de entrega de datagramas, sin conexión y no confiable que el IP; es decir, no emplea acuses de recibo para asegurarse de que llegan mensajes, no ordena los mensajes entrantes, ni proporciona retroalimentación para controlar la velocidad a la que fluye la información entre las maquinas. Por tanto, los mensajes UDP se pueden perder, duplicar o llegar sin orden.

Además, los paquetes pueden llegar más rápido de lo que el receptor los puede procesar. Podemos resumir que:

El protocolo de datagrama de usuario (UDP) proporciona un servicio de entrega sin conexión y no confiable, utilizando el IP para transportar mensajes entre maquinas. Emplea el IP para llevar mensajes, pero agrega la capacidad para distinguir entre varios destinos dentro de una computadora anfitrión.

Un programa de aplicación que utiliza el UDP acepta toda la responsabilidad por el manejo de problemas de confiabilidad, incluyendo la perdida, duplicación y retraso de los mensajes, la entrega fuera de orden y la perdida de conectividad. Por desgracia, los programadores de aplicaciones a menudo olvidan estos problemas cuando diseñan software. Además, como los programadores a menudo prueban el software de red utilizando redes de área local, altamente confiables y de baja demora, el procedimiento de pruebas puede no evidenciar las fallas potenciales.

Por lo tanto, muchos programas de aplicación que confían en él UDP. Trabajan bien en un ambiente local, pero fallan dramáticamente cuando se utilizan en una red de redes TCP/IP más grande.

3.1.1 Formato de los mensajes UDP

Cada mensaje UDP se conocen como datagrama de usuario. Conceptualmente, un datagrama de usuario consiste de dos partes: un encabezado UDP y un área de datos UDP. Como se muestra en la figura 3.1 el encabezado se divide en cuatro campos de 16 bits, que especifican el puerto desde el que se envío el mensaje, el puerto para el que se destina el mensaje, la longitud del mensaje y una suma de verificación UDP.

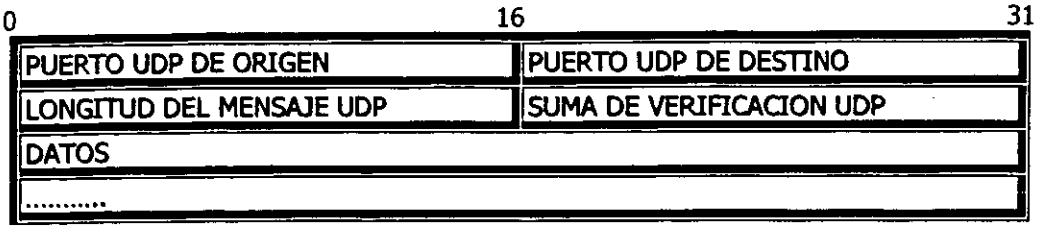


Figura 3.1 Formato del datagrama UDP

Los campos puerto de origen y puerto de destino contienen los números de puerto del protocolo UDP utilizados para el demultiplexado de datagramas entre los procesos que los esperan recibir. El puerto de origen es opcional, cuando se utiliza, especifica la parte a la que se deben enviar las respuestas, de lo contrario, puede tener valor de cero.

El campo de longitud contiene un conteo de los octetos en el datagrama UDP, incluyendo el encabezado y los datos del usuario UDP. Por lo tanto, el valor mínimo para el campo de longitud es de ocho, que es la longitud del encabezado.

La suma de verificación UDP es opcional y no es necesario utilizarla; un valor de cero en el campo suma de verificación significa que la suma no se computo. Los diseñadores decidieron hacer opcional la suma de verificaciones a fin de permitir que las implantaciones operen con poco trabajo computacional cuando utilicen UDP en una red de área local altamente confiable. Sin embargo, recuerde que IP no computa una suma de verificación de la porción de datos de un datagrama IP.

Así que, la suma de verificación UDP proporciona la única manera de garantizar que los datos lleguen intactos, por lo que se debe utilizar.
Los principiantes, a menudo, se preguntan que sucede con los mensajes UDP en los que la suma de verificación computada es cero. Un valor computacional de cero es posible debido a que él UDP utiliza el mismo algoritmo de suma de verificación que el IP: divide los datos en cantidades de 16 bits y computa el complemento de los unos de su suma de complementos de los unos. De manera sorprendente, el cero no es un problema debido a que la aritmética de los unos tiene dos representaciones para el cero: todos los bits como cero o todos los bits como uno. Cuando la suma de verificación computada es igual a cero, él UDP utiliza la representación con todos los bits como uno.

3.1.2 Pseudo – encabezado UDP

La suma de verificación UDP abarca más información de la que está presente en el diagrama UDP por sí solo. Por computar la suma de verificación, él UDP añade un pseudo-encabezado al datagrama UDP, adjunta un octeto de ceros para rellenar el datagrama y alcanzar exactamente un múltiplo de 16 bits, y computa la suma de verificación sobre todo el conjunto. El octeto utilizado como relleno y el pseudo-encabezado no se transmiten con el datagrama UDP, ni se incluyen en su longitud UDP, para computar una suma de verificación, el software primero almacena un cero en campo en el campo de suma de verificación, luego, acumula una suma de complemento de 16 bits de todo el conjunto, incluyendo el pseudo-encabezado, el encabezado UDP y los datos del usuario.

El propósito de utilizar un pseudo-encabezado es para verificar que el datagrama UDP llego a su destino correcto. La clave para entender el uso del pseudo- encabezado reside en darse cuenta de que el destino correcto consiste en una maquina especifica y en un puerto de protocolo especifico dentro de dicha maquina. Por si mismo, el encabezado UDP solo especifica él numero de puerto de protocolo. Por lo tanto, para verificar un destino, el UDP en la maquina transmisora computa una suma de verificación que cubre tanto la dirección IP de destino como el datagrama UDP. En el

destino final, el software UDP revisa la suma de verificación utilizando la dirección IP de destino, obtenida del encabezado del datagrama IP que transporto el mensaje UDP. Si la suma concuerda, debe ser verdad que el datagrama llego al anfitrión de destino deseado, así como al puerto de protocolo correcto dentro del anfitrión.

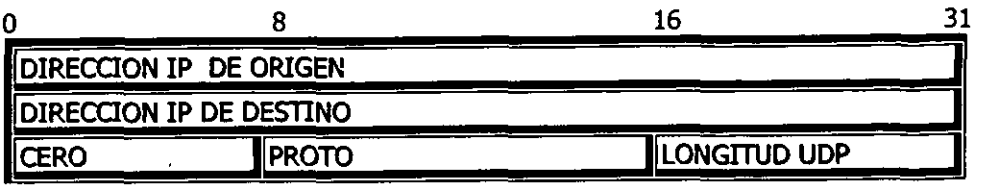


Figura 3.2 Pseudo-encabezado de la suma de verificación UDP

El pseudo-encabezado utilizado en él computo de la suma de verificación UDP consiste en 12 octetos de datos, distribuidos como se muestra en la figura 3.2 los campos en el pseudo-encabezado etiquetados como dirección IP de origen y dirección IP de destino, contienen las direcciones IP que se utilizaran cuando se envíe el mensaje UDP. El campo protocolo contiene el código del tipo de protocolo IP (17 para UDP) y el campo longitud UDP contiene la longitud del datagrama UDP 8 (sin incluir el pseudo- encabezado). Para revisar la suma de verificación, el receptor debe extraer estos.

3.1.3 Encapsulación de UDP y estratificación por capas de protocolos.

Él UDP proporciona nuestro primer ejemplo de un protocolo de transporte. El UDP reside sobre la capa del Protocolo Internet. Conceptualmente, los programas de aplicación accesan al UDP, que utiliza el IP para enviar y recibir datagramas.

Estratificar por capas él UDP por encima del IP significa que un mensaje UDP completo incluyendo el encabezado UDP y los datos, se encapsulan en un datagrama IP mientras viaja a través de una red de redes, tal como se muestra en la figura 3.3

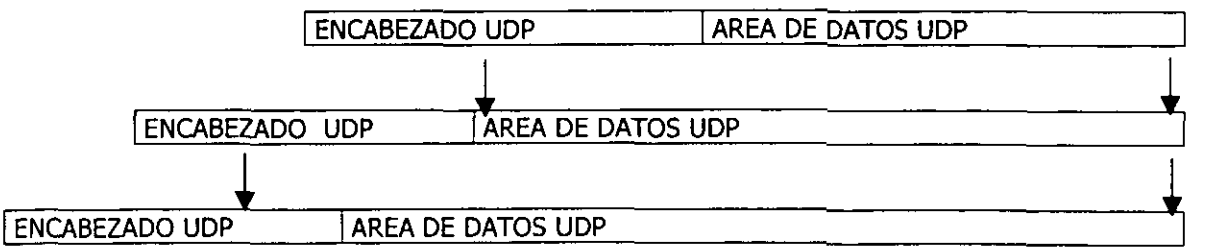


Figura 3.3 Datagrama UDP encapsulado en un datagrama IP

La encapsulación significa que él UDP adjunta un encabezado a los datos que un usuario envía y lo pasa al IP. La capa IP adjunta un encabezado a lo que recibe del UDP. Y por ultimo, la capa de interfaz de red introduce el datagrama en una trama antes de enviarlo de una maquina a otra. El formato de la trama depende de la tecnología subyacente de red. Por lo general, las tramas de red incluyen un encabezado adicional.

En la entrada, un paquete llega en la capa mas baja del software de red y comienza su ascenso a través de capas sucesivamente mas altas. Cada capa quita un encabezado antes de pasar el mensaje para que, en el momento en que el nivel mas alto pasa los datos al proceso receptor, todos los encabezados se hayan removido. Por lo tanto, el encabezado exterior corresponde a la capa mas baja del protocolo y el encabezado interior a la mas lata de protocolo. Cuando se

considera como se insertan y remueven los encabezados, es importante tener en cuenta el principio de la estratificación por capas.

En lo particular, observe que este principio se aplica al UDP paso al IP en la maquina de origen. También, los datos que él UDP entrega a un proceso usuario en la maquina receptora serán los mismos que un proceso usuario pase al UDP en la maquina transmisora. La división de funciones entre varias capas de protocolos es inflexible y clara:

La capa IP solo es responsable de transferir datos entre un par de anfitriones dentro de una red de redes, mientras que la capa UDP solamente es responsable de diferenciar entre varias fuentes o destinos dentro de un anfitrión.

Por lo tanto, solo el encabezado IP identifica los anfitriones de origen y destino, solo la capa UDP identifica los puertos de origen o destino dentro de un anfitrión.

Estratificación por capas y computo UDP de suma de verificación.

Recuerde que la suma de verificación UDP incluye un pseudo-encabezado que tiene campos para las direcciones IP de origen y de destino. Se puede decir que el usuario debe conocer la dirección IP de destino cuando envía un datagrama UDP y que este la debe pasar a la capa UDP. Por lo tanto, la capa UDP puede obtener la dirección IP de destino sin interactuar con la capa IP. Sin embargo, la dirección IP de origen depende de la ruta que el IP seleccione para el datagrama, debido a que esta dirección identifica la interfaz de red sobre la que se transmite el datagrama. Por lo tanto, él UDP no puede conocer una dirección IP de origen a menos que interactúe con la capa IP.

Asumimos que el software UDP pide a la capa IP que compute la dirección IP de origen y (posiblemente) la de destino, las utiliza para construir un pseudo-encabezado, computa la suma de verificación, descarta el pseudo-encabezado y transfiere a la capa IP el datagrama UDP para su transmisión. Con un enfoque alternativo, que produce una mayor eficiencia, se logra que la capa UDP encapsule el datagrama UDP en un datagrama IP, obtenga del IP la dirección de origen, almacene las direcciones tanto de origen como de destino en los campos apropiados del encabezado del datagrama, compute la suma de verificación UDP y pase el datagrama IP a la capa IP, que solo necesita llenar los campos restantes del encabezado IP.

El UDP esta fuertemente integrado al protocolo IP. Es claramente una transigencia de la separación pura, diseñado enteramente por razones prácticas.
Deseamos pasar por alto la violación de estratificación por capas, ya que es imposible identificar plenamente un programa de aplicación de destino sin especificar la maquina de destino y porque queremos realizar, de manera eficaz, la transformación de direcciones utilizadas por él UDP y el IP.

3.1.4 Multiplexado, demultiplexado y puertos UDP

El software UDP proporciona multiplexado y demultiplexado. Acepta datagramas UDP de muchos programas de aplicación y los pasa a IP para su transmisión, también acepta datagramas entrantes UDP del IP y los transfiere al programa de aplicación apropiado.

Conceptualmente, todo el multiplexado y demultiplexado entre el software UDP y los programas de aplicación ocurren a través del mecanismo de puerto. En la practica, cada programa de aplicación debe negociar con el sistema operativo para obtener un puerto del protocolo y un numero de puerto asociado, antes de poder enviare un datagrama UDP. Una vez que se asigna el puerto, cualquier datagrama que envíe el programa de aplicación a través de él, tendrá él numero de puerto en el campo puerto de origen UDP.

La forma más fácil de pensar en un puerto UDP es una cola de espera. En la mayor parte de las implantaciones, cuando un programa de aplicación negocia con el sistema operativo la utilización de cierto puerto, el sistema operativo crea una cola de espera interna que puede almacenar los mensajes que lleguen. A menudo, la aplicación puede especificar o modificar el tamaño de la cola de espera.

Cuando él UDP recibe un datagrama, verifica si el número de puerto de destino corresponde a uno de los puertos que están en uso. Si no, envía mensaje de error ICMP de puerto no accesible y descarta el datagrama. Si encuentra una correspondencia, él UDP pone en cola de espera el nuevo datagrama, en el puerto en que lo pueda accesar un programa de aplicación. Por supuesto, ocurre un error si el puerto se encuentra lleno y él UDP descarta el datagrama entrante.

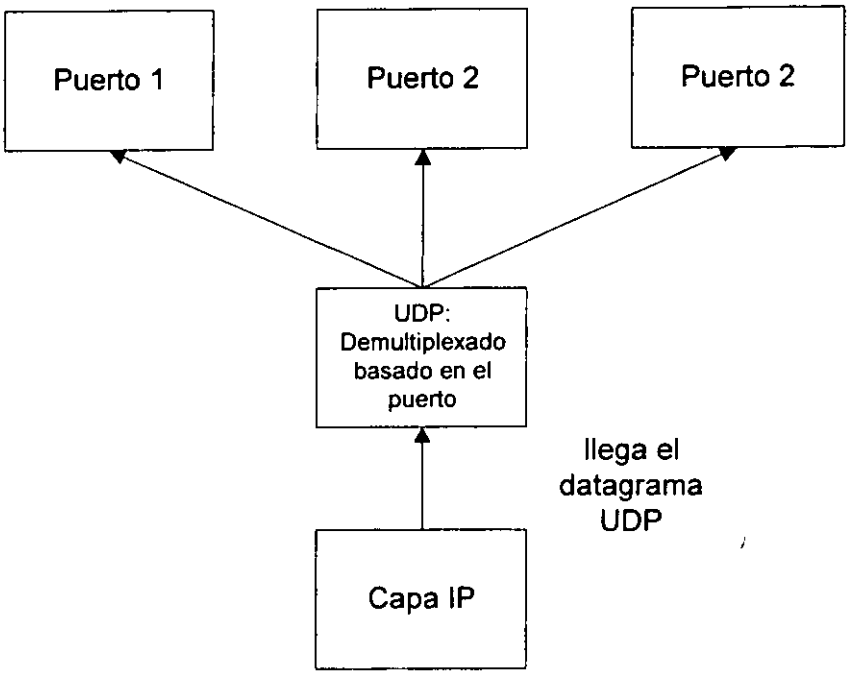


Figura 3.4 Demultiplexado de una capa sobre el IP

3.1.5 Números de Puerto UDP reservados y disponibles

Por ejemplo, cuando la computadora A quiere obtener un archivo de la computadora B, necesita saber que puerto utiliza el programa de transferencia de archivos en la computadora B. Existen dos enfoques fundamentales para la asignación de puertos. El primero se vale de una autoridad central, es decir, todos se ponen de acuerdo en permitir que una autoridad central asigne los números de puerto conforme se necesitan y que publique las asignaciones; este enfoque se conoce como enfoque universal y las asignaciones de puerto especificadas por la autoridad se conocen como asignaciones bien conocida de puerto.

El segundo enfoque para la asignación de puertos emplea la transformación dinámica, los puertos no se conocen de manera global, en vez de eso, siempre que un programa necesita un puerto, el software de red le asigna uno. Para conocer la asignación actual del puerto en otra computadora, es necesario enviar una solicitud que pregunte algo así como ¿qué puerto está utilizando el servicio de transferencia de archivos? ; la máquina objetivo responde al proporcionar el número de puerto correcto a utilizar.

Los diseñadores de TCP/IP adoptaron un enfoque híbrido que preasigna algunos números de puerto, pero que deja muchos de ellos disponibles para los sitios locales o programas de aplicación. La siguiente tabla lista algunos de los números de puerto UDP actualmente asignados.

DECIMAL	PALABRA CLAVE	P.C.UNIX	DESCRIPCION
0	-	-	Reservado
7	ECHO	Echo	Eco
9	DISCARD	Discard	Descartar
11	USERS	Systat	Usuarios activos
13	DAYTIME	Daytime	Hora del día
15	-	Netstat	Quien esta ahí
17	QUOTE	Qotd	Cita del día
19	CHARGEN	Chargen	Generador de caracteres
37	TIME	Time	Hora
42	NAMESERVER	Name	Servidor de nombres de anfitriones
43	NICNAME	Whois	Quien es
53	DOMAIN	Nameserver	Servidor de nombre de dominios
67	BOOTPS	Bootps	Servidor de protocolos bootstrap
68	BOOTPC	Bootpc	Cliente de protocolos bootstrap
69	TFTP	Tftp	Transferencia trivial de archivos
111	SUNRPC	Sunrpc	RPC de sun microsystem
123	NTP	Ntp	Protocolo de tiempo de red
161	-	Snmp	Monitor de red snmp
162	-	Snmp-trap	Interrupciones snmp
512	-	Biff	Comsat UNIX
513	-	Who	Rwho daemon UNIX
514	-	Syslog	Conexión de sistema
525	-	timed	Daemon de hora

Tabla 3.1 de los Puertos UDP

El método de enrutamiento usado para enviar un mensaje desde su origen hasta su destino, es importante, sin embargo, el método mediante el cual se transfiere la información de enrutamiento depende del papel de los gateways de red, recordemos su utilidad. Para enviar mensajes a través de redes locales, el software de la capa IP de una máquina compara la dirección destino del mensaje (contenida en la Unidad de Datos de Protocolo o PDU) con la dirección de la máquina local, el mensaje se pasa a la siguiente máquina, en una red pequeña es fácil, sin embargo, para interredes se requiere de gateways, puentes y ruteadores, los cuales tratan de establecer el mejor método para mover el mensaje hasta su destino. De tal forma que podemos concluir que:

- ✓ Gateway es un dispositivo que ejecuta funciones de enrutamiento, por lo general como un dispositivo autónomo, que, además, puede traducir del protocolo de una red al de otra. La conversión de protocolo generalmente, se realiza en las capas inferiores, en ocasiones incluyendo la capa de transporte. La conversión puede ocurrir de varias formas

- ✓ Puente es un dispositivo de red que conecta dos o más redes que usan el mismo protocolo.

- ✓ Ruteador es un nodo de red que envía datagramas por la red. Los ruteadores operan al nivel de red, enviando paquetes a su destino; en ocasiones un cambio de protocolo puede

realizarse con un ruteador que tiene disponibles varias opciones de envío, como Ethernet o líneas de serie

3.2 TCP Protocolo de Control de Transmisión

Necesidad de la entrega confiable

El TCP (Transmision Control Protocol) es un protocolo que nos proporciona la entrega confiable de flujo que el IP no puede garantizar, para esto es necesario examinar la capa de transporte y los protocolos que involucra, sabemos que en el nivel más bajo (nivel de red), las redes de comunicación proporcionan una entrega de paquetes no confiables. Los paquetes se pueden perder o destruir cuando los errores de transmisión interfieren con los datos, cuando falla el hardware de red o cuando las redes se sobrecargan demasiado. Las redes que enrutan dinámicamente los paquetes pueden entregarlos en desorden, con retraso o duplicados. Además, las tecnologías relacionadas de red pueden dictar un tamaño óptimo de paquete o formular otras obligaciones necesarias para lograr velocidades eficientes de transmisión.

En el nivel más alto, los programas de aplicación a menudo necesitan enviar grandes volúmenes de datos de una computadora a otra. Utilizar un sistema de entrega sin conexión y no confiable para las transferencias de gran volumen se vuelve tedioso y requiere que se incorpore, en cada programa de aplicación, la detección y solución de errores, siendo esto una tarea que no es Fácil de realizar. Como consecuencia, es necesario tener un solo protocolo de propósito general, que sea útil para aislar los programas de aplicación de los detalles del trabajo con redes y que permita la definición de una interfaz uniforme para el servicio de transferencia de flujo. En este momento podemos decir que el TCP es parte del grupo de protocolos Internet TCP/IP.

Puertos y sockets

La interfaz que existe entre programas de aplicación y el software de protocolo deben mencionarse antes de continuar con los demás protocolos, ya que tienen una importancia relevante en las comunicaciones de TCP/IP.

Todos los procesos de nivel de aplicación que utilicen protocolos TCP/IP se deben identificar mediante un puerto. Este numero se utiliza por las dos computadoras para identificar qué programa de aplicación va a recibir el tráfico entrante.

El uso de números de puerto proporciona capacidades de multiplexación ya que varios programas de usuario se pueden comunicar de forma concurrente con un programa de aplicación, como TCP. Los números de puerto sirven para identificar a cada aplicación.

Además del uso de puertos, los protocolos basados en TCP/IP pueden utilizar también un identificador abstracto denominado socket. El concepto de socket procede de las operaciones de entrada/salida en redes. Es muy similar a los procedimientos de acceso a archivo en UNIX, en el sentido de que se identifica un proceso de comunicaciones entre dos puntos terminales. En TCP/IP, un socket consiste en la concatenación de un número de puerto y la dirección de red (la dirección IP) de la computadora que da soporte al servicio de puertos. En la Internet, algunos números de puerto están ya preasignados. Se denominan puertos bien conocidos y se utilizan para identificar aplicaciones muy comunes que se denominan servicios bien conocidos tienen valores de 0 a 255.

3.2.1 Características del servicio de entrega confiable

La interfaz entre los programas de aplicación y el servicio TCP/IP de entrega confiable se puede caracterizar por cinco funciones:

- Orientación de flujo. Cuando dos programas de aplicación (procesos de usuario) transfieren grandes volúmenes de datos, pensamos en los datos como un flujo de bits, divididos en octetos de 8 bits, que informalmente se conocen como bytes. El servicio de entrega de flujo en la máquina de destino pasa al receptor exactamente la misma secuencia de octetos que le pasa el transmisor en la máquina de origen.
- Conexión de circuito virtual. La transferencia de flujo es análoga a realizar una llamada telefónica. Antes de poder empezar la transferencia, los programas de aplicación, transmisor y receptor interactúan con sus respectivos sistemas operativos, informándose de la necesidad de realizar una transferencia de flujo. Conceptualmente, una aplicación realiza una "llamada" que la otra tiene que aceptar. Los módulos de software de protocolo en los dos sistemas operativos se comunican al enviarse mensajes a través de una red de redes, verificando que la transferencia esté autorizada y que los dos extremos estén listos. Una vez que se establecen todos los detalles, los módulos de protocolo informan a los programas de aplicación que se estableció una conexión y que la transferencia puede comenzar. Durante la transferencia, el software de protocolo en las dos máquinas continúan comunicándose para verificar que los datos se reciban correctamente. Si la comunicación no se logra por cualquier motivo (por ejemplo, debido a que falle el hardware de red a lo largo del camino entre las máquinas), ambas máquinas detectarán la falla y la reportarán a los programas apropiados de aplicación. Se utiliza el término circuito virtual para describir dichas conexiones porque aunque los programas de aplicación visualizan la conexión como un circuito dedicado de hardware, la confiabilidad que se proporciona depende del servicio de entrega de flujo.
- Transferencia con memoria intermedia. Los programas de aplicación envían un flujo de datos a través del circuito virtual pasando repetidamente octetos de datos al software de protocolo. Cuando transfieren datos, cada aplicación utiliza piezas del tamaño que encuentre adecuado, que pueden ser tan pequeñas como un octeto. En el extremo receptor, el software de protocolo entrega octetos del flujo de datos en el mismo orden en que se enviaron, poniéndolos a disposición del programa de aplicación receptor tan pronto como se reciben y verifican. El software de protocolo puede dividir el flujo en paquetes, independientemente de las piezas que transfiere el programa de aplicación. Para hacer eficiente la transferencia y minimizar el tráfico de red, las implantaciones por lo general recolectan datos suficientes de un flujo para llenar un datagrama razonablemente largo antes de transmitirlo a través de una red de redes. Por lo tanto, inclusive si el programa de aplicación genera el flujo un octeto a la vez, la transferencia a través de una red de redes puede ser sumamente eficiente. De forma similar, si el programa de aplicación genera bloques de datos muy largos, el software de protocolo puede dividir cada bloque en partes muy pequeñas para su transmisión.
- Flujo no estructurado. Es importante entender que el servicio de flujo TCP/IP no está obligado a formar flujos estructurados de datos. Por ejemplo, no existe forma para que una aplicación de nómina haga que un servicio de flujo marque fronteras entre los registros de empleado o que identifique el contenido del flujo como datos de nómina. Los programas de aplicación que utilizan el servicio de flujo deben entender el contenido del flujo y ponerse de acuerdo sobre su formato antes de iniciar una conexión.
- Conexión Full Duplex. Las conexiones proporcionadas por el servicio de flujo TCP/IP permiten la transferencia concurrente en ambas direcciones. Dichas conexiones se conocen como full duplex. Desde el punto de vista de un proceso de aplicación, una conexión full duplex consiste en dos flujos independientes que se mueven en direcciones opuestas, sin ninguna interacción aparente. El servicio de flujo permite que un proceso de aplicación termine el flujo en una dirección mientras los datos continúan moviéndose en la otra dirección, haciendo que la conexión sea half duplex. La ventaja de una conexión full duplex es que el software

subyacente de protocolo puede enviar en datagramas información de control de flujo al origen, llevando datos en la dirección opuesta. Este procedimiento de carga, transporte y descarga reduce el tráfico en la red.

Ejemplo de entrega de flujo confiable

La mayor parte de los protocolos confiables utilizan una técnica fundamental conocida como acuse de recibo positivo con retransmisión. La técnica requiere que un receptor se comunique con el origen y le envié un mensaje de acuse de recibo (ACK) conforme recibe los datos. El transmisor guarda un registro de cada paquete que envía y espera un acuse de recibo antes de enviar el siguiente paquete. El transmisor también arranca un temporizador cuando envía un paquete y lo retransmite si dicho temporizador expira antes de que llegue un acuse de recibo. En la figura 3.5, los eventos en el transmisor y receptor se muestran a la izquierda y derecha, respectivamente. Cada línea diagonal que cruza por el centro muestra la transferencia de un mensaje a través de la red y la distancia vertical bajo la figura representa el incremento en el tiempo. Esto representa la forma ideal de envío de mensajes, sin embargo, existen casos que pueden ocurrir, por ejemplo, cuando se pierde o corrompe un paquete.

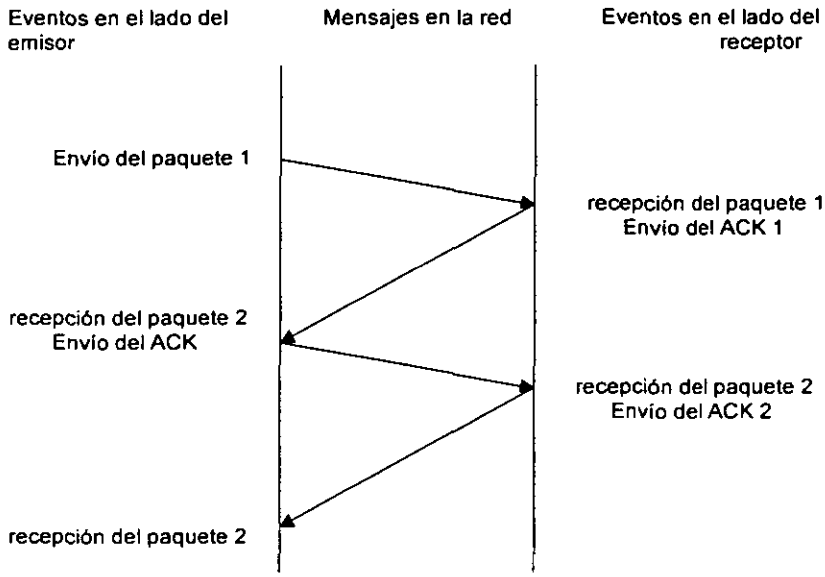


Figura 3.5 Ejemplo de un protocolo que tiene acuses de recibo positivos

El transmisor arranca un temporizador después de enviar el paquete y cuando termina el tiempo, el transmisor asume que el paquete se perdió y lo vuelve a enviar, lo cual significa un tiempo excedido; en otro caso el problema surge cuando la entrega de paquetes se duplica debido a un sistema relacionado y los duplicados también pueden surgir cuando las redes tienen grandes retrasos que provocan la retransmisión prematura. Por lo general, los protocolos confiables detectan los paquetes duplicados al asignar a cada uno un número de secuencia y al obligar al receptor a recordar que números de secuencia recibe. Para evitar la confusión causada por acuses de recibo retrasados o duplicados, los protocolos de acuses de recibo positivos envían los números de secuencia dentro de los acuses, para que el receptor pueda asociar correctamente los acuses de recibo con los paquetes.

Ventanas deslizables

Antes de examinar el servicio de flujo TCP, necesitamos explorar un concepto adicional que sirve de base para la transmisión de flujo. Este concepto, conocido como ventana deslizable, hace que la transmisión de flujo sea eficiente. Para entender lo que motiva a utilizar ventanas deslizables, retomaremos la secuencia de eventos que se muestran en la figura anterior. A fin de lograr la confiabilidad, el transmisor envía un paquete y espera un acuse de recibo antes de enviar otro; los datos sólo fluyen entre las máquinas en una dirección a la vez, inclusive si la red tiene capacidad para comunicación simultánea en ambas direcciones. La red estará del todo ociosa durante el tiempo en que las máquinas retrasen sus respuestas (por ejemplo, mientras las máquinas computan rutas o sumas de verificación). Si nos imaginamos una red con altos retrasos en la transmisión, el problema es evidente, un protocolo simple de acuses de recibo positivos ocupa una cantidad sustancial de ancho de banda de red debido a que debe retrasar el envío de un nuevo paquete hasta que reciba un acuse de recibo del paquete anterior.

Los protocolos de ventana deslizable utilizan el ancho de banda de red de mejor forma, ya que permiten que el transmisor envíe varios paquetes sin esperar un acuse de recibo. La manera más fácil de visualizar la operación de ventana deslizable es pensar en una secuencia de paquetes que se transmitirán como se muestra en la figura 3.6. El protocolo coloca una ventana pequeña y de tamaño fijo en la secuencia, y transmite todos los paquetes que residan dentro de la ventana.

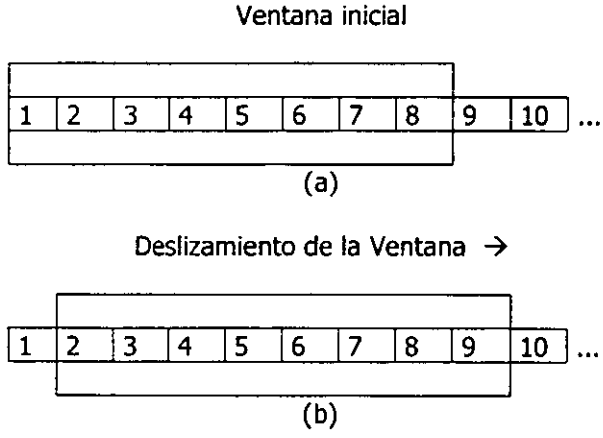


Figura 3.6 Un protocolo de ventana deslizante.

Decimos que un paquete es unacknowledged (o sin acuse de recibo) si se transmitió pero no se recibió ningún acuse de recibo. Técnicamente, el número de paquetes sin acuse de recibo en un tiempo determinado depende del tamaño de la ventana y esta limitado a un número pequeño y fijo. Por ejemplo, en un protocolo de ventana deslizable con un tamaño de ventana de 8, se permite al transmisor enviar 8 paquetes antes de recibir un acuse de recibo.

Como se muestra en la figura anterior una vez que el transmisor recibe un acuse de recibo para el primer paquete dentro de la ventana, "mueve" la misma y envía el siguiente paquete. La ventana continuará moviéndose en tanto se reciban acuses de recibo. El desempeño de los protocolos de ventana deslizable depende del tamaño de la ventana y de la velocidad en que la red acepta paquetes. Un ejemplo de la operación de un protocolo de ventana deslizable cuando se envían tres paquetes implica que el transmisor los envía antes de recibir cualquier acuse de recibo. Como un protocolo de ventana deslizable bien establecido mantiene la red completamente saturada de paquetes, con el se obtiene una generación de salida substancialmente más alta que con un protocolo simple de acuse de recibo positivo.

Conceptualmente, un protocolo de ventana deslizable siempre recuerda qué paquetes tienen acuse de recibo y mantiene un temporizador separado para cada paquete sin acuse de recibo. Si se pierde un paquete, el temporizador concluye y el transmisor reenvía el paquete. Cuando el receptor desliza su ventana, mueve hacia atrás todos los paquetes con acuse. En el extremo receptor, el software de protocolo mantiene una ventana análoga, que acepta y acusa como recibos los paquetes conforme llegan. Por lo tanto, la ventana divide la secuencia de paquetes en tres partes: los paquetes a la izquierda de la ventana se transmitieron, recibieron y acusaron exitosamente; los paquetes a la derecha no se han transmitido; y los paquetes que quedan dentro de la ventana están en proceso de transmisión. El paquete con menor número en la ventana es el primer paquete en la secuencia para el que no se ha hecho un acuse de recibo.

3.2.2 Protocolo de control de transmisión

Ya que entendimos el principio de las ventanas deslizables, podemos examinar el servicio de flujo confiable proporcionado por el grupo de protocolos TCP/IP de Internet. El servicio lo define el Protocolo de Control de Transmisión o TCP. El servicio de flujo confiable es tan importante que todo el grupo de protocolos se conoce como TCP/IP.

El protocolo especifica el formato de datos y los acuses de recibo que intercambian dos computadoras para lograr una transferencia confiable, así como los procedimientos que la computadora utiliza para asegurarse de que los datos lleguen de manera correcta.

También, especifica cómo el software TCP distingue el correcto entre muchos destinos en una misma máquina, y cómo las máquinas en comunicación resuelven errores como la pérdida o duplicación de paquetes. El protocolo también especifica cómo dos computadoras inician una transferencia de flujo TCP y cómo se ponen de acuerdo cuando se completa.

Debido a que TCP asume muy poco sobre el sistema subyacente de comunicación, TCP se puede utilizar con una gran variedad de sistemas de entrega de paquetes, incluyendo el servicio de entrega de datagramas IP. Por ejemplo, el TCP puede implantarse para utilizar líneas de marcación telefónica, una red de área local, una red de fibra óptica de alta velocidad o una red de largo recorrido y baja velocidad. De hecho, la gran variedad de sistemas de entrega que puede utilizar el TCP es una de sus ventajas.

El TCP permite que varios programas de aplicación en una máquina se comuniquen de manera concurrente y realiza el demultiplexado del tráfico TCP entrante entre los programas de aplicación. Al igual que el Protocolo de Datagrama de Usuario (UDP), el TCP utiliza número de puerto de protocolo para identificar el destino final dentro de una máquina. Cada puerto tiene asignado un número entero pequeño utilizado para identificarlo.

Estratificación por capas conceptual

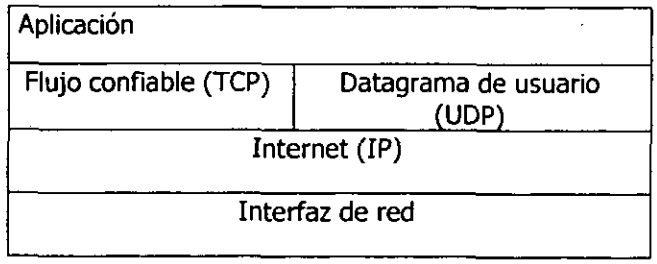


Figura 3.7 La estratificación por capas conceptual del UDP y el TCP sobre el IP.

Sin embargo, los puertos TCP son mucho más complejos, ya que un número de puerto no corresponde a un solo objeto. De hecho, el TCP se diseñó según la abstracción de conexión, en la que los objetos que se van a identificar son conexiones de circuito virtual, no puertos individuales. El TCP utiliza la conexión, no el puerto de protocolo, como su abstracción fundamental; las conexiones se identifican por medio de un par de puntos extremos.

Puntos Extremos De Una Conexión

Hemos dicho que una conexión consiste en un circuito virtual entre dos programas de aplicación, por lo que puede ser natural asumir que un programa de aplicación sirve como el "punto extremo" de la conexión. Sin embargo, no es así. El TCP define que un punto extremo es un par de números enteros (anfitrión, puerto), en donde anfitrión es la dirección IP de un anfitrión y puerto es un puerto TCP en dicho anfitrión. Por ejemplo, el punto extremo (128.10.2.3, 25), se refiere al puerto TCP 25 en la máquina con dirección IP 128.10.2.3. sabemos que una conexión se define por sus dos puntos extremos. Por lo tanto, si existe una conexión entre la máquina (18.26.0.36) en el lugar x y la máquina (128.10.2.3) en el lugar y, la conexión se definiría por los puntos extremos:

(18.26.0.36, 1069) y (128.10.2.3, 25)

Mientras tanto, otra conexión se puede dar entre la máquina (128.9.0.32) en el lugar z y la misma máquina en el lugar y, conexión identificada por sus puntos extremos:

(128.9.0.32, 1184) y (128.10.2.3, 53).

Hasta ahora, nuestros ejemplos de conexiones han sido directos, ya que los puertos utilizados en todos los puntos extremos han sido únicos. Sin embargo, la abstracción de conexión permite que varias conexiones compartan un punto extremo. Por ejemplo, podemos agregar otra conexión a las dos arriba mencionadas entre la máquina (128.2.254.139) en el lugar x1 y la máquina en el lugar y:

(128.2.254.136, 1184) y (128.10.2.3, 53).

Puede parecer extraño que dos conexiones utilicen al mismo tiempo el puerto TCP 53 en la máquina 128.10.2.3, pero no hay ambigüedad. Debido a que el TCP asocia los mensajes entrantes con una conexión en vez de hacerlo con un puerto de protocolo, utiliza ambos puntos extremos para identificar la conexión apropiada, es decir: el TCP identifica una conexión por medio de un par de puntos extremos, varias conexiones en la misma máquina pueden compartir un número de puerto TCP.

Lo cual significa que un programador puede diseñar un programa que proporcione servicio concurrente a varias conexiones al mismo tiempo, sin necesitar números únicos del puerto local para cada una; por ejemplo, la mayor parte de los sistemas proporciona acceso concurrente a su servicio de correo electrónico, lo cual permite que varias computadoras les envíen correo electrónico de manera concurrente. Debido a que el programa que acepta correo entrante utiliza TCP para comunicarse, solo necesitan emplear un puerto TCP local, aun cuando permita que varias conexiones se realicen en forma concurrente.

El TCP es un protocolo orientado a la conexión, el cual requiere que ambos puntos extremos estén de acuerdo en participar. Esto es, antes de que el tráfico TCP pueda pasar a través de una red de redes, los programas de aplicación en ambos extremos de la conexión deben estar de acuerdo en que desean dicha conexión. En ese momento, el sistema operativo asigna un número de puerto TCP a su extremo de la conexión. El programa de aplicación en el otro extremo debe contactar a su sistema operativo mediante una solicitud de apertura activa para establecer una conexión. Los

dos módulos de software TCP se comunican para establecer y llevar a cabo la conexión. Una vez que se crea ésta, los programas de aplicación pueden comenzar a transferir datos; los módulos de software TCP en cada extremo intercambian mensajes que garantizan la entrega confiable.

3.2.3 Segmentos y números de secuencia

El TCP visualiza el flujo de datos como una secuencia de octetos (o bytes) que divide en segmentos para su transmisión. Por lo general, cada segmento viaja a través de una red de redes como un solo diagrama IP.

El TCP utiliza un mecanismo especializado de ventana deslizable para solucionar dos problemas importantes: la transmisión eficiente y el control de flujo, este mecanismo de ventana del TCP hace posible enviar varios segmentos antes de que llegue un acuse de recibo. Hacerlo así aumenta la generación total de salida ya que mantiene ocupada a la red. La forma TCP de un protocolo de ventana deslizable también soluciona el problema de control de flujo de extremo a extremo, al permitir que el receptor restrinja la transmisión hasta que tenga espacio suficiente en memoria intermedia para incorporar más datos.

El mecanismo TCP de ventana deslizable opera a nivel de octeto, no a nivel de segmento ni de paquete. Los octetos del flujo de datos se numeran de manera secuencia, y el transmisor guarda tres apuntadores asociados con cada conexión. Los apuntadores definen una ventana deslizable, como se muestra en la figura 3.8 el primer apuntador marca el extremo izquierdo de la ventana deslizable, separa los octetos que ya se enviaron y envía el acuse de recibo de los octetos ya enviados. Un segundo apuntador marca el extremo derecho de la ventana deslizable y define el octeto más alto en la secuencia que se puede enviar antes de recibir más acuses de recibo. El tercer apuntador señala la frontera dentro de la ventana que separa los octetos que ya se enviaron de los que todavía no se envían. El software de protocolo envía sin retraso todos los octetos dentro de la ventana, por lo que en general la frontera dentro de la ventana se mueve rápidamente de izquierda a derecha.

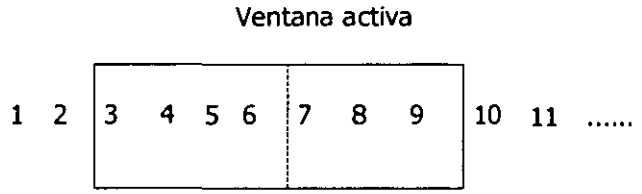


Figura 3.8 Ventana deslizante del TCP.

Hemos descrito cómo la ventana TCP del transmisor se desliza y hemos mencionado que el receptor debe tener una ventana similar para ensamblar de nuevo el flujo. Sin embargo, es importante entender que, como las conexiones TCP son de tipo full duplex, se llevan a cabo dos transferencias al mismo tiempo en cada conexión, una en cada dirección. Pensamos en las transferencias como en algo totalmente independientes porque, en cualquier momento, los datos pueden fluir a través de la conexión en una o en ambas direcciones. Por lo tanto, el software TCP en cada extremo mantiene dos ventanas por cada conexión (un total de cuatro), una se desliza a lo largo del flujo de datos que se envía, mientras la otra se desliza a lo largo de los datos que se reciben.

La sobrecarga de las máquinas intermedias se conoce como congestionamiento y los mecanismos que resuelven el problema se conocen como mecanismos de control de congestionamiento. El TCP

emplea su esquema de ventana deslizable para resolver el problema de control de flujo extremo a extremo; no cuenta con un mecanismo explícito para el control de congestionamientos.

3.2.4 Formato del segmento TCP.

La unidad de transferencia entre el software TCP de dos máquinas se conoce como segmento. Los segmentos se intercambian para establecer conexiones, transferir datos, enviar acuses de recibo, anunciar los tamaños de ventanas y para cerrar las conexiones.

Debido a que el TCP utiliza acuses de recibo incorporados, un acuse que viaja de la máquina A a la máquina B puede viajar en el mismo segmento en el que viajan los datos de la máquina A a la máquina B, aun cuando el acuse de recibo se refiera a los datos enviados de B hacia A. En la figura 3.9 se muestra la unidad de datos del protocolo TCP.

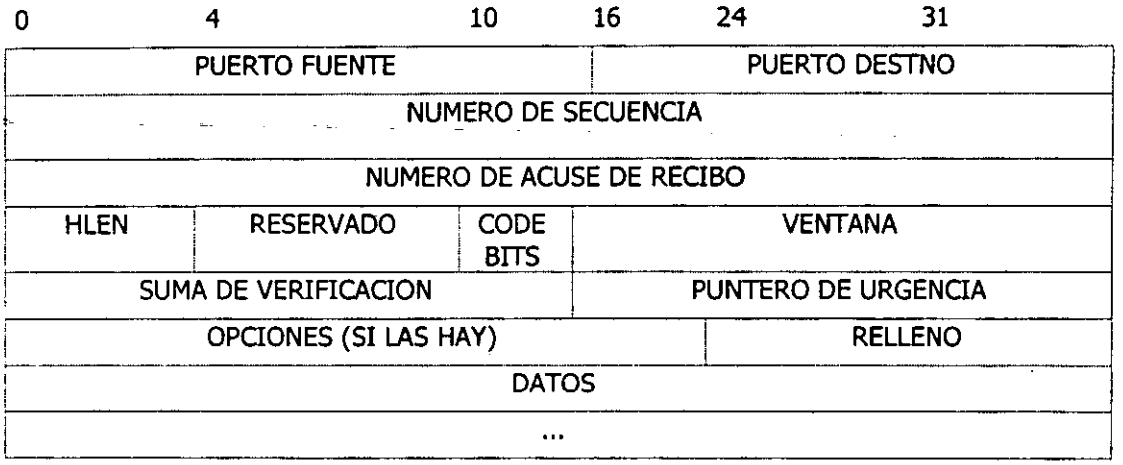


Figura 3.9 Formato de un segmento TCP con un encabezado TCP seguido de datos.

Cada segmento se divide en dos partes: encabezado y datos. El encabezado, conocido como encabezado TCP, transporta la identificación y la información de control. Los campos SOURCE PORT (PUERTO FUENTE) y DESTINATION PORT (PUERTO DESTINO) contienen los números de puerto TCP que identifican a los programas de aplicación en los extremos de la conexión. El campo SEQUENCE NUMBER (NUMERO DE SECUENCIA) identifica la posición de los datos del segmento en el flujo de datos del transmisor. El campo ACKNOWLEDGEMENT NUMBER (NUMERO DE ACUSE DE RECIBO) identifica el número de octetos que la fuente espera recibir después. Observe que el número de secuencia se refiere al flujo que va en la misma dirección que el segmento, mientras que el número de acuse de recibo se refiere al flujo que v en la dirección opuesta al segmento.
El campo HLEN contiene un número entero que especifica la longitud del encabezado del segmento, medida en múltiplos de 32 bits. Es necesario porque el campo OPTIONS (OPCIONES) varia en su longitud, dependiendo en que opciones se haya incluido. Así el tamaño del encabezado TCP varia dependiendo de las opciones seleccionadas. El campo de 6 bits marca como RESERVED (RESERVADO), esta reservado para usarse en el futuro.

Algunos segmentos sólo llevan un acuse de recibo y otros solamente llevan datos. Otros llevan solicitudes para establecer o cerrar una conexión. El software TCP utiliza el campo de 6 bits, etiquetado como CODE BITS, para determinar el propósito y contenido del segmento. Los seis bits indican cómo interpretar otros campos en el encabezado, de acuerdo con la siguiente tabla

Bit (de izquierda a derecha)	Significado si el bit está puesto a 1
URG	El campo de puntero de urgente es válido
ACK	*El campo de acuse de recibo es válido*
PSH	Este segmento solicita una operación push
RST	Iniciación de la conexión
SYN	Sincronizar números de secuencia
FIN	El emisor ha llegado al final de su flujo de octetos

Tabla 3.2 Bits del campo CODE en el encabezado TCP.

El software TCP informa sobre cuántos datos está dispuesto a aceptar cada vez que envía un segmento, al especificar su tamaño de memoria intermedia en el campo WINDOW. El campo contiene un número entero sin signo de 16 bits en el orden de octetos estándar de red. Los anuncios de ventana proporcionan otro ejemplo de acuse de recibo de carga, transporte y descarga ya que acompañan a todos los segmentos, tanto a los que llevan datos, como a los que sólo llevan un acuse de recibo.

El protocolo especifica que, cuando se encuentra con datos urgentes, el TCP receptor debe notificar al programa de aplicación, que esté asociado con la conexión, que entre en "modalidad urgente". Después de asimilar todos los datos urgentes, el TCP indica al programa de aplicación que regrese a su operación normal.

El mecanismo utilizado para marcar los datos urgentes cuando se transmiten en un segmento consiste en un bit de código URG y en un campo URGENT POINTER (PUNTERO DE URGENCIA). Cuando se activa el bit URG, el indicador urgente especifica la posición dentro del segmento en la que terminan los datos urgentes.

Opción de tamaño máximo de segmento.

No todos los segmentos que se envían a través de una conexión serán del mismo tamaño. Sin embargo, ambos extremos necesitan acordar el tamaño máximo de los segmentos que transferirán. El software TCP utiliza el campo OPTIONS para negociar con el software TCP en el otro extremo de la conexión; una de las opciones permite que el software TCP especifique el tamaño máximo de segmento (MSS) que está dispuesto a recibir.

Por lo tanto, si los dos puntos extremos residen en la misma red física, el TCP por lo general computará un tamaño máximo de segmentos de tal forma que los datagramas IP resultantes correspondan con la MTU de la red. Si los puntos extremos no residen en la misma red física, pueden intentar descubrir la MTU mínima a lo largo del camino entre ellos o pueden escoger un tamaño máximo de segmento de 536 (tamaño máximo asignado por omisión de un datagrama IP, 576, menos el tamaño estándar de los encabezados IP y TCP). Los segmentos TCP viajan encapsulados dentro de datagramas IP, que a su vez están encapsulados en tramas de red física.

Por lo tanto, cada segmento tiene al menos 40 octetos de encabezados TCP e IP, además de los datos. Así pues, los datagramas que sólo llevan un octeto de datos utilizan como máximo 1/41 del ancho de banda de la red subyacente para los datos de usuario, en la práctica, las brechas mínimas entre paquetes y el hardware de red que ponen bits en tramas hacen que el rango sea aún muy pequeño.

Computo de suma de verificación TCP

El campo CHECKSUM (VERIFICACION DE SUMA) en el encabezado TCP contiene una suma de verificación de números enteros y 16 bits que se utiliza para verificar la integridad de los datos así como el encabezado TCP. En la Figura 3.11, se muestra el formato del pseudo-encabezado empleado en el cómputo de la suma de verificación.

0	8	16	31
DIRECCION IP DE LA FUENTE			
DIRECCION IP DEL DESTINO			
CERO	PROTOCOLO	LONGITUD TCP	

Figura 3.11 Formato del pseudo-encabezado utilizado en el cálculo de la suma de verificación del TCP. En la localidad receptora, esta información se extrae del datagrama IP que transportaba el segmento.

El TCP transmisor asigna al campo PROTOCOL (PROTOCOLO) el valor que utilizará el sistema subyacente de entrega en su campo de tipo de protocolo. Para los datagramas IP que transporten TCP, el valor es 6. El campo TCP LENGHT (LONGITUD TCP) especifica la longitud total del segmento TCP, incluyendo el encabezado TCP. En el extremo receptor, la información utilizada en el pseudo-encabezado se extrae del datagrama IP que transportó el segmento y se incluye en el cómputo de la suma para verificar que el segmento llegó intacto al destino correcto.

Acuses de recibo y retransmisión

Como el TCP envía los datos en segmentos de longitud variable, y debido a que los segmentos retransmitidos pueden incluir más datos que los originales, los acuses de recibo no pueden remitirse fácilmente a los datagramas o segmentos.

Como los segmentos viajan en datagramas IP, se pueden perder o llegar en desorden; el receptor utiliza los números de secuencia para reordenar los segmentos. Al esquema TCP de acuse de recibo se le llama acumulativo porque reporta cuánto se ha acumulado del flujo. Los acuses de recibo acumulativos tienen ventajas y desventajas. Una ventaja es que los acuses de recibo son fáciles de generar y no son ambiguos. Otra es que los acuses de recibo perdidos no necesariamente forzarán la retransmisión. Una gran desventaja es que el receptor no obtiene información sobre todas las transmisiones exitosas, sino únicamente sobre una sola posición en el flujo que se recibió.

Tiempo límite y retransmisión

La terminación de tiempo (time out) y la retransmisión en el TCP espera que el destino envíe acuses de recibo siempre que recibe exitosamente nuevos octetos del flujo de datos. Cada vez que envía un segmento, el TCP arranca un temporizador y espera un acuse de recibo. Si se termina el tiempo antes de que se acusen de recibidos los datos en el segmento, el TCP asume que dicho segmento se perdió o corrompió y lo retransmite.

Para recolectar los datos necesarios para un algoritmo adaptable, el TCP registra la hora en la que se envía cada segmento y la hora en la que se recibe un acuse de recibo para los datos en el segmento. Considerando las dos horas, el TCP computa el tiempo transcurrido, conocido como tiempo ejemplo de viaje redondo o ejemplo de viaje redondo. Siempre que obtiene un nuevo ejemplo de viaje redondeo, el TCP ajusta su noción del tiempo de viaje redondo promedio para la conexión. Por lo general, el software TCP almacena el tiempo estimado de viaje redondo, RTT

(round trip time), como promedio calculado y utiliza nuevos ejemplos de viaje redondo para cambiar lentamente dicho promedio.

En teoría, la medición de una muestra de viaje redondo es trivial –consiste en substraer la hora a la que se envía el segmento de la hora a la que llega el acuse de recibo. Sin embargo, surgen complicaciones debido a que el TCP se vale de un esquema de acuses de recibo acumulativos en el que un acuse se refiere a los datos recibidos y no al caso de un datagrama específico que transporta datos. Considere una retransmisión. El TCP forma un segmento, lo coloca en un datagrama y lo envía, el tiempo termina y el TCP vuelve a enviar el segmento en un segundo datagrama. Como ambos datagramas llevan exactamente los mismos datos, el receptor no tiene forma de saber si un acuse de recibo corresponde al datagrama original o al retransmitido. Este fenómeno se conoce como ambigüedad de acuse de recibo (acknowledgement ambiguity), y se dice que los acuses de recibo TCP son ambiguos.

Si llega un acuse de recibo después de una o más retransmisiones, el TCP medirá la muestra de viaje redondo de la transmisión original y computará un RTT nuevo utilizando la muestra excesivamente larga. Por lo tanto, el RTT más largo resultará en terminaciones de tiempo ligeramente más grandes, por lo que si llega un acuse de recibo después de una o más retransmisiones, el siguiente tiempo de muestra de viaje redondo será aún más largo, y así sucesivamente.

Respuesta al congestionamiento

En la práctica, el TCP también debe reaccionar al congestionamiento en la red de redes. El congestionamiento es una condición de retraso severo causada por una sobrecarga de datagramas en uno o más puntos de conmutación (por ejemplo, en ruteadores): Cuando ocurre un congestionamiento, los retrasos aumentan y los ruteadores comienzan a colocar en las colas de salida a los datagramas hasta poderlos rutear. Debemos recordar que cada ruteador tiene una capacidad finita de almacenamiento y que los datagramas compiten por dicho almacenamiento (por ejemplo, en una red de redes basada en datagramas, no existe una prelocalización de recursos para conexiones TCP individuales). En el peor de los casos, el número total de datagramas entrantes a un ruteador congestionado, crece hasta que el ruteador alcanza su capacidad máxima y comienza a descartar datagramas.

3.2.5 Establecimiento de una conexión TCP

Para establecer una conexión, el TCP utiliza un saludo (handshake) de tres etapas. En el caso más sencillo, este intercambio procede como se muestra en la figura 3.11.

El primer segmento del saludo se puede identificar porque tiene activo el bit SYN en el campo de código. El segundo mensaje tiene tanto el bit SYN como el bit ACK activos, indicando tanto el acuse de recibo del primer segmento SYN como el hecho de que se continúa con el intercambio. El mensaje final del saludo es sólo un acuse de recibo y nada más se utiliza para informar al destino que ambos extremos están de acuerdo en establecer una conexión.

Por lo general, el software TCP en una máquina espera de forma pasiva el intercambio de señales y el software TCP en otra máquina lo inicia. Sin embargo, el saludo (handshake) está cuidadosamente diseñado para funcionar aun cuando ambas máquinas intenten iniciar una conexión al mismo tiempo. Por lo tanto, se puede establecer una conexión desde cualquier extremo o desde ambos al mismo tiempo. Una vez que se establece la conexión desde cualquier extremo o desde ambos al mismo tiempo. Una vez que se establece la conexión, los datos pueden fluir en ambas direcciones por igual. No existe un maestro ni un esclavo.

El saludo de tres etapas es necesario y suficiente para la sincronización correcta entre los dos extremos de la conexión. Para entender por qué, recuerde que el TCP se construye sobre un servicio de entrega no confiable de paquetes, así que los mensajes pueden perderse, retrasarse, duplicarse o entregarse en desorden. Por lo tanto, el protocolo debe utilizar un mecanismo de terminación de tiempo y retransmitir las solicitudes perdidas. Sucederán algunos problemas si las solicitudes originales y retransmitidas llegan mientras se establece la conexión o si las solicitudes retransmitidas se retrasan hasta que se establezca, utilice y termine una conexión. Un saludo de tres etapas (más la regla de que el TCP ignora solicitudes adicionales de conexión después de que se establezca la misma), resuelve estos problemas.

El saludo (handshake) de tres etapas realiza dos funciones importantes. Garantiza que ambos lados estén listos para transferir datos (y que tengan conocimiento de que ambos están listos) y permite, a ambas partes, acordar un número de secuencia inicial. Los números de secuencia son enviados y reconocidos durante el saludo. Cada máquina debe seleccionar un número de secuencia inicial en forma aleatoria que se utilizará para identificar octetos en el flujo que se está enviando. Los números de secuencia no pueden comenzar siempre con el mismo valor. En particular, el TCP no puede seleccionar una secuencia 1 cada vez que crea una conexión (en uno de los ejercicios se examinan los problemas que se pueden originar si se hace de esta manera). Por supuesto, es importante que ambas partes acuerden un número inicial, así como el número de octetos empleados en un acuse de recibo de acuerdo a los utilizados en el segmento de datos.

Para entender cómo pueden acordar las máquinas un número de secuencia para dos flujos después de tres mensajes solamente, recordemos que cada segmento contiene un campo de número de secuencia y un campo de acuse de recibo. La máquina A, que inicia un saludo, transfiere un número de secuencia inicial, x, en el campo de secuencia del primer segmento SYN como parte del saludo de tres etapas. La segunda máquina B, recibe el SYN, registra el número de secuencia y responde enviando su número de secuencia inicial en el campo de secuencia así como un reconocimiento que especifica el octeto x+1 esperado por B. En el mensaje final del saludo, A envía un "acuse de recibo" de la recepción del mensaje de B de todos los octetos a través de y. En todos los casos, los acuses de recibo siguen la convención de utilizar el número del próximo octeto esperado.

Hemos descrito cómo el TCP normalmente transporta el saludo de tres etapas intercambiando segmentos que contienen una cantidad mínima de información. Debido al diseño del protocolo es posible enviar datos junto con los números de secuencia iniciales en los segmentos de saludo. En cada caso el software TCP debe manejar los datos hasta que se complete el saludo. Una vez que la conexión se ha establecido, el software TCP puede liberar los datos manejados y entregarlos rápidamente al programa de aplicación. El lector deberá referirse a las especificaciones del protocolo para obtener mas detalles.

3.2.6 Terminación de una conexión TCP

Dos programas que utilizan el TCP para comunicarse pueden terminar la conversación cortésmente valiéndose de la operación close. De manera interna, el TCP utiliza una modificación del saludo de tres etapas para cerrar conexiones. Recordemos que las conexiones TCP son de tipo full duplex y que hemos visto que éstas contienen dos transferencias de flujo independientes, una en cada dirección. Cuando un programa de aplicación informa al TCP que ya no tiene más datos para enviar, éste cerrará la conexión en una dirección. Para cerrar la mitad de una conexión, el emisor TCP termina de transmitir los datos restantes, espera la recepción de un acuse de recibo y, entonces envía un segmento con el bit FIN activado. El receptor TCP reconoce el segmento FIN e informa al programa de aplicación en su extremo que no tiene más datos disponibles (por ejemplo, mediante el mecanismo de fin de archivo de sistema operativo).

Una vez que la conexión se ha cerrado en una dirección dada, TCP rechaza más datos en esta dirección. Mientras tanto, los datos pueden continuar fluyendo en la dirección opuesta hasta que el emisor se cierra. Por supuesto, los acuses de recibo continúan fluyendo hacia el emisor incluso después de que la conexión se ha cerrado. Cuando ambas direcciones se han cerrado, el software TCP en cada punto extremo borra sus registros de la conexión.

Los detalles del cierre de una conexión son más sutiles de lo que se ha sugerido anteriormente porque el TCP utiliza un saludo de tres etapas modificado para cerrar una conexión. La figura 3.13 220 ilustra el procedimiento.

3.3 Interred, Subred Y Superred

Es necesario recordar que en el esquema de direccionamiento IP cada red física tiene asignada una dirección única; cada anfitrión en la red tiene la dirección de red como prefijo de su dirección individual.
La mayor ventaja de dividir una dirección IP en dos partes surge del tamaño de las tablas de ruteo que necesitan los ruteadores. En vez de almacenar un registro de ruteo por cada anfitrión de destino, un ruteo puede tener un registro por cada red y examinar sólo la porción de red de la dirección de destino cuando tome decisiones de ruteo.

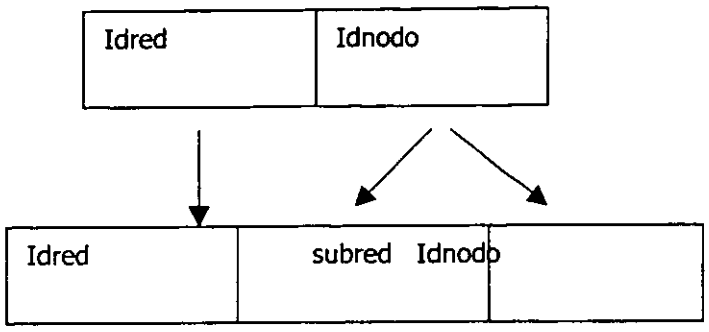
EL TCP/IP incorpora muchos tamaños de red por el hecho de tener tres tipos de direcciones. Las redes que tienen asignadas direcciones A dividen los 32 bits en una porción de red de 8 bits y una porción de anfitrión d e24 bits. Las direcciones de tipo B dividen lo s32 bits en porciones de red y de anfitrión de 16 bits, y las direcciones tipo C dividen la dirección en una porción de red de 24 bits y una porción de anfitrión de 8 bits. Sin embargo, es posible que una localidad pueda asignar y utilizar internamente direcciones IP de manera no usual siempre y cuando:

- Todos los anfitriones y los ruteadores en dicha localidad estén de acuerdo en seguir el esquema de direccionamiento.

- Otras localidades en Internet puedan manejar las direcciones como en el esquema original.

De acuerdo con el modelo original del TCP/IP este fue diseñado para una red con cientos de redes y miles de anfitriones, sin embargo, no se consideran la integración de redes pequeñas de computadoras personales; como ejemplo tenemos Internet, cuyo tamaño se duplica constantemente de tal forma que: se requiere mucho trabajo administrativo para manejar las direcciones de red, las tablas de ruteo de los ruteadores son muy grandes y finamente el espacio para las direcciones se acabará eventualmente. En consecuencia de lo antes mencionado, el problema es importante porque cuando los ruteadores intercambian información de sus tablas de ruteo, la carga de la red de redes es alta, así como también el esfuerzo de software requerido por los ruteadores participantes; adicionalmente el esquema principal de direcciones no puede incorporar prefijos de tipo B para cubrir todas las redes de tamaño mediano en Internet. Para solucionar este problema, se minimizan las direcciones de red, muchas redes físicas deben compartir el mismo prefijo IP de red. Para minimizar las direcciones tipo B, se deben utilizar direcciones tipo C; claro esta, se deben modificar los procedimientos de ruteo y todas las máquinas que se conectan a las redes afectadas deben utilizar las normas utilizadas. La idea de compartir una dirección de red entre muchas redes físicas ha tomado muchas formas, se considero al mencionar en el capítulo anterior el ***proxi*** ARP, así mismo existen los ruteadores transparentes, las subredes IP estándar y el direccionamiento sin tipo, que es asignar muchas direcciones tipo C en vez de direcciones tipo B.

3.3.1 Subredes



Para subdividir una red en subredes se requiere emplear una máscara de bits, llamado máscara de subred. Este determina cuando la dirección IP será empleada para Idred y que tanto será empleado para Idnodo.

Una máscara de subred es una máscara de 32 bits, usualmente escritas en forma hexadecimal. Por ejemplo, para una red clase B se ha seleccionado el tercer byte como subred y el último byte como Idnodo. La máscara sería:

0xffffff00

Con la máscara de subred se realiza la operación lógica AND con la dirección IP. El resultado es el nuevo Idred. Esto es un ejemplo sencillo, pero se puede seleccionar un número diferente de bits para la subred. Además, el número de bits deberá ser constante en toda la clase original. Los ruteadores pueden conectar a redes con máscaras diferentes siempre y cuando sea de otra red lógica

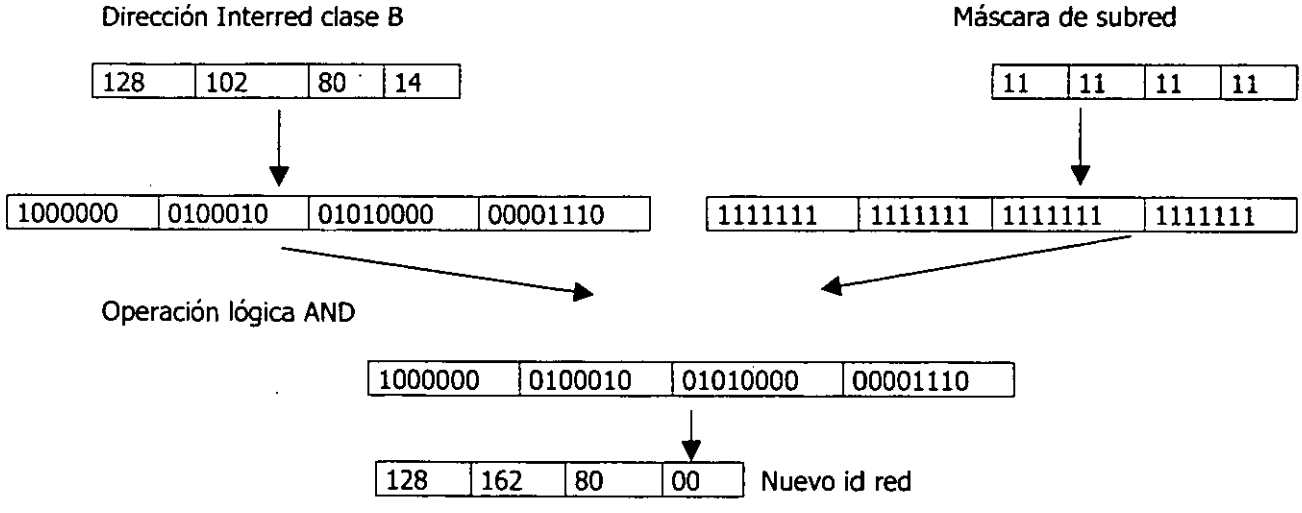


Figura 3.13 Máscara para Subredes

Direccionamiento de una subred

El direccionamiento de subred permite que una sola dirección de red abarque muchas redes físicas y se conoce también como ruteo de subred o utilización de subredes. La utilización de subredes (subnetting) es la más empleada y es la que se ha estandarizado, de hecho el direccionamiento de subred es una parte obligatoria del direccionamiento IP. La manera más sencilla de entender el

direccionamiento de subred es imaginándose que una localidad tiene asignada una sola dirección de red IP tipo B, pero tiene dos o más redes físicas. Solo los ruteadores locales saben que existen muchas redes físicas y como rutear el tráfico entre ellas, los ruteadores en otros sistemas autónomos rutean todo el tráfico como si solo hubiera una red física, en la figura 3.14 se muestra un ejemplo.

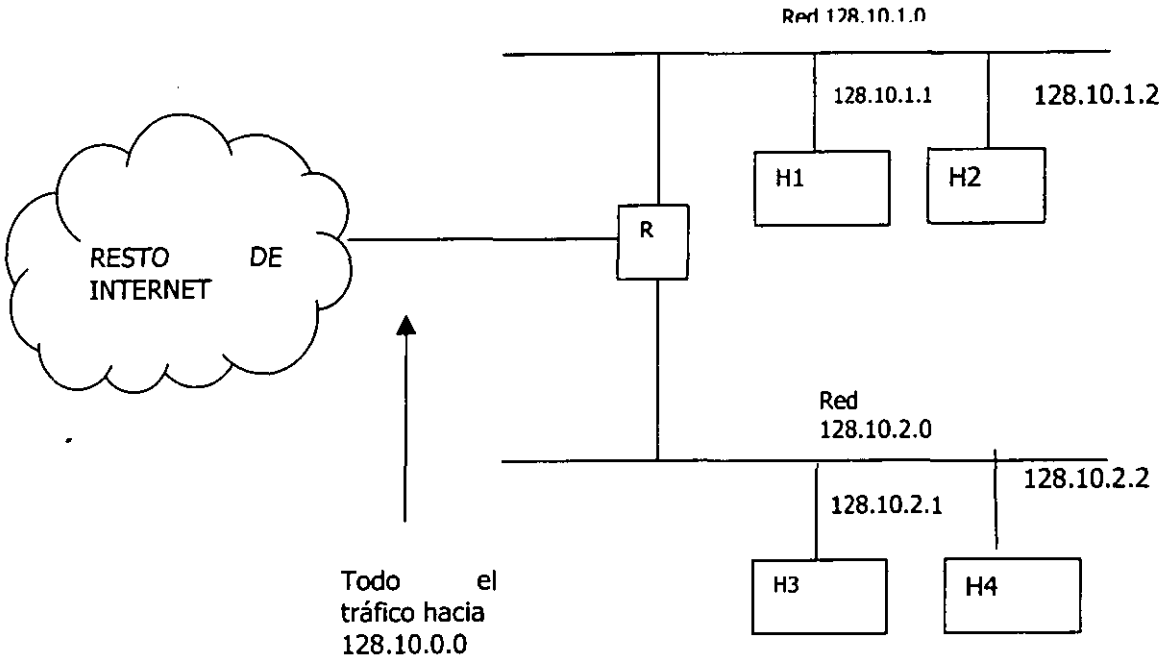


FIGURA 3.14 Direccionamiento de subred

En el ejemplo la localidad sólo utiliza la dirección de red *tipo B 128.10.0.0* para referirse a dos redes. Con excepción del ruteador R, todos los demás rutean como si fueran una sola red física. Una vez que un paquete llega a R, lo debe enviar a su destino a través de la red física correcta. P ara hacer que la elección sea eficiente, el sitio local utiliza el tercer octeto de la dirección para distinguir entre las dos redes. El administrador asigna a las máquinas, en una red física, una dirección con la forma *128.10.1.X* y a las máquinas en la otra red *128.10.2.X,* donde *x* representa un número entero pequeño, utilizado para identificar un anfitrión especifico. Para escoger una red física, R examina el tercer octeto de al dirección de destino, rutea los datagramas que tengan el valor 1 hacia la red *128.10.1.0* y los que tengan el valor de dos hacia la red *128.10.2.0.*

La interpretación de direcciones IP, en las subredes es dividir la dirección en una porción de red y una porción local, es decir, una dirección IP de 32 bits tiene una porción de red de redes y una porción local, en donde la porción de red identifica una localidad, posiblemente con muchas redes físicas, y la porción local identifica una red física y un anfitrión en dicha localidad. La idea básica es interpretar una parte del idnodo de la dirección Internet como **"subred"** y otro como **idnodo.** El mundo exterior interpreta en forma tradicional, peor localmente se emplea en la red subdividida. En el ejemplo anterior, se mostró como el direccionamiento de subred con una dirección tipo B que tenía una porción de red de redes de dos octetos y una porción local de dos octetos; para lograr que el ruteo entre las redes físicas sea eficaz, el administrador de la localidad utilizo un octeto de la porción local a fin de identificar una red física y el otro octeto para identificar un anfitrión en dicha red, como lo muestra la siguiente trama en la figura 3.15.

Parte de Internet	Parte local	
Parte de Internet	Red física	anfitrión

Figura3.15 Utilización del esquema de subred

El resultado es una forma de direccionamiento jerárquico que lleva al correspondiente ruteo jerárquico. El nivel superior de ruteo jerárquico (por ejemplo, otros sistemas autónomos en la red de redes) utiliza los primeros dos octetos cuando rutea y el siguiente nivel (por ejemplo, el sitio local) utilizan un octeto adicional. Finalmente el nivel más bajo (por ejemplo, la entrega a través de una red física) utiliza toda la dirección.

El direccionamiento jerárquico, se muestra de manera clara en el sistema telefónico de los Estados Unidos de América, en donde un número telefónico de 10 dígitos se divide en un código de área de 3 dígitos, una serie de 3 dígitos y una conexión de cuatro dígitos. La ventaja de utilizar direccionamiento jerárquico es que puede incorporarse un gran crecimiento, ya que significa que una ruta no necesita saber muchos detalles sobre destinos distantes, lo mismo que sobre destinos locales. Una desventaja es que seleccionar una estructura jerárquica es difícil como, también, difícil cambia runa jerarquía ya establecida.

El estándar TCP/IP para el direccionamiento de subred reconoce que no todas las localidades tienen la misma necesidad de una jerarquía de direcciones; es decir, permite que se tenga flexibilidad al poder escoger como asignarlas. Para permitir una máxima flexibilidad al particionar las direcciones de subred, el estándar TCP/IP de subred permite que la interpretación se escoja de forma independiente para cada red física. Una vez que se selecciona una partición de subred, todas las máquinas la deben utilizar.

Máscaras para subredes

Para subdividir una red en subredes se requiere emplear una máscara de bits, llamada máscara de subred, está determina cuanto de la dirección IP será empleado para idred y que tanto será empleado para idnodo. Una máscara de subred es un a máscara de 32 bits, usualmente escritas en forma hexadecimal, por ejemplo para una red clase B se ha seleccionado el tercer byte como subred y el último byte como idnodo, la máscara sería:

0xffffff00

Con la máscara de subred se realiza la operación lógica AND con la dirección IP, el resultado es el nuevo idred.

Este es un ejemplo muy sencillo, pero se pueden seleccionar un número diferente de bits para la subred. Además, el número de bits deberá ser constante en toda la clase original. Los ruteadores pueden conectar a redes con máscaras diferentes siempre y cuando sean de otra red lógica.
Ahora en la tabla de ruteo se almacenan 3 entradas pro ruta: el destino, el siguiente ruteador y la máscara de subred.

Haciendo que los formatos se inserten en la tabla de ruteo para todos los casos específicos, se simplifica el algoritmo. Se crea un ciclo iterativo que busca una ruta directa o indirecta, si la

encuentra lo ejecuta y termina el ciclo, sino lo encuentra reporta un error. En muchas ocasiones la ruta default se inserta en la tabla como 0.0.0.0 por simplicidad.

El estándar especifica que una localidad que utiliza el direccionamiento de subred, debe escoger una máscara de subred de 32 bits para cada red. Los bits en la máscara de subred se indican como 1, si la red trata al bit correspondiente de la dirección IP como parte de la dirección de red, y se indica como 0, si se trata al bit como parte del identificador de anfitrión. Por ejemplo, la máscara de subred de 32 bits:

11111111 11111111 11111111 00000000

Específica que los tres primeros octetos identifican a la red y el cuarto a un anfitrión en dicha red. Una máscara de subred puede tener 1 para todos los bits para todos los bits que correspondan a la porción de red de la dirección (por ejemplo, las máscaras de subred para una red tipo b tendrá 1 en los primeros dos octetos) y adicionalmente uno o más bits en los dos últimos. Este giro en el direccionamiento de subredes surge porque el estándar no restringe a las máscaras de subred para que seleccionen bits continuos a la dirección. Por ejemplo, una red puede tener asignada la máscara:

11111111 11111111 00011000 01000000

La cual selecciona los primeros dos octetos, dos bits del tercer octeto y un bit del cuarto. Aunque tal flexibilidad hace posible que se puedan realizar asignaciones interesantes de direcciones, también causa que la asignación de direcciones del anfitrión y que el entendimiento de las tablas de ruteo sea un poco confuso. Por lo tanto se recomienda que las localidades utilicen máscaras contiguas de subred y empleen la misma máscara a lo largo de todo un grupo de redes físicas que compartan una sola dirección IP.

La representación decimal con puntos también es popular para las máscaras de subred; funciona mejor cuando las localidades alinean el direccionamiento de subred en grupos de octetos. Por ejemplo, se asignan direcciones tipo B para subred al utilizar el tercer octeto a fin de identificar *la red física y el cuarto para identificar a los anfitriones, en este caso la máscara de subred tiene* una representación decimal con puntos de 255.255.255.0, lo que facilita su escritura y comprensión.

3.3.2 Superred

El esquema llamado direccionamiento de superred, tiene un enfoque opuesto al de direccionamiento de subred. En vez de utilizar una sola dirección IP de red para muchas redes físicas en una organización, el direccionamiento de superred permite la utilización de muchas *direcciones IP de red para un asola organización. Para entender como funciona el direccionamiento* de superred, considere una organización mediana que se une a Internet. Esta preferiría utilizar una sola dirección tipo B por dos razones:

Una dirección tipo C no puede incorporar más de 254 anfitriones y una dirección tipo B tiene suficientes bits para que el direccionamiento de superred sea conveniente; para conservar los números tipo B, el esquema de direccionamiento de superred asigna a la organización un grupo de direcciones tipo C en vez de un solo número tipo B. el grupo debe ser lo suficientemente grande para numerar todas las redes que eventualmente conectará a Internet, suponiendo que una organización solicita una dirección tipo B, que piensa direccionar por subred utilizando el tercer octeto como campo de subred, en vez de asignar un solo numero tipo B, el direccionamiento de superred asigna a la organización un grupo de 256 números tipo C, para que esta los asigne a las redes físicas.

Asignar muchas direcciones tipo C en vez de una sola tipo B conserva los números tipo B y resuelve el problema inmediato de la terminación de espacio para direcciones. Sin embargo, crea un problema: la información que los ruteadores almacenan e intercambian aumenta dramáticamente. En particular, una tabla de ruteo, en vez de tener un registro por cada organización, contiene muchos registros para cada una.

Una técnica conocida como ruteo sin tipo de inter-dominio (CIDR, Classless Inter-Domain Routing) resuelve el problema. Conceptualmente, la CIDR colapsa un grupo de direcciones contiguas tipo C en un solo registro por dos datos.

(dirección de red, conteo)

En donde la dirección de red es la dirección de la red más pequeña del grupo y conteo especifica el número total de direcciones en grupo. Por ejemplo, el par de datos.

(192.5.48.0, 3)

Se puede utilizar para identificar las tres direcciones de red 192.5.48.0, 192.5.49.0 y 192.5.50.0.

Si unos cuantos proveedores de servicio forman el núcleo Internet y cada un es dueño de un gran grupo de números contiguos de red IP, el beneficio del direccionamiento de superred es evidente, considere registros de una tabla de ruteo del proveedor de servicio P, por supuesto, la tabla debe tener una ruta correcta hacia cada suscriptor de P. la tabla no necesita contener un registro para cada uno de los demás proveedores. El registro identifica el grupo de direcciones del proveedor.

En la práctica la CIDR no restringe los números de red sólo a direcciones tipo C, ni utiliza un conteo de números enteros para especificar el tamaño de un grupo. Por ejemplo, suponiendo que una organización tiene asignado un grupo de 2048 direcciones contiguas, comenzando en la dirección 234.170.168.0. En la tabla de la figura 3.16 se muestran los valores binarios de las direcciones en dichos rangos.

	Notación decimal con puntos	**Equivalencia binaria de 32 bits**
Más baja	234.170.168.0	11101010 10101010 10101000 00000000
Más alta	234.170.175.255	11101010 10101010 10101111 11111111

FIGURA 3.16 Ejemplo decimal con puntos y binario de grupo 2048 direcciones

En la figura anterior la CIDR, requiere que dos valores especifiquen el rango: la dirección más baja y una máscara de 32 bits. La máscara opera como una máscara estándar de subred al delimitar el fin del prefijo. Para el rango mostrado, la máscara CIDR tiene el grupo d e21 bits.

11111111 11111111 11111000 00000000
255.255.248.0

Para hacer uso de todas las direcciones posibles de anfitrión en un rango, los ruteadores en una localidad que utilizan direccionamiento sin tipo se deben cambiar. Cuando el software de ruteo busca una ruta, no interpreta el tipo de dirección de destino. En vez de eso, cada registro en la tabla de ruteo contiene una dirección y una máscara, y el software de ruteo utiliza un paradigma de correspondencia mayor para seleccionar la ruta. Por lo tanto un grupo de direcciones se puede subdividir y pueden introducirse rutas separadas para cada subdivisión. Como resultado, aunque el

grupo de computadoras en una red tendrá asignadas direcciones en un rango fijo, éste no necesita corresponder a un valor binario.

Físicamente las redes están conectadas por un equipo que se conecta a las dos redes. Para asegurar que los nodos en diferentes redes físicas se pueden comunicar, este equipo que conecta a redes físicas envía los paquetes entre las dos redes. Esta tarea es conocida como rutear. El equipo que realiza este trabajo es conocido como ruteador y en terminología de TCP/IP un gateway.

El ruteo se realiza a nivel IP, y los equipos que realizan el ruteo de paquetes de llaman ruteadores IP.

El ruteo se puede dividir en dos tipos: directo e indirecto; cuando dos equipos se conectan en una misma red física, se realiza ruteo directo y los datos se encapsulan en un paquete físico y se envían al nodo destino. Esta es la base de comunicación con TCP/IP. Equipos que no se conectan directamente en el medio físico deben enrutar sus paquetes por uno o más ruteadores; este proceso se conoce como ruteo directo.

El algoritmo de ruteo se basa en una tabla de ruteo, una forma de mantener esta tabla es manualmente, conocido como rutas estáticas.

En casos más complejos, se requiere que los cambios y mantenimiento sean automáticos por programa. Esto se llama ruteo dinámico. La tabla de ruteo tiene entradas en una pareja: destino, siguiente ruteador.

El destino es la dirección Internet de un nodo específico o de una red. El siguiente ruteador es el nombre o dirección de un ruteador directamente conectado a la red que puede rutear tráfico hacia el nodo o la red destino. Existen tres tipos de rutas: específico para nodos, específico para redes o de default (por emisión).

Una ruta especifica para un nodo es empleado para rutear paquetes para un nodo en particular.

Una ruta específica de red es empleada para rutear los paquetes para una red en particular. La ruta default es usada para rutear paquetes que no tienen camino especifico. Todos los paquetes que no son conectados directamente y no tienen una ruta específica se envían al ruteador indicado por la ruta de default.

3.4 Enrutamiento

Dentro de una red en cada máquina en la que entra un paquete se analiza el contenido del *encabezado del paquete y decide su acción con base en la información dentro del encabezado.* Si la dirección de destino del paquete concuerda con la dirección de la máquina el paquete deberá retenerse y procesarse con protocolos de nivel superior. Si la dirección de destino no concuerda con la de la máquina, el paquete se envía adelante por la red. El envío puede ser a la máquina de destino misma o a un gateway o a un puente si el paquete tiene que dejar la red local. El enrutamiento es un contribuyente primario a al complejidad de las redes con packet-switching. Es necesario contar con una ruta óptima de la máquina fuente a la de destino, así como de manejar problemas como una carga pesada en una máquina mediadora o la pérdida de una conexión. Los detalles de la ruta están contenidos en una tabla de enrutamiento y varios algoritmos funcionan con la tabla de enrutamiento para desarrollar una ruta óptima para un paquete. Crear una tabla de enrutamiento y mantenerla con registros válidos son aspectos importantes de un protocolo, los elementos comunes para crear la tabla de enrutamiento son:

- ✓ Se crea una tabla fija con un mapa de la red, la cual debe modificarse y releerse cada vez que haya un cambio físico en cualquier parte de la red.

- ✓ Se usa una tabla dinámica que evalúa la carga y los mensajes del tráfico de otros nodos para afinar una tabla interna.

- ✓ Se usa una tabla de enrutamiento central fija que se carga desde el depósito central, mediante los nodos de red a intervalos regulares o cuando es necesario.

Los métodos antes mencionados tienen sus ventajas y desventajas. El enfoque de la tabla fija, ya sea que se localice en cada nodo de red o, se transfiera a intervalos regulares desde una tabla fija mantenida en forma centralizada, es inflexible y no puede reaccionar con rapidez ante los cambios en la topología de la red. La tabla central es mejor que la primera opción, tan solo porque es posible para un administrador mantener la tabla única con mucha mayor facilidad que una tabla en cada nodo.

La tabla dinámica es la mejor para reaccionar ante los cambios, aunque requiere mejor control, software más complejo y más tráfico de red. Sin embargo, las ventajas por lo general sobrepasan a las desventajas y una tabla dinámica es el método usado con mayor frecuencia en Internet.

3.4.1 Tablas de ruteo

Los ruteadores IP proporcionan interconexiones activas entre las redes. Cada ruteador está conectado a dos o más redes físicas y envía datagramas IP entre estas, acepta datagramas que llegan por medio de una interfaz de red y los rutea hacia otra interfaz. Excepto para los destinos conectados directamente a la red, los anfitriones pasan todo el tráfico IP hacia los ruteadores, los cuales envían los datagramas hacia su destino final. Un datagrama viaja de un ruteador a otro hasta encontrar un ruteador que se encuentre conectado directamente a la misma red en la que se ubica su destino final. Así el sistema de ruteo forma la arquitectura básica de una red de redes y maneja todo el tráfico, excepto en el caso de las entregas directas de un anfitrión a otro. Cada introducción de información en la tabla de ruteo especifica la porción de red de una dirección de destino y establece la dirección de la siguiente máquina a lo largo de una ruta utilizada para alcanzar la red; como en le caso de los anfitriones, los ruteadores entregan directamente datagramas a su destino en la red a la que el ruteador está conectado.

En general el establecimiento de rutas comprende procesos de iniciación y actualización, cada ruteador debe establecer un conjunto inicial de rutas cuando es iniciado y debe actualizar las tablas cuando las rutas cambian.

La diferencia principal entre los ruteadores y los anfitriones comunes es que los anfitriones por lo general saben poco acerca de la estructura de la red de redes a la que están conectados. Los anfitriones no tienen un conocimiento completo de todas las direcciones de destino o todas las redes de destino posibles. De hecho, muchos anfitriones tienen solo dos rutas en su tabla de ruteo: uno para la red local y otra por omisión hacia un ruteador cercano. El ruteador envía todos los datagramas no locales hacia el ruteador local para su entrega. Un anfitrión puede rutear datagramas exitosamente aun cuando sólo cuente con información de ruteo parcial ya que puede basarse en un ruteador.

La tabla de ruteo en un ruteador determinado contiene información parcial relacionada con destinos posibles. El ruteo que emplea información parcial permite que las localidades tengan autonomía para hacer cambios locales de ruteo, pero introduce la posibilidad de que se den inconsistencias, con las que algunos destinos podrían volverse inaccesibles para algunas fuentes.

Se pueden dividir los ruteadores en dos grupos un pequeño conjunto de ruteadores con núcleo INOC y un conjunto extenso de ruteadores sin –núcleo.

3.4.2 Algoritmo de ruteo

- ✓ Obtener la dirección IP del encabezado del paquete
- ✓ Extraer la red destino y la dirección destino.
- ✓ Si la red destino es la misma con que sé esta conectando entonces,
  - Obtiene la dirección física para la dirección lógica
  - Encapsula el datagrama en un paquete físico
  - Envía el paquete
- ✓ Si no si la dirección destino tiene una ruta especifica entonces,
  - Rutea el datagrama según la tabla de ruteo
  - Si no si la red destino tiene una ruta especifica entonces,
  - Rutea el datagrama según la tabla de ruteo
- ✓ *Si no si existe la ruta default entonces,*
  - Rutea el datagrama según la tabla de ruteo

Figura 3.17 Muestra del algoritmo de ruteo

3.4.3 Ruteadores Transparentes

El esquema de ruteador transparente se basa en la observación de que una red que tiene asignada una dirección IP tipo A se puede extender mediante un sencillo truco, que se muestra en la figura 3.18.El truco consiste en hacer que una red física, por lo general una WAN, realice el multiplexado de muchas conexiones de anfitrión a través de un solo puerto, es decir, un ruteador T, de propósito especial, conecta un solo puerto de anfitrión de al red de área amplia (WAN) a una red de área local. T se conoce como ruteador transparente, debido a que los otros anfitriones y ruteadores en la WAN no saben que existe.

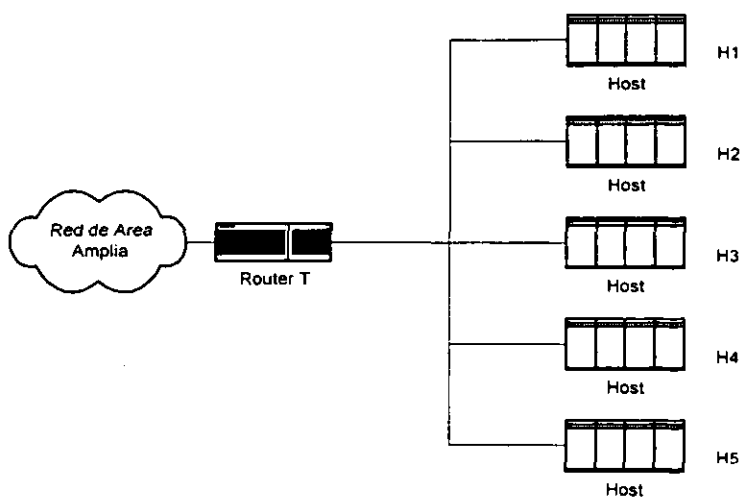


Figura 3.18 ruteador transparente

La red de área local no posee su propio prefijo IP; los anfitriones conectados tiene asignadas direcciones como si se conectaran de manera directa con la WAN; el ruteador transparente realiza el demultiplexado de los datagramas que llegan de la WAN al enviarlos hacia el anfitrión apropiado (utilizando una tabla de direcciones). El ruteador transparente también acepta datagramas de los

anfitriones en la red de área local y los rutea a través de la WAN hacia su destino. Para realizar de manera eficiente el demultiplexado, los ruteadores transparentes a menudo dividen la dirección IP en muchas partes y codifican la información dentro de las partes no utilizadas.

Ventajas y desventajas.

Los ruteadores transparentes tienen ventajas y desventajas cuando se les compara con los ruteadores convencionales. La ventaja principal es que requieren menos direcciones de red, ya que la red de área local no necesita un prefijo IP por separado, además, puede incorporar el balanceo de carga, es decir, si dos ruteadores transparente se conectan a la misma red de área local, se puede dividir el tráfico hacia ellos; en comparación los ruteadores convencionales sólo pueden manejar una ruta hacia cierta red.

Una desventaja de los ruteadores transparentes es que sólo trabajan con redes que tienen un espacio de direcciones grande, de donde escoger la de los anfitriones, por lo tanto trabajan bien con las redes tipo A, y no así con las redes tipo C. otra desventaja es que, como no son ruteadores convencionales, los ruteadores transparentes no proporcionan los mismos servicios, tal como el participar del todo en el ICMP o en el manejo de red con SNMP, por lo tanto, no genera respuestas de eco ICMP (no se puede utilizar ping, para determinar si un ruteador transparente está operando).

3.4.4 Enrutamiento de menos saltos

La mayoría de las redes y gateways hacia Interredes funcionan con la suposición de que la ruta más corta (en términos de máquinas por las que se pasa) es la mejor manera de enrutar los mensajes. Cada máquina por la que pasa un mensaje se llama un salto, de modo que este método de enrutamiento se conoce como menos saltos.
Para proporcionar un enrutamiento de menos saltos se desarrolla una tabla de la distancia entre dos máquinas cualquiera o se dispone de un algoritmo para ayudar a calcular el número de saltos requeridos para alcanzar una máquina objetivo

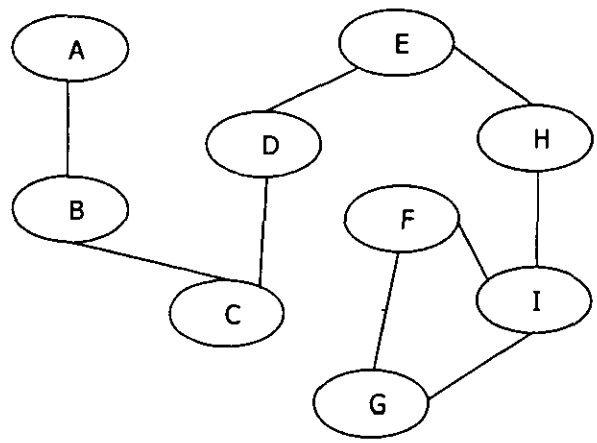


Figura 3.19 Demostración de opciones de ruta menos saltos

	A	B	C	D	E	F	G	H	I
A		1	2	1	2	5	5	3	4
B	1		1	2	3	6	6	4	5
C	2	1		1	2	5	5	3	4
D	1	2	1		1	4	4	2	3
E	2	3	2	1		3	3	1	2
F	5	6	5	4	3		1	2	1
G	5	6	5	4	3	1		2	1
H	3	4	3	2	1	2	2		1
I	4	5	4	3	2	1	1	1	

Tabla 3.3 de menos saltos correspondiente a una subred de gatways

Cuando se va a enrutar un mensaje usando el enfoque de menos saltos se consulta la tabla distancias y se selecciona la ruta con el menor número de saltos. El mensaje sé enruta entonces al gateway que este más cercano a la red de destino. Cuando gateways intermedios reciben el mensaje, ejecutan el mismo tipo de consulta de la tabla y lo envían al siguiente gateway en l a ruta.

En cuanto a las desventajas este método no considera la velocidad de transferencia, las fallas en línea que pueden afectar el tiempo de viaje hasta el destino, es decir, se preocupa por la distancia mas corta aparente sin considerar que es posible algún cambio en las tablas de los gateways que intervienen ya que considera a todas las conexiones iguales.

3.4.5 Enrutamiento por tipo de servicio

Este tipo de enrutamiento depende del tipo de servicio de enrutamiento disponible de gateway a gateway (TOS, Type of Service); y tiene consideración para la velocidad y la confiabilidad de las conexiones, y para factores como la seguridad y la especificidad de la ruta.

Para realizar un enrutamiento TOS, la mayor parte de los sistemas usan actualizaciones dinámicas de las tablas que reflejan condiciones de tráfico y enlace. También toman en cuenta las longitudes de las colas actuales en cada gateway, debido a que la ruta teórica más rápida podría no importar si el mensaje queda atorado en una cola. Esta información se obtiene por medio de la transferencia frecuente entre gateways, en especial cuando se deterioran las condiciones.

La actualización dinámica de las tablas puede tener la desventaja de que si las tablas se actualizan con demasiada frecuencia, un mensaje podría circular a través de una sección de la Interred sin un enrutamiento apropiado hacia su destino o avanzar a través de una ruta larga; por esta razón la actualización dinámica ocurre a intervalos regulares, pero no demasiado frecuentes, par impedir que se extravíen datagramas por circular demasiado en la Interred, es importante la información Time to Live (TTL, Tiempo de Vida) en el encabezado IP del mensaje.

La naturaleza dinámica del enrutamiento TOS, en ocasiones puede causar que fragmentos de un mensaje sean enrutados en formas diferentes hacia su destino. Por ejemplo, sí un mensaje largo de 10 datagramas se está enviando por una ruta, pero las tablas de enrutamiento se cambian durante la transmisión para reflejar un embotellamiento, el resto de los datagramas podrían enviarse por una ruta alterna. Por supuesto, ya sabemos que la máquina de destino reensambla el mensaje en el orden apropiado conforme se reciben los datagramas.

3.5 Ruteo entre Gateways (EXTERNOS)

Los protocolos gateways se utilizan para intercambiar información con otros gateways de una manera rápida y confiable. El uso de protocolos gateway ha demostrado que aumenta el tiempo de transmisión pro interredes grandes (p.e. Internet).

Internet provee dos tipos de gateways: con núcleo y sin núcleo. Todos los gateways con núcleo son administrados por Internet Network Operations Center, los gateways sin núcleo a su vez están fuera del Internet y son operados por grupos externos a Internet como corporaciones e instituciones educativas. El crecimiento de Internet genero la creación del Gateway to Gateway Protocol (GGP), el cual se uso entre gateways con núcleo y su finalidad era difundir información acerca de los gateways sin núcleo, unidos a cada gateway con núcleo, permitiendo crear tablas de enrutamiento.

Dentro de una red, el método de transferencia de información de enrutamiento entre gateways interiores, por lo general es el Routing Information Protocol (RIP; Protocolo de Información de Enrutamiento) o el protocolo HELLO, los cuales son Interior Gateway Protocols (IGP, Protocolos de Gateway Interior). Estos protocolos están diseñados de manera especifica para vecinos interiores. En Internet los mensajes entre dos gateways exteriores son a través del Exterior Gateway Protocol (EGP, Protocolo de Gateway Exterior). RIP; HELLO Y EGP se basan todos en una transferencia frecuente (cada treinta segundos) de información entre gateways para actualizar las tablas de enrutamiento.

3.5.1 Ruteo en subredes

Se debe modificar el algoritmo estándar de ruteo IP para trabajar con direcciones de subred. Todos los anfitriones y ruteadores conectados a una red que utilice el direccionamiento de subred deben emplear dicho algoritmo modificado, al cual se le conoce como ruteo de subred. La regla de subred es que: Para lograr un ruteo óptimo, una máquina M debe utilizar el ruteo de subred para una dirección IP de red N, a menos que exista un solo camino, P, que sea el más corto entre M y cualquier red física que sea subred de N, sin embargo, la regla de subred tiene algunas limitantes, por lo que si una localidad utiliza el direccionamiento de subred, las subredes se deben mantener tan simples como sea posible, es decir, todas las subredes en una dirección IP de red deben ser contiguas, las máscaras de subred deben ser uniformes a través de todas las redes y todas las máquinas deben participar en el ruteo de subred.

El algoritmo modificado de ruteo que se utiliza en las subredes guarda información adicional en la tabla de ruteo. Cada registro dentro de la tabla contiene un campo adicional que especifica la máscara de subred utilizada con la red.

Cuando el algoritmo modificado elige rutas, utiliza la máscara de subred para extraer bits de al dirección de destino y compararlos con registros en la tabla. Es decir, realiza una operación booleana inteligente, y con los 32 bits de la dirección IP de destino así como con el campo de máscara subred de un registro; luego verifica si el resultado es igual al valor del campo de dirección de red en es e registro. Si es así, rutea el datagrama a la dirección especificada en el campo de dirección de salto siguiente del registro.

ALGORITMO
Ruta_IP_Datagrama ((datagrama, tabla_ruteo)
Computar la dirección IP de destino, I_N
Si I_N corresponde a cualquier dirección de red conectada enviar el datagrama a su destino a través de dicha red
De otra forma, para cada registro en la tabla de ruteo hacer lo siguiente
Dejar que N sea el bit-wise-and de Id y de la máscara de subred
Si N es igual al campo de dirección de red del registro, entonces rutear el datagrama a la dirección especificada del salto siguiente
Fin-de- ciclo
Si no se encuentran correspondencias, declarar un error de ruteo

FIGURA 3.20 Algoritmo Unificado de ruteo IP

El algoritmo modificado puede manejar rutas hacia anfitriones individuales, rutas asignadas por omisión y rutas a redes conectadas directamente, utilizando la misma técnica de enmascaramiento, que utiliza para las subredes.

Además, las máscaras pueden manejar rutas hacia redes convencionales. La flexibilidad surge de la capacidad para combinar valores arbitrarios de 32 bits en un campo de máscara de subred, con direcciones arbitrarias de 32 bits, en un campo de dirección de red. Por ejemplo para instaurar una ruta para un solo anfitrión, se utiliza una máscara con todos 1 y con la dirección de red igual a la dirección IP del anfitrión. Para instaurar una ruta asignada por omisión, se utiliza una máscara de subred con todos 0 y una dirección de red con todos 0 (debido a que toda dirección de destino mas 0 es igual a 0). Para instaurar una ruta hacia una red tipo B, estándar y no subred, se especifica una máscara con dos octetos de 1 y dos octetos de 0.

La asignación y propagación de máscaras de subred, se determina de la siguiente manera:

La máscara de subred utilizada en una red local, se propaga cuando una máquina envía un mensaje de solicitud de máscara de subred a un ruteador y recibe una respuesta de máscara de subred. La máquina que hace la solicitud puede enviar directamente el mensaje, si conoce la dirección del ruteador, o transmitir el mensaje por difusión. El formato de un mensaje de máscara de subred se muestra en la siguiente figura:

TIPO (17 Ó 18)	CODIGO (0)	SUMA DE VERIFICACION
IDENTIFICADOR		NUMERO DE SECUENCIA
MASCARA DE DIRECCIÓN		

FIGURA 3.21 Formato del mensaje ICMP de solicitud de máscara de red o de respuesta de máscara de red

El campo TYPE en un mensaje de máscara de dirección especifica si el mensaje es una solicitud (17) o una respuesta (18). Una respuesta contiene la máscara de dirección de subred en el campo ADDRESS MASK. Como es usual, los campos IDENTIFIER y SEQUENCE NUMBER permiten que una máquina asocie las solicitudes con las respuestas.

Por lo general para identificar una red, una localidad selecciona bits contiguos de la porción local de una dirección y utiliza la misma división (por ejemplo, la misma máscara) para todas las redes físicas; muchas localidades utilizan un solo octeto de subred cuando manejan una dirección tipo B.

La difusión en las subredes es más difícil en esta arquitectura, dentro de un grupo de redes con subredes, es posible transmitir por difusión hacia una subred especifica (por ejemplo, transmitir por difusión hacia todos los anfitriones en una red física que tiene asignada una de las direcciones de subred). El estándar de direcciones de subred se vale de un campo de anfitrión de todos 1 para denotar la difusión de subred. Ahora bien, una dirección de difusión de subred es:

{red, subred,-1}

La consideración de las direcciones de difusión de subred así como la difusión de subred, aclara la recomendación para utilizar una máscara consistente de subred a través de todas las redes que comparten una dirección IP de subred. Mientras los campos de subred y de anfitrión sean idénticos, las direcciones de difusión de subred no serán ambiguas. Las asignaciones más complejas de dirección de subred pueden o no permitir la difusión a subgrupos seleccionados de las redes físicas que las comprenden.

Protocolos Gateway IGP y EGP

Los gateways necesitan saber lo que esta sucediendo en el resto de la red, a fin de enrutar datagramas en forma apropiada y eficiente. Esto no solo incluye la información de enrutamiento sino también las características de las subredes. Pro ejemplo si un Gateway es muy lento, pero es el único método de acceso a una subred, otros gateways en la red pueden modificar el tráfico para adaptarlo.

Un GGP se usa para intercambiar información de enrutamiento entre dispositivos. Es importante no confundir la información de enrutamiento (la cual contiene direcciones, topología y detalles sobre demoras de enrutamiento) con los algoritmos usados para hacer la información de enrutamiento. Por lo general, los algoritmos de enrutamiento se fijan dentro de un gateway y no se modifican; por supuesto, conforme cambia la información de enrutamiento, el algoritmo adapta las rutas elegidas para reflejar la nueva información.

Los GGP se utilizan en redes autónomas, y deben considerarse dos clases de gateways; los gateways entre subredes más pequeñas ayudan a unir a los sistemas pequeños en una red corporativa más grande, pero los gateways para cada subred, por lo general están bajo el control de un sistema. Estos gateways se consideran autónomos, debido a que las conexiones entre gateways son constantes y rara vez cambian, estos gateways se comunican por medio de un IGP.

Las interredes grandes como Internet no son tan estáticas como los sistemas autónomos. Los gateways pueden cambiar en forma constante conforme las redes subsidiarias hagan cambios y las rutas de comunicación entre gateways estén sujetas a más cambios. Las comunicaciones entre los gateways son ligeramente diferentes que cuando están conectadas en forma física, estos gateways se comunican por medio de un EGP.

3.6 Protocolo Gateway a Gateway (GGP)

El GGP se utiliza para comunicaciones entre gateways con núcleo para intercambiar información de ruteo. El GGP se diseño para viajar en datagramas IP de la misma forma que los datagramas UDP o los segmentos TCP. Cada mensaje GGP tiene un encabezado de formato fijo que identifica el tipo de mensaje y el formato de los campos restantes. Dado que solo los ruteadores núcleo

participan en el GGP y que estos son controlados por INOC, otros ruteadores no pueden interferir en el intercambio.

El sistema de núcleo fue diseñado para permitir que nuevos ruteadores núcleo se añadieran sin modificar los ruteadores existentes. Cuando se añadía un nuevo ruteador al sistema de núcleo, este era asignado a uno o más núcleos vecinos con los que se comunicaban, los vecinos miembros del, difundían la información de ruteo entre los demás. Así el nuevo ruteador sólo necesitaba informar a sus vecinos sobre las redes que podían alcanzar; estos a su vez actualizaban las tablas de ruteo y difundían la nueva información.

El GGP es un protocolo de vector-distancia, lo que significa que los mensajes tienden a especificar un destino (vector) y la distancia hasta ese destino. Los protocolos de distancia vector también se llaman protocolos Bellman-Ford, para que un protocolo de distancia –vector sea efectivo, un gateway debe tener información completa acerca de todos los gateways en la red; de otra manera, calcular la distancia con un protocolo del tipo menso saltos no puede tener éxito. La información del intercambio de rutas en le GGP consiste en un conjunto pares (N,D) donde N es una dirección de red IP y D es una distancia medida en saltos. Puede decirse que un ruteador que utiliza el GGP anuncia las redes que pueden alcanzar y el costo para alcanzarlas. El GGP mide las distancias en saltos de ruteador, donde un ruteador se define en cero saltos si esta conectado directamente a la red, un salto para redes que están conectadas a través de otro ruteador y así sucesivamente. De esta manera, el número de saltos o el conteo de saltos, a lo largo de una trayectoria de una fuente dada en un destino, se refiere al número de ruteadores que el datagrama encontrará a lo largo de su recorrido.

Ejemplo:

Un gateway establece sus conexiones con otros gateways enviando mensajes, esperando las respuestas y luego creando una tabla. Esto se logra al inicio cuando un gateway se instala y no tiene información de enrutamiento en absoluto. Este aspecto de las comunicaciones no se define dentro del GGP sino se basa en mensajes específicos de red. Una vez que la tabla inicial se ha definido se usa el GGP para todos los mensajes. La conectividad con otro Gateway en Internet se determina usando el método K de N. En este procedimiento un gateway envía un mensaje de resonancia a otro gateway y espera la respuesta, realiza esta tarea cada 15 segundos. De acuerdo con las normas de Internet, si el gateway no recibe 3 (K) respuestas de 4 (N) solicitudes el otro gateway se considera caído, o inutilizable, y los mensajes de enrutamiento no se envían a ese gateway. Si un gateway caído se activa de nuevo, las normas de Internet requieren que se acuse recibo de dos de cuatro mensajes de resonancia. Esto se llama J de M, donde J es dos y M es cuatro. Los valores asignados por Internet para J,K,M y N pueden cambiarse para redes autónomas.

Cada mensaje entre gateways tiene un número de secuencia que se incrementa con cada mensaje transmitido. Cada gateway rastrea su propio número de secuencia para enviarlo a todas las otras gateways que estén conectadas a ella, así como los números de secuencia que llegan de ese gateway; no necesariamente son los mismos, debido a que podrían fluir más mensajes en una dirección que en otra, aunque por lo general cada mensaje debería tener un acuse de recibo o un a respuesta de algún tipo. Los números de secuencia tienen significados importantes para los mensajes y no sólo son para mantener una cuenta creciente del volumen de tráfico. Cuando un gateway recibe un mensaje de otro gateway, compara el número de secuencia en ese mensaje con el último numero de secuencia recibido en sus tablas internas. Si el último mensaje tiene un número de secuencia más alto que el último mensaje recibido, el gateway acepta el mensaje y actualiza su número de secuencia con le último valor recibido. Si el número fue menor que el último número de secuencia recibido, el mensaje se considera obsoleto y se ignora, y se devuelve

un mensaje de error conteniendo el mensaje recién recibido. En la siguiente figura se muestra el proceso.

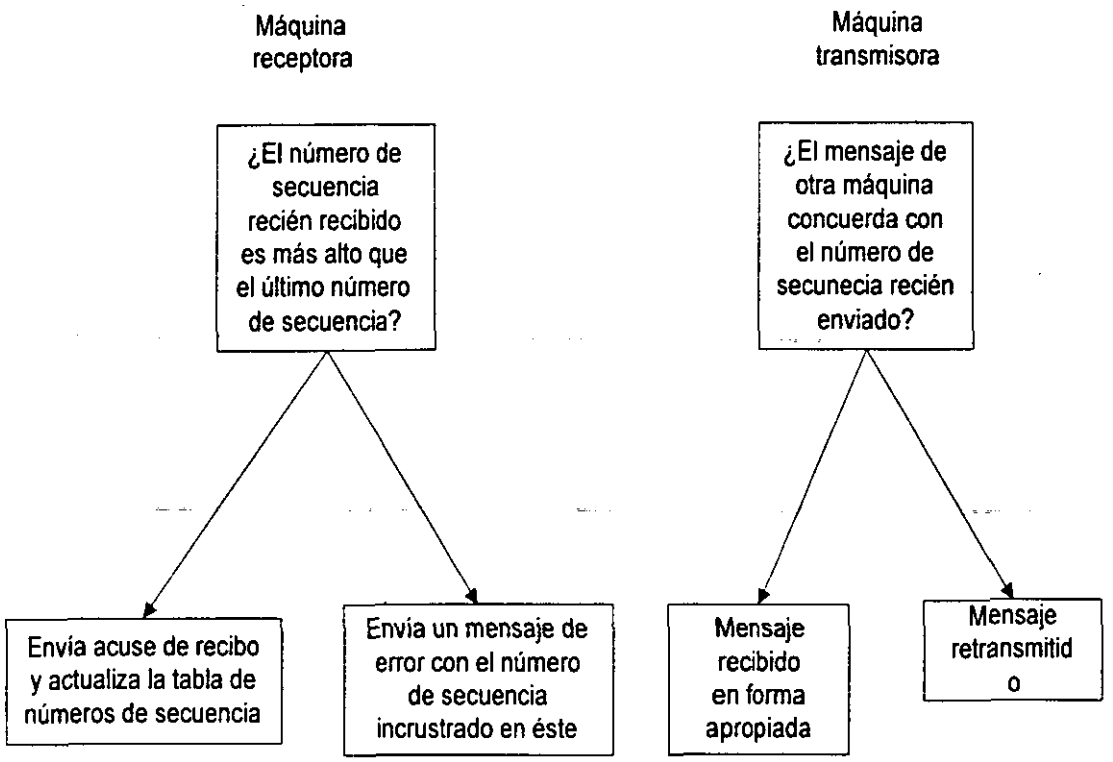


FIGURA 3.22 Números de secuencia de procesamiento en el GGP

El gateway receptor acusa recibo del mensaje recibido, enviando un mensaje de regreso que contiene el número de secuencia del mensaje recién recibido. El otro gateway compara ese número con el número de su último mensaje enviado, y si son iguales, el gateway sabe que el mensaje fue recibido en forma apropiada. Si los números no concuerdan, el gateway sabe que ocurrió un error y transmite el mensaje de nuevo.

Cuando el gateway receptor ignora un mensaje, el gateway transmisor recibe un mensaje con le número de secuencia del mensaje ignorado. Puede determinar entonces cuáles mensajes se omitieron y se ajusta en concordancia, retransmitiendo los mensajes que necesiten enviarse.

3.6.1 Formato de los mensajes GGP

El formato de los mensajes GGP se muestra en la figura 3.23. Después de que se encapsula en un datagrama IP que incluye direcciones fuente y destino. El primer campo es el tipo de mensaje, el cual se fija en un valor de 12 para información de enrutamiento. El número de secuencia se estudio antes y constituye un contador creciente para cada mensaje. EL campo Update (Actualización) está establecido con un valor de 0, a menos que el gateway transmisor desee una actualización del enrutamiento para al dirección de destino proporcionada, en cuyo caso se fija en un valor de 1. El campo number of distance (Número de distancias) contiene el número de grupos de direcciones contenidos en el mensaje actual.

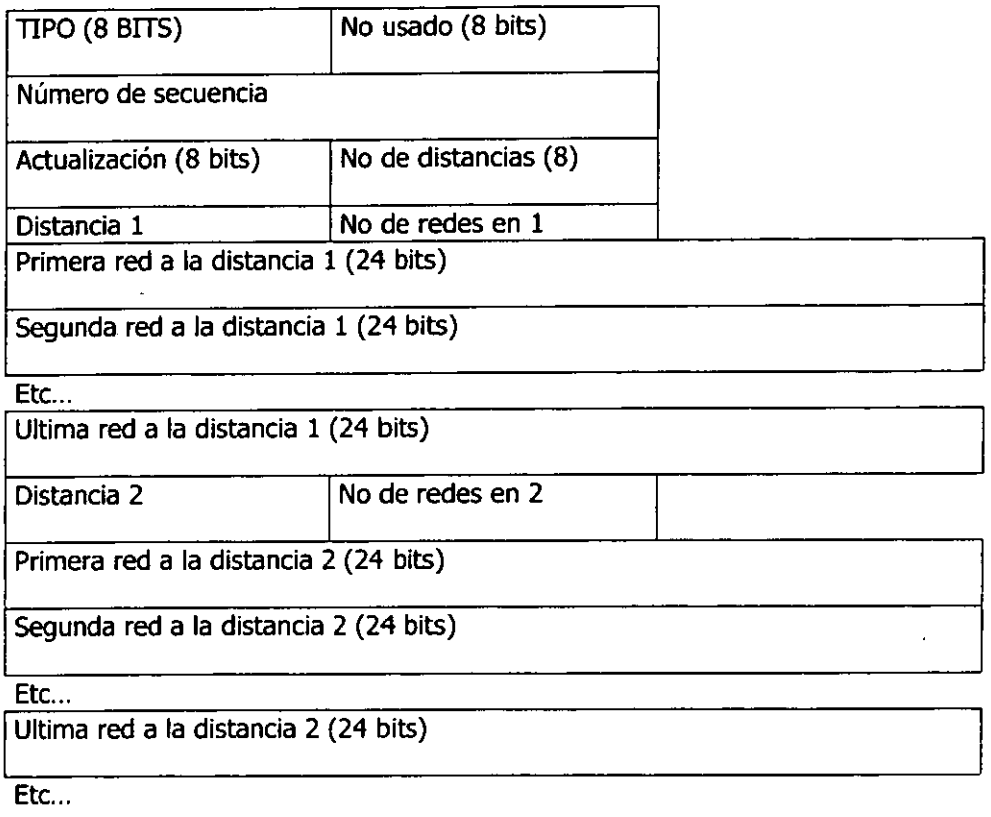


FIGURA 3.23 Formato de los mensajes GGP

Para cada grupo de distancias en el mensaje se proporciona un valor de distancia y el número de redes que puede alcanzarse en ésa, seguidos por todas las identificaciones de al dirección de la red, de acuerdo con la norma GGP, no todas las distancias necesitan reportarse, pero entre más información se proporcione, mayor utilidad tendrá el mensaje para cada gateway.

EL GGP no trata de manera específica con direcciones Internet completas, así que la parte del Host de la dirección no tiene que incluirse necesariamente en la dirección, aunque siempre se proporciona la dirección de la red. Esto puede dar como resultado longitudes diferentes de las direcciones en el campo de identificación (8,16 o 24 bits, dependiendo del tipo de dirección).

Como se muestra en la figura 3.24 se usan otros tres formatos con mensajes GGP, los mensajes de acuse de recibo usan el campo Type, para indicar si el mensaje es un acuse de recibo positivo (el tipo se fija en 2) o un acuse de recibo negativo (el tipo se fija en 10). EL número de secuencia, como se menciono antes se usa para identificar el mensaje al que se aplica el acuse de recibo.

Tipo (8 bits)	No usado (8 bits)
Numero de secuencia (16 bits)	

Acuse de recibo GGP

Tipo (8 bits)
No usado (24 bits)

Solicitud de resonancia y respuesta de resonancia GGP

Tipo (8 bits)
No usado (24 bits)

Estado de interfaz de la red GGP

FIGURA 3.24 Otros formatos del mensaje GGP

Los mensajes de solicitud de resonancia y respuesta de resonancia se pasan entre gateways para informar a éstos de cambios de estado y para asegurar que el gateway está activo. Una solicitud de resonancia tiene el campo Type fijado en un valor de 8, en tanto que una respuesta de resonancia tiene el campo Type fijado en un valor de 0. Debido a que la dirección del gateway transmisor está incrustrada en el encabezado IP, no se duplica en el mensaje GGP, los 24 bits restantes del mensaje no se usan.

El mensaje de estado de interfaz de red lo usa un gateway para asegurar que es capaz de enviar y recibir mensajes en forma apropiada. Este tipo de mensaje puede enviarse al gateway fuente con el campo tipo fijado en un valor de 9 y la dirección IP en el encabezado establecida con al dirección de la interfaz de la red.

3.7 Protocolo Gateway Externo (EGP)

El EGP se usa para transferir información entre gateways vecinos sin núcleo. Los gateways sin núcleo contienen detalles completos acerca de los vecinos inmediatos y las máquinas enlazadas con ellos, pero carecen de información sobre el resto de la red. Los gateways con núcleo saben de todo acerca de los otros gateways con núcleo, pero con frecuencia carecen de los detalles de las máquinas que están más allá de un gateway.

El EGP por lo general está restringido a información dentro del sistema autónomo del gateway; esto impide que pase demasiada información a través de las redes, en especial cuando la mayor parte de la información que se relaciona con sistemas autónomos externos sería inutilizable para otro gateway. Por consiguiente, el EGP impone restricciones a los gateways acerca de las máquinas a las que el EGP pasa información de enrutamiento.

3.7.1 Vecinos

El concepto de "vecino" no significa que las redes deben estar una junta a otra, es decir, están conectadas mediante un gateway, el término vecino tiene que ver con las conexiones, no con la geografía; en una Interred se define de la manera siguiente, los gateways son vecinos si comparten la misma subred; podrían ser gateways par ala misma red o trabajar con redes diferentes. Cuando los dos desean intercambiar información primero deben establecer comunicaciones entre sí; básicamente los dos gateways están de acuerdo en intercambiar información de enrutamiento. Este proceso se llama adquisición de vecino.

El proceso de convertirse en vecino es formal, porque un gateway podría desear no volverse vecino en ese momento en particular (sí esta ocupado por ejemplo). El camino comienza con una Solicitud, la cual va seguida, ya sea por una aceptación (Confirmar) o por un rechazo (Refuse) de la segunda máquina. Si los dos gateways son vecinos, cualquiera puede interrumpir la relación con un mensaje Cease (Cesar).

Después de que dos gateways se vuelven vecinos, se aseguran entre sí de que todavía están en contacto, enviando en forma ocasional un mensaje Hello, al que le segundo gateway responde con un mensaje IHU (heard you/te escucho); tan pronto como sea posible, estos mensajes HELLO/IHU pueden enviarse en cualquier momento. Con varios gateways que participan en una red el número de mensajes Hello puede volverse considerable mientras los gateways continúan permaneciendo en contacto. Este proceso se llama asequibilidad de vecino.

Debido a que el EGP fue ideado para permitir que sistemas intercambien información de enrutamiento y mensajes de estado, el protocolo se basa, sobre todo, en solicitudes o comandos seguidos por respuestas. Los cuatro comandos EGP y sus respuestas posibles se muestran en la siguiente tabla:

Nombre del comando	**Descripción del comando**	**Nombre de la respuesta**	**Descripción de la respuesta**
Request	Solicita que un vecino se vuelva un gateway	Confirm/Refuse	Acepta o rechaza la solicitud
Cease	Solicita la terminación de un vecino	Cease-Ack	Acepta la terminación
Hello	Solicita confirmación de enrutamiento a un vecino (asequibilidad de vecino)	IHU	Confirma el enrutamiento
Poll	Solicita que el vecino proporcione información de la red (asequebilidad de la red)	Update	Proporciona información de la red

Tabla 3.4 Comandos y Respuestas del protocolo EGP

Los mensajes restantes de la tabla sirven para verificar la asequibilidad de la red, en cuyo caso un gateway envía un mensaje POLL (Encuesta) y espera un mensaje Update (Actualización) en respuesta. La respuesta contiene una lista de redes que pueden alcanzarse por medio de ese gateway, con un numero que representa la cantidad de saltos que deben darse para alcanzar las redes. Al ensamblar los mensajes Update de vecinos diferentes, un gateway puede decidir la mejor ruta para enviar un datagrama. Por último, se regresa un mensaje de error siempre que el gateway no puede entender un mensaje EGP que recibe.

3.7.2 Mensajes EGP

La estructura de los diferentes mensajes usados por el EGP se muestran en la figura y los campos tienen los siguientes significados:

- ✓ El campo versión (Versión) contiene el numero de versión del EGP de la máquina transmisora (la versión actual es 2).
- ✓ El campo Type (Tipo) identifica el tipo de mensaje EGP, existen 10 tipos de mensajes en el EGP.

- ✓ El campo Code (Código) contiene un valor que identifica el subtipo del mensaje.
- ✓ El campo Status (Estado) se usa con los campos Type y Code para reflejar el estado actual del gateway.
- ✓ El campo Checksum (suma de verificación) se calcula para el mensaje EGP de la misma manera que en otros encabezados TCP/IP.
- ✓ El System number (número del sistema) es una identificación del sistema autónomo al que pertenece el gateway transmisor.
- ✓ El Sequence Number (número de secuencia) del mensaje es un contador creciente para cada mensaje, usado también para identificar una respuesta a un mensaje previo.

Versión	Tipo	Código	Estado
Suma de verificación		No de sistema	
No de secuencia		Intervalo Hello	
Intervalo Poll			

Adquisición de vecino

Versión	Tipo	Código	Estado
Suma de verificación		No de sistema	
No de secuencia			
Asequibilidad de vecino			
Mensaje error			

Poll

Versión	Tipo	Código	Estado
Suma de verificación		No de sistema	
No de secuencia		No usado	
Dirección IP de la red fuente			

Versión	Tipo	Código	Estado
Suma de verificación		No de sistema	
No de secuencia		Razón	
Mensaje error			

FIGURA 3.25 formato del mensaje EGP

- ✓ El campo Reason (Razón) del mensaje Error puede contener uno de los siguientes enteros:

0 Error no especificado

1 Encabezado EGP malo

2 Campo de datos EGP malo

3 Información de asequibilidad no disponible

4 Polling (encuestamiento) excesivo

5 Respuesta a una encuesta no recibida

Por medio de una combinación de los campos Type, Code y Status, el propósito y significado del mensaje EGP puede determinarse con mayor precisión. La siguiente tabla muestra todos los valores de código y estados.

TIPO	DESCRIPCION	CODIGO	DESCRIPCION	ESTADO	DESCRIPCION
1	Update	0		0	Indeterminado
				1	Activo
				2	Caído
				128	No solicitado
2	poll	0		0	Indeterminado
				1	Activo
				2	Caído
3	Adquisición de vecino	0	Request	0	No especificado
		1	Confirm	1	Modo activo
		2	Refuse	2	Modo pasivo
		3	Cease	3	Recursos insuficientes
		4	Cease-ack	4	Prohibido
				5	Cerrado
				6	Problema de parámetro
				7	Violación de protocolo
5	Asequibilidad de vecino	0	Hello	0	Indeterminado
		1	1 heard you	1	Activo
				2	Caído
8	Error	0		0	Indeterminado
				1	Activo
				2	Caído
				128	No solicitado

Tabla 3.5 Valores de Código y Estado del protocolo EGP

El campo Status puede indicar si un gateway está activo o caído. En el estado caído, el gateway no ejecuta ningún enrutamiento. El indicador de estado Adquisición de vecino puede mostrar si la máquina esta activa o pasiva. Cuando está pasiva, el gateway no genera ningún comando Hello, pero responde a ellos. Al menos un vecino tiene que estar en estado activo para emitir los comandos Hello.

Cuando debe agregarse una lista de redes y sus distancias a un encabezado EGP, se hace en el formato mostrado en la figura 3.26. El número de distancias se especifica en la lista, seguido por registros con el mismo formato que dan la distancia (número de saltos) al gateway, el número de redes que pueden alcanzarse por medio de ese gateway y las direcciones de la red. El número de gateways internos y externos en el encabezado EGP le dice al gateway cuántos registros hay en la lista. Al utilizar el EGP, los gateways pueden actualizarse entre sí y mantener al corriente sus tablas de enrutamiento.

Versión	Tipo	Código	Estado
Suma de Verificación		Numero de Sistema	
Numero de Secuencia		# Int	# Ext
Dirección IP de la red fuente			

Dirección IP del Gateway	
Numero	
Distancia	# Redes
Red 1	
Red 2	

Figura 3.26 Información de enrutamiento en un encabezado EGP

Mensajes de Adquisición de vecino

Un mensaje de Neighbor Acquisition (tipos de mensaje Request, Confirm y Refuse Acquisition) se envía cuando un vecino, se revisa para adquisición. Se usa el mismo formato de mensaje si el mensaje particular es una solicitud, una confirmación o un rechazo.

El tipo se fija en un valor de 3 para indicar que el mensaje es una adquisición de vecino y el campo Code proporciona los detalles del tipo de mensaje Acquisition, como se muestra en la siguiente tabla:

Códigos de mensaje de adquisición EGP

Código	**Descripción**
0	Solicitud de adquisición
1	Confirmación de adquisición
2	Rechazo de adquisición
3	Cesar
4	Cesar acuse de recibo

El campo de status en el encabezado del mensaje Acquisition se establece en uno de ocho valores posibles y se usa para proporcionar mayor información sobre al solicitud. Los valores válidos del campo status se muestran a continuación:

Valores Status del mensaje acquisition del EGP

Código	**Descripción**
0	No especificado; usado cuando ningún otro código es aplicable
1	Modo de estado activo
2	Modo de estado pasivo
3	Recursos disponibles insuficientes
4	Prohibido administrativamente
5	Terminado ya sea pro intervención del operador o porque expira el temporizador
6	Error de parámetro con el mensaje de llegada
7	Violación de protocolo en el mensaje de llegada o el mensaje de respuesta es incompatible con el estado actual de la máquina

El mensaje neighbor Acquisition del EGP agrega dos campos nuevos al encabezado del mensaje EGP básico. El campo Hello Interval de 16 bits especifica el intervalo mínimo entre las encuestas del comando Hello, en segundos. El campo Poll Interval de 16 bits especifica el intervalo mínimo entre las encuestas del comando Poll, también en segundos.

Mensajes de asequibilidad de vecino

Los mensajes Neighbor Reachability se usan para asegurarse que un vecino que fue adquirido con anterioridad está activo todavía y comunicándose. No se agregan campos extra al formato de mensajes EGP básico mostrado en la figura 3.25.

El campo Type se establece con un valor de 5, pero el campo Code tiene un valor ya sea de 0 para un mensaje Hello, o de 1 para una respuestaIHU (I Heard You; te escucho). El campo Status puede tener uno de tres valores, mostrados en la siguiente tabla:

Valores del campo Status de la Neighbor Reachability del EGP

Código	Descripción
0	Indeterminado; usado cuando ningún otro código es aplicable
1	El vecino esta en un modo activo
2	El vecino esta en un estado caído

Mensajes Poll

Los mensajes poll se usan para solicitar información de asequibilidad de red. Al formato del mensaje EGP básico se agregan dos campos extra, los cuales son un campo reservado de 16 bits para uso futuro y un campo IP Source Network (Red fuente IP) de 32 bits.

Los campos Poll tiene el campo Type establecido en un valor de 2 y el campo Code establecido en un valor de 0. El campo status se fija en uno de los mismos tres valores usados en el mensaje Reachability, mostrados en la tabla de arriba.

El campo Reserved de 16 bits unido al final del formato del mensaje EGP básico se ignora en las versiones actuales del EGP. Un campo IP Source Network de 32 bits se usa para especificar la dirección IP de al red acerca de la que esta solicitando información de asequibilidad el gateway.

Mensajes Update

Los mensajes Update se envían como respuesta a un mensaje Poll y proporcionan información *acerca de la asequibilidad de la red. El formato del mensaje Update se muestra en la siguiente* figura 3.28 y es similar al formato GGP.

El Type de un mensaje Update se establece en 1 y el Code en 0. El campo Status se fija en uno de los valores mostrados en la siguiente tabla.

Después de la información conocida del encabezado EGP hay tres campos nuevos. Los campos del número de gateways internos y el número de gateways externos, especifican la cantidad de gateways interiores y exteriores que se reportan en el mensaje, respectivamente. El campo IP Source Network Address contiene la dirección IP de la red con la que se relaciona la información.

Tabla de Valores del campo Status del mensaje Update del EGP

Código	Descripción
0	Indeterminado; usado cuando ningún otro código es aplicable
1	El vecino esta en un estado activo
2	El vecino esta en un estado caído
128	Mensaje no solicitado

versión (8 BITS)	Tipo de mensaje (8 bits)
Código (8 bits)	Estado (8 bits)
Suma de verificación	
No. de sistema (16 bits)	
No..de secuencia (16 bits)	
Numero de gateways internos (8 bits)	No. de gateways externos (8 bits)
Dirección IP de la red fuente (8 a 24 bits)	

Dirección IP del gateway 1 (8 a 24 bits)	
Numero de distancias (8 bits)	distancia 1 (8 bits)
Dirección IP de la red 1 (8 a 24 bits)	

Etc.

FIGURA 3.27 Formato de los mensajes EGP

Después de los tres resúmenes de gateway y el encabezado usual hay una serie o más de información acerca de cada gateway al que esta enviando información el sistema actual. Los cuales se llaman bloques gateway, debido a que cada serie de campos se refiere a un gateway. El primer campo es la dirección IP del gateway. El campo number of distances (Número de distancias) proporciona el número de distancias que se reportan en el bloque gateway y el número de redes que se encuentran a esa distancia. Luego, para cada distancia especificada se proporciona la dirección IP de red de cada red. Muchos bloques de información de gateway pueden proporcionarse en un mensaje Update.

Mensajes Error

EL mensaje EGP final es el mensaje Error, el cual tiene el mismo formato que el mensaje EGP básico, con dos campos agregados. El primer campo de 16 bits está reservado, el que le sigue es un campo de 96 bits que contienen los primeros 96 bits del mensaje que ha generado el error.

3.8 Comunicación entre EGP y GGP

Los gateways con núcleo usan el GGP y los gateways sin núcleo el EGP, de tal modo que debe deber existir un método para que los dos se comuniquen entre sí para encontrar máquinas y redes ocultas que se hallan más allá de sus tablas de enrutamiento. Esto se muestra en la figura 3.28,

donde el gateway A es un gateway con núcleo que conduce de una interred a una red que tiene gateways sin núcleo, que conducen a otras dos redes. Otro gateway en la Interred carece de información acerca de las redes y gateways que están más allá del gateway con núcleo, a menos que se actualice de manera especifica y por medio de una solicitud.

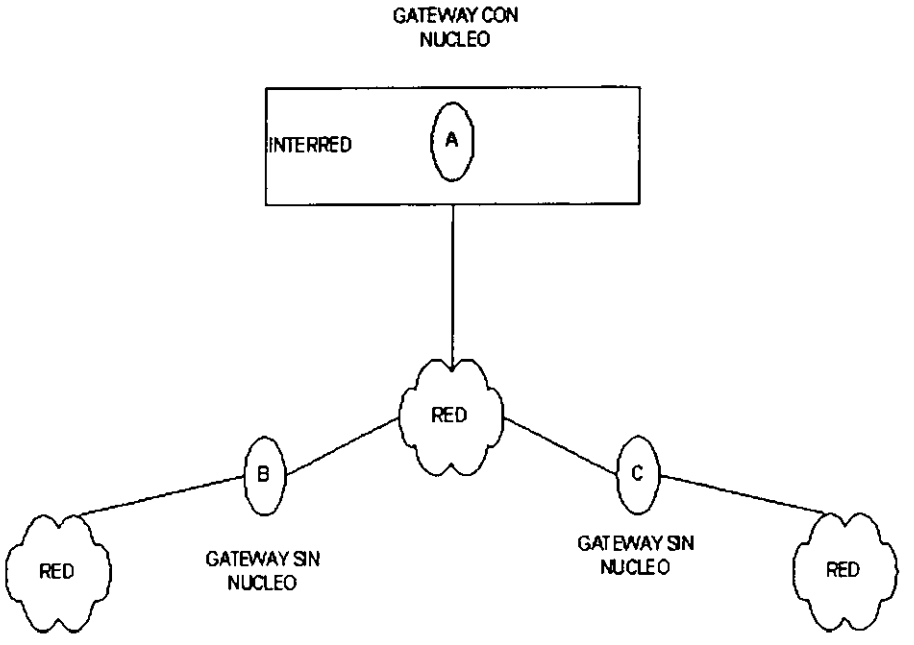


Figura 3.28 Gateways con núcleo y sin núcleo

Internet utiliza un método mediante el cual cualquier gateway autónomo (sin núcleo) puede enviar información de asequibilidad a otros sistemas, la cual debe pasar también al menos por un gateway con núcleo. Si existe una red autónoma más grande, por lo general un gateway asume la responsabilidad para manejar esta información de asequibilidad. En la figura anterior se muestra que el gateway A es el responsable de enviar información acerca de las tres redes que surgen de ella, así como de los dos gateways sin núcleo.

Los EGP usan un proceso de encuesta para mantenerse informados de sus vecinos conforme se activan o se caen y para intercambiar información de enrutamiento y estado con todos sus vecinos. El EGP también es un protocolo controlado por el estado, lo que significa que depende de una tabla de estado que contiene valores que reflejan las condiciones del gateway y un conjunto de operaciones que deben realizarse cuando cambia un registro de la tabla de estado. Existen cinco estados que son los siguientes:

Estado	Descripción
0	Idle
1	Acquisition
2	Down
3	Up
4	Cease

Los significados de cada uno de estos estados EGP son los siguientes:

- ✓ Un estado Idle significa que el gateway no participa en ninguna actividad y que no tiene recursos asignados. Por lo general responde a un mensaje para iniciarse a sí mismo, pero ignora todos los demás mensajes a menos que cambie a un estado Down o a un estado acquisition.

- ✓ Un estado acquisition capacita a un gateway para transmitir mensajes, pero no actúa como un gateway mensajero por completo. Puede recibir mensajes y cambiar a los estados Down o Idle.

- ✓ El estado Down es cuando el gateway no está en operación en lo que respecta a operaciones de encuesta. Los mensajes no se reciben ni se generan.

- ✓ El estado Up se utiliza siempre que un gateway está procesando y respondiendo a todos los mensajes EGP que recibe y puede transmitir mensajes.

- ✓ Un gateway esta en estado cease cuando el gateway cesa todas las operaciones de actualización, pero todavía puede enviar y recibir mensajes Cease y Cease Acknowledgment.

Todos los mensajes EGP quedan dentro de una de tres categorías: Comandos, respuestas o indicaciones. Un comando por lo general requiere que se ejecute una acción, en tanto que una respuesta es una contestación a un comando para ejecutar alguna acción. Una indicación muestra el estado actual. Las señales comando respuesta se muestran en la siguiente tabla:

Comando EGP y sus Respuestas

Comando	**Respuesta**
Request	Confirm
Refuse	ninguna
Error	ninguna
Cease	Cease ack
Error	ninguna
Hello	IHU (I heard you)
Error	ninguna
Poll	Update
Error	ninguna

Variables de estado y temporizadores EGP

En el EGP, el estado actual del sistema depende del último mensaje recibido o de la condición de uno de los temporizadores del software. El EGP mantiene una tabla de estado con varios parámetros que pueden consultarse para determinar acciones. Estos valores por lo general se refieren a demoras entre el envío o la recepción de mensajes de un tipo específico. Además, sé mantiene un conjunto de temporizadores para asegurar que los intervalos entre eventos son razonables. Los parámetros y temporizadores del EGP se muestran en la siguiente tabla usando los nombres empleados en el RFC que define al EGP.

Parámetros y temporizadores del EGP

Nombre	Descripción
M	Modo de encuesta Hello
P1	Intervalo mínimo aceptable entre comandos Hello sucesivos recibidos. El intervalo predeterminado es de 30 segundos.
P2	Intervalo mínimo aceptable entre comandos Poll sucesivos recibidos. El intervalo predeterminado es de 120 segundos.
P3	Intervalo entre transmisiones de comando Request o Cease. El intervalo predeterminado es de 30 segundos.
P4	Intervalo durante el cual las variables de estado se mantienen sin recibir un mensaje de llegada cuando esta en el estado Up o Down. El intervalo predeterminado es de 1 hora.
P5	Intervalo durante el cual las variables de estado se mantienen sin recibir un mensaje de llegada cuando esta en el estado Cease o acquisition. El intervalo predeterminado es de 2 minutos.
R	Recibe el número de secuencia.
S	Envía el número de secuencia.
T1	Intervalo entre retransmisiones del comando Hello.
T2	Intervalo entre retransmisiones del comando Poll.
T3	intervalo durante el cual se cuentan los intentos de asequibilidad.
t1	Temporizador de retransmisión para mensajes request, hello y Cease.
t2	Temporizador de retransmisión para mensajes Poll.
t3	Temporizador Abort (Abortar).

Muchos de los parámetros de estado se determinan durante el establecimiento de una conexión entre vecinos. Las excepciones son los valores P1 al P5, los cuales los establece el sistema Host y no los modifican los vecinos. El número de secuencia de envío se determina solo después de que se ha recibido un mensaje desde el otro gateway.

3.9 Protocolos Internos.

En un sistema autónomo, se utiliza un ruteador para anunciar redes dentro de su sistema a otros sistemas autónomos, es decir se utiliza el EGP (Exterior Gateway Protocol). Ahora cuando un ruteador en un sistema autónomo aprende sobre otras redes dentro de un sistema autónomo; es decir dos ruteadores dentro de un sistema autónomo, se les llama ruteadores internos con respecto de otro. Por ejemplo, dos ruteadores núcleo Internet son interiores en comparación con otro debido a que el núcleo forma un solo sistema autónomo, dos ruteadores en un campus universitario son considerados interiores con respecto a otros mientras las máquinas en el campus estén reunidas en un solo sistema autónomo.

Analicemos el siguiente ejemplo, la figura 3.29 muestra un una red de redes pequeñas la cual cambia lentamente, por lo tanto, los administradores pueden establecer y modificar rutas a mano. El administrador tiene una tabla de redes y actualiza la tabla si una red nueva se añade o se elimina del sistema autónomo, El ruteo para cada red de redes es insignificante porque solo existe una ruta entre cualquiera de los dos puntos. El administrador puede configurar manualmente las rutas en todos los anfitriones y ruteadores, si la red de redes cambia, el administrador debe reconfigurar las rutas en todas las máquinas.

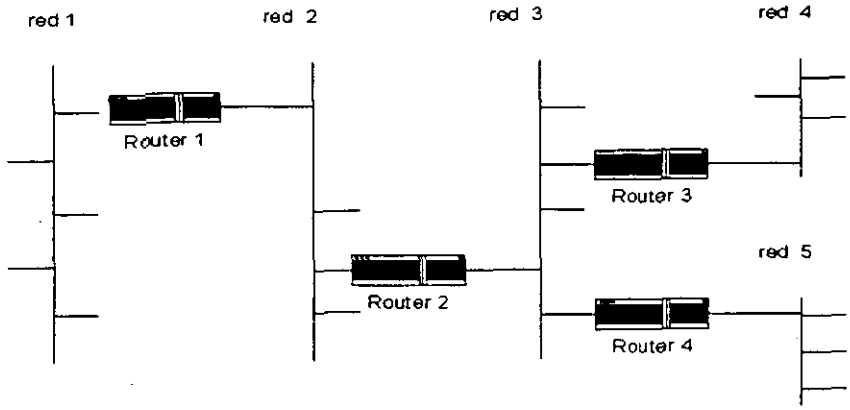


Figura 3.29 cinco redes Ethernet y 4 ruteadores en una red de redes

La desventaja de un sistema manual es obvia; los sistemas manuales no se pueden adaptar al crecimiento o a los cambios rápidos. En un ambiente de cambios rápidos como el de Internet, es necesario hacer esto cambios con métodos automatizados; estos métodos pueden también ayudar a mejorar la confiabilidad y la respuesta a las fallas en pequeñas redes de redes que tienen rutas alternativas, en la figura 3.30 analicemos lo que ocurre cuando se agrega una ruta adicional de red de redes a la figura anterior.

En arquitectura de red de redes que tienen varias rutas físicas, los administradores por lo regular seleccionan una de ellas como ruta primaria. Si el ruteador instalado a lo largo de la trayectoria primaria falla, las rutas se deben cambiar para enviar el tráfico hacia una ruta alternativa, el cambio manual puede ser lento y con errores por lo que se necesitan métodos automatizados para hacerlo de rápidamente y de manera confiable.

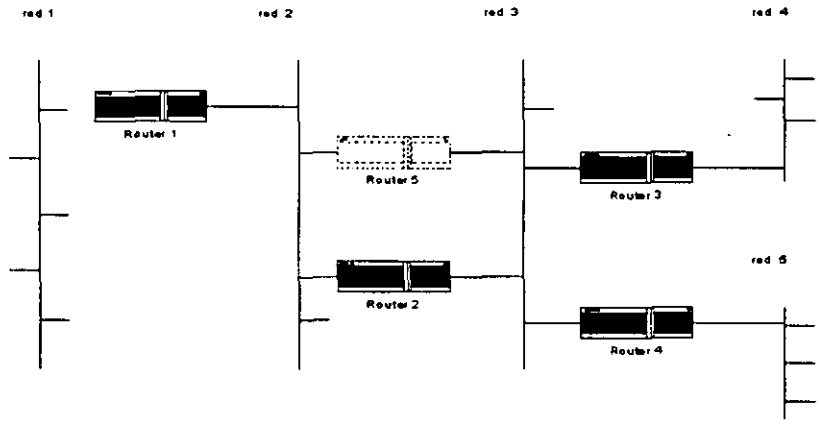


Figura 3.30 cinco redes Ethernet y 4 ruteadores en una red de redes y una ruta alterna entre las redes 2 y 3 con r5

Para automatizar de manera segura el trabajo de información sobre la accesibilidad de una red dada, los ruteadores interiores normalmente se comunican con otros, intercambian información de accesibilidad de red o información de ruteo de red, a partir de la cual la accesibilidad se puede deducir. Una vez que la información de accesibilidad para un sistema autónomo completo se ha ensamblado, uno de los ruteadores en el sistema puede anunciarlo a otros sistemas autónomos utilizando el EGP.

A diferencia de esto la comunicación de un ruteador exterior, para el cual el EGP proporciona un estándar ampliamente aceptado, no se ha desarrollado un solo protocolo que se utilice con los sistemas autónomos. Una de las razones de esta diversidad proviene de la variedad de topologías y tecnologías que se utilizan en los sistemas autónomos, así como el compromiso entre la simplicidad y la funcionalidad, los protocolos que son fáciles de instalar y configurar no proporcionan una funcionalidad sofisticada, ahora en general solo se ha utilizado en la mayoría de los sistemas autónomos un protocolo exclusivo para difundir información de ruteo internamente.

3.10 Protocolo de Pasarela Interior (IGP)

El término (Interior gateway Protocol) IGP se utiliza de modo genérico para referirnos a cualquier algoritmo que utilice ruteadores interiores cuando intercambia información sobre accesibilidad de red o de ruteo. La figura 3.31 muestra un sistema autónomo que utiliza un IGP para difundir accesibilidad entre ruteadores interiores; en la figura IGP1 se remite al protocolo de ruteador interior utilizado dentro del sistema autónomo 2 y adicionalmente un solo ruteador puede utilizar dos diferentes protocolos de ruteo simultáneamente, uno para al comunicación con el exterior del sistema autónomo y otro para la comunicación al interior del sistema autónomo.

En particular, los ruteadores que corren el EGP para anunciar accesibilidad por lo general necesitan correr también un IGP para obtener información desde el interior del sistema autónomo.

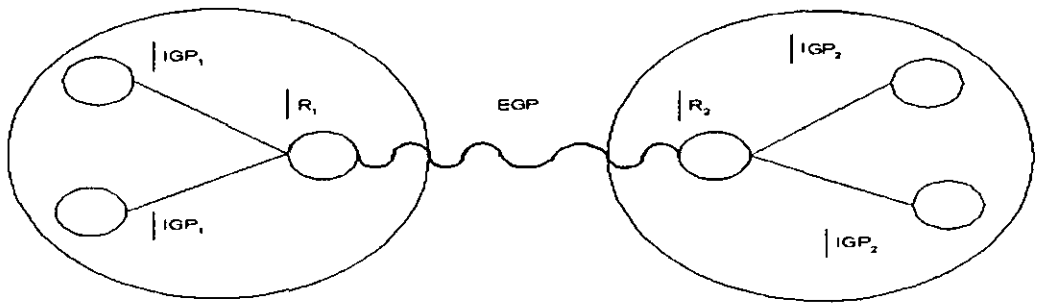


Figura 3.31 Dos sistemas autónomos, y como corren EGP con IGP

3.11 Protocolo de Información de Ruteo (RIP)

Uno de los IGP mas utilizados es el Protocolo de Información de Ruteo (RIP, Routing Information Protocol), y fue diseñado originalmente para proporcionar información consistente de ruteo y accesibilidad entre las máquinas de su red local. Este se apoya en la difusión de red física para realizar el intercambio de ruteo rápidamente, en consecuencia el RIP termina en la implantación del ruteo de vector - distancia para redes locales, es decir, divide las máquinas en activas y pasivas(silenciosas). Los ruteadores activos anuncian sus rutas a los otros; las máquinas pasivas

listan y actualizan sus rutas con base en estos anuncios, pero no anuncian. Solo un ruteador puede correr RIP d e modo activo; un anfitrión debe utilizar el modo pasivo.

Un ruteador que corre RIP de modo activo difunde un mensaje cada 30 segundos; el mensaje contiene información tomada de la base de datos de ruteo actualizada. Cada mensaje consiste de pares donde cada par contiene una dirección de red IP y un entero que representa la distancia hacia esta red. RIP utiliza una métrica de conteo de saltos (hop count metric) para medir la distancia hacia un destino. En la métrica RIP, un ruteador define un salto desde la red conectada directamente, dos saltos desde la red que esta al alcance a través de otro ruteador, y así sucesivamente. De esta manera el número de saltos (number of hops) o el contador de saltos (hop count) a lo largo de una trayectoria desde una fuente dada hacia un destino dado hace referencia al número de ruteadores que un datagrama encontrará a lo largo de su trayectoria. Debe ser obvio, que utilizar el conteo de saltos para calcular la trayectoria más corta no siempre produce resultados óptimos, por ejemplo, una trayectoria con un conteo de saltos igual a tres que cruza tres redes Ethernet puede ser notablemente más rápido que una trayectoria con un contador de saltos igual a dos que atraviesa dos líneas seriales lentas. Para compensar las diferencias tecnológicas, muchas implantaciones RIP permiten que los administradores configuren artificialmente los contadores de saltos con valores altos cuando deban anunciar conexiones hacia redes lentas.

Tanto los participantes RIP activos como los pasivos "escuchan" todos los mensajes difundidos y actualizan sus tablas de acuerdo al algoritmo vector – distancia; en la red de redes de la figura 3.31, el ruteador R1 difundirá un mensaje en la red 2 que contiene el par (1,1), dando a entender que puede alcanzar la red 1 al costo 1. Los ruteadores R2 y R5 recibirán la difusión e instalarán una ruta hacia la red 1 a través de R1 (al costo 2) después, los ruteadores R2 y R5 incluirán el par (1,2) cuando difundan sus mensajes RIP en la red 3. Finalmente todos los ruteadores y anfitriones instalarán una ruta hacia la red 1.

RIP especifica unas cuantas reglas para mejorar el desempeño y la confiabilidad, en el ejemplo anterior, si los ruteadores R2 y R5 anuncian la red 1 al costo 2, los ruteadores R3 y R4 instalarán una ruta a través del que logre anunciarlo primero, estas reglas son las siguientes:

- ✓ Para prevenir que los ruteadores oscilen entre dos o más trayectorias de costos iguales, RIP especifica que se deben conservar las rutas existentes hasta que aparezca una ruta nueva con un costo estrictamente menor.
- ✓ Si falla el primer ruteador que anuncia la ruta, RIP especifica que todos lós escuchas deben asociar un tiempo límite a las rutas que aprenden por medio del RIP. Cuando un ruteador instala una ruta en su tabla, inicia un temporizador para tal ruta. Este tiempo debe iniciarse cada vez que el ruteador recibe otro mensaje RIP anunciando la ruta. La ruta queda inválida si transcurren 180 segundos sin que el ruteador haya recibido un anuncio nuevamente.

RIP maneja tres tipos de errores:

- ✓ En primer lugar, dado que el algoritmo no especifica detección de ciclos de ruteo, RIP debe asumir que los participantes son confiables o deberá tomar precauciones para prevenir los ciclos.
- ✓ En segundo lugar, para prevenir inestabilidades, RIP debe utilizar un valor bajo para la distancia máxima posible (RIP utiliza 16). Así para una red de redes, en la que es válido un contador de saltos de cerca de 16, los administradores deben dividir la red de redes en secciones o utilizar un protocolo alternativo.

Tercero el algoritmo vector – distancia empleado por RIP crea un problema de convergencia lenta (slow convergence) o conteo al infinito (count to infinite), problema en el cual aparecerán

inconsistencias, debido a que los mensajes de actualización de ruteo se difunden lentamente a través de la red. Seleccionando un infinito pequeño (16) se ayuda a limitar la convergencia lenta, pero no se elimina.

La inconsistencia en las tablas de ruteo no es exclusiva de RIP, este es un problema fundamental que presenta cualquier protocolo vector – distancia en el que los mensajes de actualización transportan únicamente pares de redes de destino y distancias hacia estas redes.

3.11.1 Formato del mensaje RIP

Los mensajes RIP pueden ser clasificados, a grandes rasgos, en dos tipos: mensajes de información de ruteo y mensajes utilizados para solicitar información. Ambos se valen del mismo formato, consistente en un encabezado fijo seguido por una lista opcional de pares de redes y distancias El formato se muestra en la siguiente figura 3.32

Figura 3.32 Formato del Mensaje RIP

En la figura el COMMAND especifica una operación de acuerdo con la siguiente tabla:

Comando	Significado
1	Solicitud para información parcial o completa de ruteo
2	Respuesta con distancias de red de pares desde la tabla de ruteo del emisor.
3	Activar el modo de trazado (obsoleto).
4	Desactivar el modo de trazado (obsoleto)
5	Reservado para uso interno de Sun Microsystems.

Un ruteador o anfitrión puede solicitar información de ruteo a otro para enviar un comando request. El ruteador responde a la solicitud mediante el comando response. Sin embargo, en la mayoría de los casos, los ruteadores difunden mensajes de respuesta no solicitados periódicamente. El campo VERSION (versión) contiene el número de la versión del protocolo (actualmente 1) y lo utiliza el receptor para verificar que interpretará el mensaje de manera correcta.

El formato de dirección no está limitado al uso con TCP/IP; puede utilizarse con múltiples conjuntos de protocolos de red, en el formato del mensaje RIP observamos que cada dirección de red reportada por RIP puede tener una dirección de hasta 14 octetos. Por supuesto las direcciones IP necesitan solo cuatro; RIP especifica que los octetos restantes deben ser iguales a cero. El campo FAMILY OF NET i, identifica la familia de protocolo bajo la que la dirección de red deberá interpretarse. A demás de las direcciones normales IP, RIP utiliza la convención de que la dirección 0.0.0.0 denota una ruta por omisión. RIP asocia una métrica de distancia para todas las rutas anunciadas, incluyendo las rutas por omisión. Así, es posible hacer que dos ruteadores anuncien una ruta por omisión a diferentes métricas (esto es una ruta hacia el resto red de redes), haciendo una de ellas de ruta primaria y la otra de ruta de respaldo. El campo final en cada entrada de información en un mensaje RIP, DISTANCE TO NET i, contiene un contador entero de la distancia hacia la red especificada. La distancia es medida en saltos de ruteador, pero los valores están limitados al rango entre 1 y 16, con la distancia 16 utilizada para dar a entender una distancia infinita (esto significa que la ruta no existe).

Transmisión de mensajes RIP.

Los mensajes RIP no contienen un campo de longitud explícito; de hecho RIP asume que los mecanismos de entrega dirán al receptor la longitud de un mensaje entrante, en particular cuando se utiliza con el TCP/IP, los mensajes RIP dependen del UDP para informar al receptor la longitud del mensaje. RIP opera el puerto 520 en UDP, aun cuando una solicitud RIP puede originar otro puerto UDP, el puerto de destino UDP para solicitudes es siempre 520, que es el puerto de origen desde el cual en principio RIP difunde los mensajes.

El uso de RIP como protocolo de ruteo interior limita el ruteo a una métrica basada en contadores de saltos. Casi siempre los contadores de saltos proporcionan solo una medición general de las respuestas de red o de la capacidad que no produce rutas óptimas. Además, calcular rutas con base en el conteo mínimo de saltos tiene la severa desventaja de que hace el ruteo relativamente estático, dado que las rutas no pueden responder a los cambios en la s cargas de la red.

3.12 Protocolo OSPF

El protocolo OSPF es el protocolo estándar de enrutamiento interior para Internet (lo cual no quiere decir que lo adopten todos los Sistemas Autónomos).

El original fue un protocolo de vector de distancia (RIP) basado en el algoritmo Bellman-Ford. Este protocolo funcionó bien en sistemas pequeños, pero sus resultados fueron empeorando a medida que aumentaba el tamaño de los Sistemas Autónomos. Padecía también el problema de conteo a infinito y una convergencia lenta, por lo cual se le reemplazó en mayo de 1979 por un protocolo de estado de enlace. En 1988, se dio a conocer el OSPF (Open Shortest Path First, que abre primero la trayectoria más corta). Se puede consultar este algoritmo del "mínimo esfuerzo", en el RFC 1247. El grupo que diseñó el protocolo, gracias a la larga experiencia con otros protocolos de enrutamiento, tenía una ambiciosa lista de requisitos, los cuales se listan a continuación:

1. El algoritmo tenía que publicarse de libre distribución, sin que ninguna compañía lo patentase (de ahí la 'O' de "OSPF"). Además, la patente de un algoritmo como este, de un uso generalizado en comunicaciones, provocaría todo tipo de inestabilidades, con el consiguiente esfuerzo extra para los desarrolladores de software.

2. Tendría que reconocer una variedad de métricas incluidas distancia física, retardo y otras. (por causas obvias, si consideramos sólo un tipo de distancia, podemos estar mandando la información por un sitio poco eficiente en cuestión de retardos)

3. Tenía que ser un algoritmo dinámico, uno que se adaptara a los cambios de topología rápida y automáticamente.

4. El OSPF tenía que reconocer el enrutamiento basado en el tipo de servicio, o sea, enrutar el tráfico de tiempo real de una manera y otros tipos diferentes de tráfico de otra. El protocolo IP tiene el campo tipo de servicio, pero ningún protocolo existente lo usaba.

5. El nuevo protocolo tenía que equilibrar la carga en las líneas, evitando cargar únicamente la mejor ruta y repartiendo entre las mejores rutas, que en muchos casos, produce una mejora en el rendimiento de la transmisión. Lo que hacían los algoritmos hasta ahora era utilizar únicamente la mejor ruta, mandando todos los paquetes de información por ella, olvidándose de la segunda mejor ruta.

6. Se requería el reconocimiento de sistemas jerárquicos, o sea, que no fuese necesario que el router se supiese de cabo a rabo la topología completa de la red, sino que mediante un mecanismo de jerarquía el router no necesitase conocer toda la topología para poder enrutar la información.

7. Se requería también un mínimo de seguridad para evitar que los estudiantes ociosos burlaran a los enrutadores enviándoles información de enrutamiento falsa (claro que eso lo podían haber arreglado como se arregla aquí: mandándonos prácticas, que así estamos ocupados).

8. También se necesitaba un mecanismo que manejase los enrutadores que se conectasen a Internet a través de un túnel, puesto que los protocolos antecesores no manejaban bien esto.

Dicho esto, la OSPF reconoce tres tipos de conexiones y redes:

- ✓ Líneas punto a punto entre dos enrutadores (o sea, exactamente)
- ✓ Redes multiacceso con difusión (por ejemplo, la mayoría de las LAN)
- ✓ Redes multiacceso sin difusión (por ejemplo, la mayoría de las WAN de conmutación de paquetes)

Una red multiacceso es aquella que puede tener varios enrutadores, cada uno de los cuales puede comunicarse directamente con todos los demás. Los host, normalmente, no desempeñan ningún papel en OSPF, que funciona haciendo una abstracción del conjunto de redes, enrutadores y líneas en un grafo dirigido en el que a cada arco se le asigna una costo que puede ser una distancia, un retardo. Entonces se puede calcular la distancia más corta en base a los pesos de los arcos. Por lo tanto, una conexión en serie entre dos enrutadores se presenta como dos arcos, uno en cada dirección, cuyos pesos pueden NO ser iguales ya que consideramos diferentes factores.

Una red multiacceso se representa con un nodo para la propia red y otro nodo para cada enrutador. Los arcos del nodo de red a los enrutadores tienen un peso de 0 y se omiten en el grafo. El OSPF permite la división de un sistema Autónomo en áreas numeradas. Un área numerada es una red o un grupo de redes contiguas que generalizan el concepto de "subred", y que no se traslapan, pero tampoco son exhaustivas (un enrutador no tiene porqué pertenecer a un área). El OSPF también proporciona un ocultamiento de información de un área fuera de ésta, sus detalles y topología no son visibles fuera. Cada AS tiene un backbone, llamada área 0, a la cual se conectan todas las demás áreas, posiblemente mediante túneles, por lo que se puede ir de cualquier área del AS a cualquier otra mediante el backbone. Un túnel se representa en el grafo como un arco y tiene un costo y cada enrutador que esté conectado a dos o más áreas es parte del backbone. Esta área 0, com. las demás, cumple con el ocultamiento de detalles y topología. Los enrutadores manejan bases de datos de estado de enlace para cada área y ejecutan el

algoritmo de trayectoria más corto (un algoritmo por cada área, al igual que una base de datos por área), teniendo como misión calcular la distancia más corta desde ellos hasta todos los demás enrutador del área, incluyendo el que esté conectado al backbone (al menos uno). La manera en que el OSPF maneja el enrutamiento es a través de tres grafos (costo de rendimiento, de retardo y de confiabilidad), lo cual triplica el procesamiento pero ayuda a optimizar estas tres variables, generando rutas separadas para cada una de ellas. Durante la operación normal pueden necesitarse tres tipos de rutas:

Intraerea: El enrutador origen ya conoce la trayectoria más corta al enrutador de destino y tiene tres pasos:

- ✓ Del ORIGEN al BACKBONE
- ✓ Del BACKBONE al ÁREA DE DESTINO
- ✓ Dentro del ÁREA DE DESTINO, al DESTINO.

Obliga a que se configure en estrella el OSPF, con el Backbone de "centro". InterAS.

El OSPF admite cuatro clases de enrutadores:

- ✓ Enrutadores internos que están contenidos en una sola área.
- ✓ Enrutadores de borde de área que conectan dos o más áreas.
- ✓ Enrutadores de backbone, que están en el susodicho.
- ✓ Enrutadores de frontera de AS que hablan con los enrutadores de otras AS. Se permite la traslapación de estas clases (los enrutadores de borde son parte del backbone, uno que esté en el backbone y no esté en ninguna área más es un enrutador interno...)

3.12.1 Mensajes "HELLO"

En el arranque de un enrutador, este envía menajes "**HELLO**" por todas sus líneas punto a punto y los multitransmite por las LAN al grupo que consiste en todos los demás enrutadores (en las WAN, cada enrutador necesita cierta información para saber con quién tiene que comunicarse). A partir de ahí, cada enrutador aprende quiénes son sus vecinos. El OSPF funciona intercambiando información entre enrutadores adyacentes. Se puede ver claramente que no es eficiente el que todos intercambien información con todos; por eso se declara un enrutador designado, que será el encargado de intercambiar información con sus adyacentes, que son todos los demás enrutadores y un enrutador designado de respaldo por si acaso la principal falla. Los enrutadores vecinos que no son adyacentes no intercambian información entre ellos.

Durante la operación normal, cada enrutador INUNDA periódicamente con mensajes de ACTUALIZACIÓN DEL ESTADO DE ENLACE a todos sus enrutadores adyacentes (indica el estado del enrutador y proporciona los costos usados en la Base de datos topológica). Estos mensajes se reconocen para hacerlos confiables, y tienen un número de secuencia para saber su antigüedad respecto al que se tiene actualmente. Los mensajes de DESCRIPCIÓN DE LA BASE DE DATOS dan los números de secuencia de todas las entidades de estado de enlace guardadas actualmente por el transmisor, y, mediante la comparación de los valores obtenidos con los propios, determinar quién tiene la información más nueva.

En este punto, cualquiera de las partes puede pedir información acerca del estado de enlace de la otra mediante mensajes de SOLICITUD DE ESTADO DE ENLACE, con lo cual cada par de enrutadores adyacentes verifica quién tiene la información más nueva y de esta manera se

distribuye información nueva a través del área. Los mensajes anteriormente citados se envían en paquetes IP (en bruto). Por lo tanto: - Mediante inundación, cada enrutador informa a los demás enrutadores de su área acerca de sus vecinos y sus costos; Esta información permite a cada enrutador crear su propio grafo de costos para cada área a la que pertenezca con el objeto de calcular la distancia más corta (el área de backbone también lo hace). Además, los enrutadores de Backbone aceptan información de los enrutadores de borde de área a fin de calcular la mejor ruta de cada enrutador de backbone a los demás enrutadores, por lo que esta información se propaga de regreso a los enrutadores de borde de área, quienes la divulgan en sus áreas, para así, con esta información, provocar que un enrutador a punto de enviar un paquete interárea pueda seleccionar el mejor enrutador de salida al backbone.

3.13 Protocolo De Pasarela Exterior: BGP

Dentro de un solo AS, el protocolo de enrutamiento es el OSPF (aunque no es el único que se usa). Entre los AS se utiliza un protocolo diferente, el BGP (Border Gateway Protocol). El que se use un protocolo diferente para comunicar las diferentes AS se debe a que las metas de un protocolo de pasarela interior y uno de pasarela exterior son diferentes, puesto que en el exterior, además de la meta de transportar paquetes de datos eficientemente, se han de administrar una serie de requisitos políticos. Por ejemplo, un AS corporativo podría querer ser capaz de enviar y recibir de/a cualquier instalación Internet, pero a lo mejor no quiere transportar paquetes en tránsito de un AS externo que van a otro AS externo, aunque su AS forma parte de la trayectoria más corta. Los intereses económicos (por ejemplo, una compañía telefónica puede estar encantada de que sus clientes utilicen su AS, pero no querrá que los no-clientes lo utilicen) Algunos ejemplos de políticas restrictivas de enrutamiento pueden ser:

1. Prohibición del tráfico en tránsito entre ciertas AS.

2. Nunca poner a Iraq en una ruta que comience con el pentágono.

3. No utilizar a Estados Unidos para llegar de la Columbia Británica a Ontario.

4. Sólo transitar por Albania si no hay otra ruta alternativa hacia el destino.

5. El tráfico que comience o termine en IBM no debe transitar por Microsoft (y nos imaginamos que el de Sun, Corel, Netscape.... tampoco transitará por Microsoft...). Estas políticas se configuran manualmente en cada enrutador BGP, porque no son parte del protocolo Desde el punto de vista de un enrutador BGP, el mundo consiste en otros enrutadores BGP y líneas que los conectan, o sea, dos enrutadores BGP están conectados si comparten una red común.

Para facilitar el manejo de políticas, las redes se dividen en tres categorías:

1.Redes de punta: Solo tienen una conexión al grafo BGP. No se pueden usar para el tráfico en tránsito porque no hay nadie al otro lado.

2.Redes multiconectadas: Estas se podrían utilizar para tránsito, pero se niegan.

3.Redes de tránsito: Como su propio nombre indica, estas se utilizan para tránsito, como los backbone, que están dispuestas a manejar paquetes de datos de terceros, aunque con ciertas restricciones.

Los enrutadores BGP se conectan entre si por medio de conexiones TCP, que proporcionan una conexión confiable y esconden todos los detalles de la red por la que se pasa. El BGP es un protocolo de distancia, pero muy diferente a sus similares (como el RIP). En lugar de mantener

sólo el costo a cada destino, cada enrutador mantiene el registro de la trayectoria seguida. Así, los vecinos transmiten sus trayectorias hacia el destino al enrutador origen, y este evalúa las posibles rutas, eliminando las que pasen por sí mismo y las que impliquen romper alguna limitación política, por medio de un algoritmo que asigna un número a cada "distancia" al destino por esa ruta, asignando un infinito a las que rompan algún protocolo político. El enrutador entonces toma la distancia más corta. Hay que denotar que el algoritmo de ponderación no es parte del protocolo BGP, pudiendo elegir el administrador del sistema la que encuentre más apropiada. El BGP soluciona fácilmente el problema de conteo a infinito que arrastran la mayoría de los algoritmos de enrutamiento, ya que aunque un enrutador vecino caiga, los demás seguirán enviando rutas al destino al enrutador origen, que seguirá teniendo rutas válidas por las que dirigirse. Otros algoritmos se equivocan al elegir rutas, puesto que no pueden saber cuáles de sus vecinos tienen rutas independientes a los destinos y cuáles no. La definición actual del BGP está en el RFC 1654, y se puede encontrar información adicional en el RFC 1268.

3.14 Interacción de redes LAN y redes WAN

Los sistemas de comunicación de datos deben ser capaces de realizar todas las funciones necesarias para permitir la comunicación entre dos o más sistemas, sin importar el hardware usado y deben ser capaces de hacerlo en una forma amigable para el usuario.

Algunos de los principales retos de la comunicación son, la interacción entre las redes de área local (LAN) con las de área amplia (WAN) y la obtención de un sistema de transmisión confiable de información que pueda entregar los datos en forma inteligible al nodo destino y la optimización de los anchos de banda. Los estándares en los que se basan la arquitectura de red con sus capas y protocolos nos ayuda a resolver dichos problemas.

La comunicación de datos comprende dos aspectos principales, el Transporte, el cual involucra todas las funciones relacionadas con la transferencia de datos entre dos usuarios finales y la Manipulación de datos, ya que estos deben ser liberados en una forma inteligible, en algunos casos estos deben ser convertidos.

En cualquier arquitectura de red, el propósito de cada capa es ofrecer ciertos servicios a las capas superiores, liberándolas del conocimiento detallado sobre como se realizan dichos servicios.

La capa ***n*** en un dispositivo conversa con la capa ***n*** de otro dispositivo. Las reglas y convenciones utilizadas en esta conversación se conocen conjuntamente como **protocolo de la capa *n***, como se ilustra en la figura 3.40 para el caso de una arquitectura de red de siete capas.

Los procesos que se llevan a cabo entre capas homólogas de dispositivos diferentes se denominan **procesos de igual a igual (peer to peer)**. Estos procesos son los que se comunican mediante el uso del protocolo. Un **protocolo** es un conjunto de reglas que gobiernan el formato y el significado de las tramas, paquetes o mensajes que se intercambian entre capas homólogas.

En realidad no existe una transferencia directa de datos desde la capa ***n*** de un dispositivo a la capa ***n*** de otro, más bien, cada capa pasa la información de datos y control a la capa inmediata inferior, y así sucesivamente hasta que se alcanza la capa localizada en la parte más baja de la estructura. Debajo de la capa 1 está el medio físico, a través del cual se realiza la comunicación real, es decir, entre capas homólogas se establece una **comunicación virtual**.

Entre cada par de capas adyacentes hay una **interfase,** la cual define los servicios y operaciones que la capa inferior ofrece a la superior. En la figura 3.40 se puede ver la utilización del modelo OSI con los diferentes protocolos e interfases. Cuando los diseñadores de redes deciden el número de capas por incluir en una arquitectura de red, así como lo que cada una de ellas deberá hacer,

una de las consideraciones más importantes consiste en definir claramente las interfases entre capas. Hacer esto, a su vez, requiere que cada capa efectúe un conjunto específico de funciones bien definidas.

El diseño adecuado de una interfase, además de minimizar la cantidad de información que debe pasarse entre capas, hace más simple la sustitución de la implementación de una capa por otra completamente diferente (por ejemplo, reemplazo de líneas telefónicas por canales satelitales). Así todo lo que se necesita de la nueva es que ofrezca exactamente el mismo conjunto de servicios a la capa superior contigua, tal y como lo hacía la antigua implementación.

Una vez que un protocolo es estandarizado se convierte en parte de una **norma** o **recomendación** según sea el caso del organismo que la proponga. Un ejemplo de un protocolo de comunicación está contenido en la recomendación X.25 del I.T.U. que especifica la forma en que una computadora puede comunicarse con una red pública de conmutación de paquetes X.25.

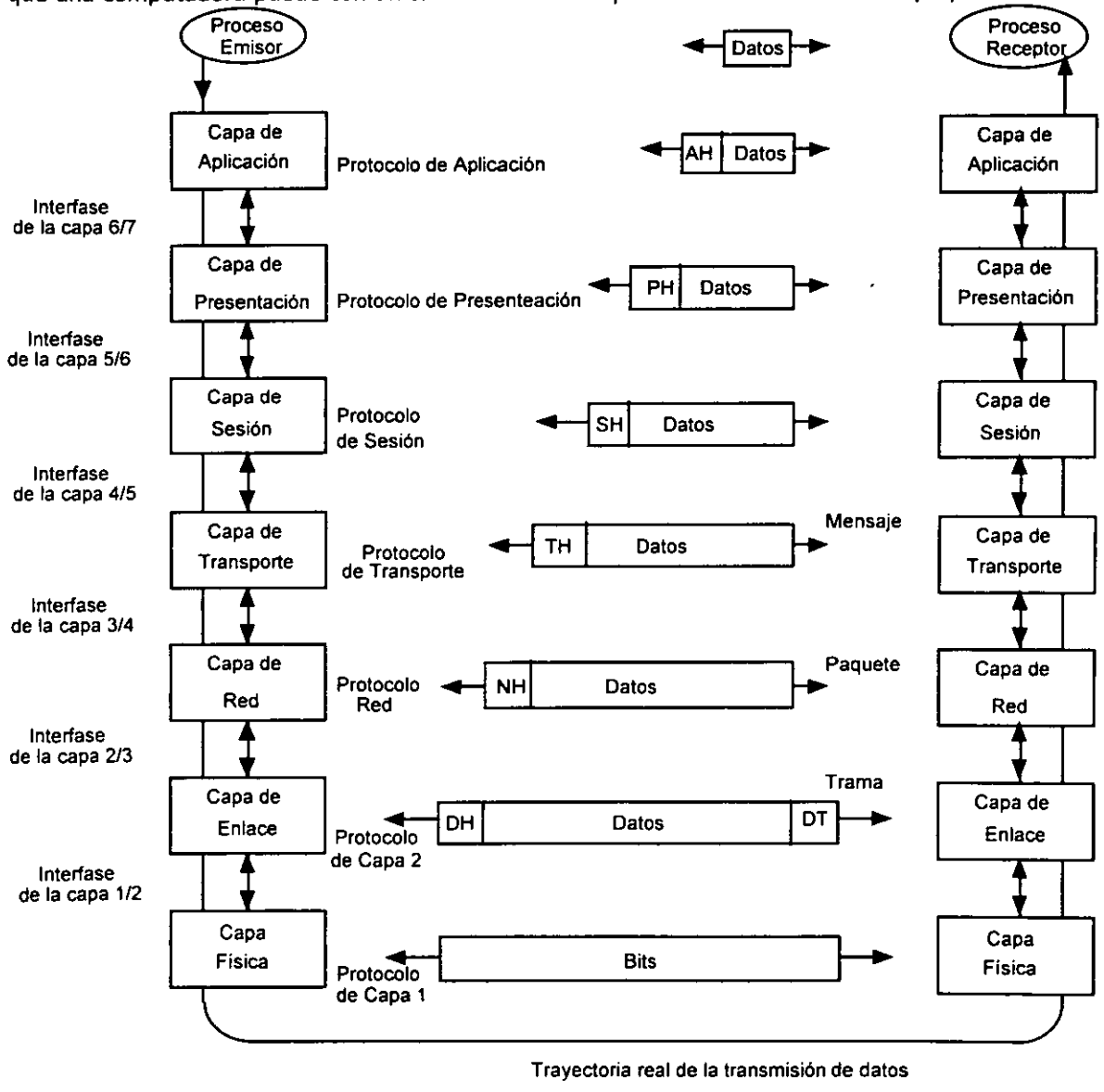


Figura. 3.33 Ejemplo de utilización del modelo OSI (algunos de los encabezados pueden ser nulos).

3.15 Interconexión de Redes

Actualmente, existen varias arquitecturas de red que aunque son compatibles en cierta forma con el modelo OSI no especifican el mismo tipo de capas y los protocolos que utilizan son diferentes. A este tipo de arquitecturas se les llama **propietarias** debido a que están diseñadas tomando en cuenta sólo los productos de un fabricante y no son compatibles con los de otros. Las arquitecturas de red propietarias más conocidas son: **SNA** (**System Network Architecture**) de IBM, **XNS** (**Xerox Network Systems**) de Xerox y **DNA** (**Digital Network Architecture**) o también conocida como **DECNET** de Digital Equipment Corporation.

Varios miles de redes SNA, XNS y DECNET, así como un gran número de redes LAN's de todos los tipos imaginables, están funcionando diariamente en todo el mundo. Muchas de estas redes LAN's no están basadas en el modelo OSI. Para poder interconectar redes y hacerlas interoperables se ha desarrollado diferentes tipos de dispositivos que cumplen funciones específicas y cuya complejidad dependerá fundamentalmente de qué tan parecidas sean las redes por conectar en términos de estructura de tramas, paquetes, mensajes y de protocolos (grado de compatibilidad).

El principal reto de la interconexión de redes es proporcionar el hardware y el software que permitan a dispositivos (computadoras) de diferentes redes comunicarse eficientemente entre ellos. Los dispositivos que interconectan redes son conocidos genéricamente como **relevadores** o **retransmisores** y pueden operar en diferentes capas del modelo OSI.

Existen 4 tipos de relevadores (figura 3.34):

Repetidores: funcionan en la capa física.
Puentes: interconectan redes en la capa de enlace de datos.
Enrutadores: trabajan en las tres primeras capas de modelo OSI.
Compuertas: manejan protocolos de las capas superiores a la de red.

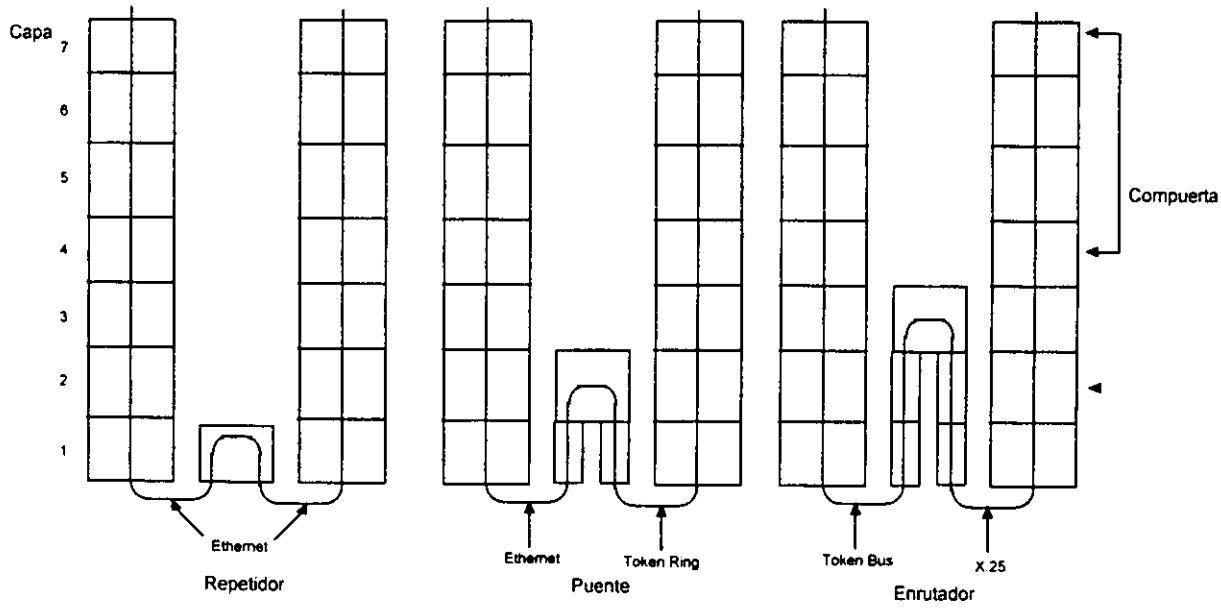


Figura. 3.34 Relación de repetidores, puentes, enrutadores y compuertas con el modelo OSI.

Repetidor Simplemente reexpide bits de una red hacia otra, haciendo que las dos se vean lógicamente como una sola red, es decir, se encarga de recibir, amplificar y transmitir señales en ambas direcciones. A menudo las redes se dividen en dos o más segmentos, como consecuencia de las restricciones de máxima longitud de cable de cada segmento individual. Los repetidores son poco inteligentes (no hay software), sólo copian bits ciegamente sin entender lo que están haciendo.

Una serie de cables conectados por repetidores, no es diferente a un solo cable (excepto por algún retardo introducido por los mismos repetidores).

Puente Puede utilizarse para conectar dos redes en la capa de enlace de datos. Este planteamiento es útil, por ejemplo, cuando las redes tienen la misma capa de red pero difieren en las capas física y de enlace de datos. En una conexión realizada entre una Ethernet y una Token Ring las tramas de Ethernet llegan al puente, en la forma fijada por Ethernet, y se copian en la forma fijada por Token Ring, o viceversa. Los puentes son inteligentes (están diseñados con software), y pueden programarse para copiar tramas en forma selectiva y hacer los cambios necesarios mientras están realizando esa tarea.

Los puentes también pueden ser utilizados como repetidores selectivos para organizar el cableado de una red en una colección de segmentos separados. A diferencia de los repetidores ordinarios, que únicamente se dedican a dejar pasar bits a través de ellos sin que los examinen, los puentes pueden examinar cada trama y sólo reexpedir aquellas que necesitan llegar a otro segmento de la red.

Enrutador Proporciona servicios más sofisticados que un puente debido a que puede seleccionar una de muchas posibles trayectorias para transmitir un paquete. Esta decisión puede estar basada en parámetros como retardo de tránsito, congestión en otros enrutadores, o el número de enrutadores entre el nodo origen y el destino. Además, los enrutadores se utilizan para interconectar dos redes que utilizan la misma capa de transporte y tienen diferentes capas de red por lo que también se denominan **enrutadores multiprotocolos**. Por ejemplo, para una conexión entre una red Token Ring y una red pública X.25, se emplea un enrutador que convierte las tramas de Token Ring a la forma que exige la red X.25.

Compuerta Se emplea para conectarse a una red que no utiliza de ninguna manera, el modelo OSI. En la mayoría de los casos la conexión se tendrá que hacer en la capa de aplicación. También se le llama **convertidor de protocolos**. El término compuerta es frecuentemente utilizado para designar a un enrutador e inclusive un puente en la literatura.

La evolución en la transmisión de datos en los últimos años ha sido importante, se ha pasado de manera muy rápida del escenario de redes locales de datos al escenario de redes de comunicaciones de datos de cobertura amplia (Redes de Area Amplia – WAN). En México hasta la fecha, se ha venido efectuando la interconectividad de las redes locales de datos a través del uso de dorsales (Backbones) ofrecidas por diferentes tecnologías. Las redes de área local se han convertido en la base de las Redes de Area Amplia (WAN), de las Redes de Area Global (GAN), de las Redes de Area Metropolitana (MAN), de las Redes Virtuales (Virtual LANs) y de la misma supercarretera de la información que pretende comunicar al mundo a través de una red global.

Redes de Area Amplia

Una Red de Area Amplia (WAN) es una red de comunicación de datos diseñada para extender locaciones sobre un área amplia, geográficamente dispersa. Un buen ejemplo sería las redes de conmutación de datos privadas o públicas y las redes telefónicas nacionales.

Red de Area Metropolitana

Una Red de Area Metropolitana (MAN) es una red que se extiende en un rango de 50 km., opera a una velocidad desde 1 hasta 200 megabits por segundo y proporciona la conjunción de dispositivos para la transmisión de datos, voz e imagen.

En esta sección explicaremos algunas de las alternativas tecnológicas más utilizadas para redes WAN, como son HDLC, X.25, Frame Relay, RDSI, etc.

Microondas Como una alternativa del cable coaxial, en aplicaciones para comunicaciones de larga distancia, se ha utilizado muy ampliamente la transmisión por radio de microondas.

Las antenas parabólicas de estos sistemas se pueden montar sobre torres para enviar un haz de señales a otra antena que se encuentre a decenas de kilómetros de distancia. Estos sistemas son ampliamente utilizados en transmisiones telefónicas y de video; cuanta mayor altura tenga la torre, más grande será el alcance que se obtenga. Con una torre de 100 metros de altura, por ejemplo, es posible que la señal alcance a transmitirse entre dos torres separadas por una distancia de 100 Km.

La ventaja de las microondas es que la construcción de dos torres resulta, por lo general, más económico que abrir una zanja de 100 Km. de longitud sobre la cual se pueda depositar el cable o la fibra, y posteriormente volver a cubrirla.

Sin embargo, las señales de una antena pueden dividirse y propagarse, siguiendo trayectorias ligeramente diferentes hacia la antena receptora. Cuando estas señales, que se encuentran desfasadas, se recombinan, puede haber interferencia entre ellas, de tal manera que se reduce la intensidad de la señal. La propagación de las microondas también se ve afectada por las tormentas y otros fenómenos atmosféricos.

La transmisión mediante microondas se lleva a cabo en una escala de frecuencias que va de 2 a 40 GHz, correspondiendo a longitudes de onda de 15 y 0.75 cm, respectivamente.

La mayor parte del tráfico relacionado con llamadas telefónicas de larga distancia se realiza en la banda de 4-6 GHz, gracias a que esta banda presenta la menor reducción de la potencia (**atenuación**) de la señal transmitida debido a fenómenos atmosféricos. A medida que se incrementa la frecuencia, la señal se vuelve más directiva (casi inmune a cualquier problema de derivación y obstrucción) pero sufre una mayor atenuación por fenómenos atmosféricos.

Transmisión
Vía Satélite La comunicación mediante satélite tiene algunas propiedades que la hacen atractiva en algunas aplicaciones donde se necesita una gran cobertura geográfica. Este tipo de comunicación puede imaginarse como si un enorme repetidor de microondas estuviese localizado en el cielo. Un satélite está constituido por varios dispositivos receptor-transmisor llamados **transpondedores**, cada uno de los cuales escucha cierto rango de frecuencias, amplificada la señal de entrada y después la retransmite en otra frecuencia. Esta conversión de frecuencia es para evitar interferencias con las señales de entrada.

El flujo dirigido hacia abajo puede ser muy amplio y cubrir una parte significativa de la superficie de la tierra, o bien, puede ser estrecho y cubrir un área de unos cientos de kilómetros de diámetro. Algunos satélites pueden ser reconfigurados mientras están en órbita para cubrir diferentes áreas geográficas.

Actualmente, la mayoría de los satélites de comunicaciones comerciales se encuentran en la **órbita geoestacionaria** o **geosincrónica** (órbita en la cual la velocidad de desplazamiento de un satélite está en sincronía con la velocidad de rotación de la tierra, dando la apariencia de que el satélite está fijo en el espacio) aproximadamente a **36,000 Km.** sobre el ecuador. La órbita geoestacionaria puede solamente dar cabida a 180 satélites.

Con objeto de prevenir un posible caos en el cielo, se han establecido acuerdos internacionales sobre las frecuencias de transmisión satelital. Las bandas de 3.7 a 4.2 GHz y de 5.9 a 6.4 GHz, se han designado como frecuencias de telecomunicación vía satélite, para flujos de información provenientes del satélite o hacia el satélite, respectivamente. En la actualidad estas bandas, a las que en general se les conoce como la **banda 4-6 GHz** o **banda C**, se encuentran superpobladas porque también son utilizadas por los proveedores de servicios portadores para enlaces terrestres de microondas.

La banda superior siguiente que se encuentra disponible para la telecomunicación, es la de **12-14 GHz** o **banda Ku**, la cual no se encuentra todavía congestionada. Sin embargo, existe otro problema: la lluvia. El agua es un excelente absorbente de estas microondas tan cortas. Afortunadamente, las tormentas pueden localizarse con facilidad, por lo que, utilizando varias estaciones terrestres suficientemente separadas, en lugar de una sola, puede resolverse el problema, pagando el costo adicional por el empleo de antenas, cables y partes electrónicas extras, cuya función sería llevar a cabo una serie de conmutaciones rápidas entre estaciones. La banda de frecuencias de **20-30 GHz** o **banda Ka** también se ha reservado para el área de telecomunicaciones, pero el costo del equipo necesario para utilizarla es todavía muy elevado.

Un satélite, por ejemplo, que tenga un ancho de banda de 500 MHz, puede dividirlo en aproximadamente una docena de transpondedores cada uno con un ancho de banda de 36 MHz. Cada transpondedor puede emplearse para transmitir un flujo de información de 50 Mbps u 800 canales de voz digitalizada de 64 Kbps.

Línea Conmutada Refiriéndose al canal de comunicación se habla de una línea conmutada cuando dos nodos distintos se comunican a través de una línea que pasa por centrales de conmutación pública, es decir, que son líneas compartidas virtualmente, esto es que la línea se ocupará solamente el tiempo que dure la conexión, tal línea podrá ser utilizada por otros usuarios cuando se ha terminado esta llamada.

Línea Privada La conexión entre nodos es a través de una línea privada cuando dichas líneas se han rentado a la compañía telefónica para uso exclusivo del usuario. Esta línea no pasa por centros de conmutación pública y por lo tanto no está sujeta a las degradaciones a las que están propensas las líneas conmutadas en los centros de conmutación.

Conexión Punto a Punto Toda línea empleada como conexión en una configuración fija de dos nodos, se denomina conexión punto a punto. En una conexión punto a punto con una línea conmutada, se establece la comunicación y se mantiene hasta finalizada ésta. En el caso de una conexión punto a punto con una línea privada, proporciona el trayecto entre los dos nodos, estén o no en actividad.

Conexión Multipunto La línea multipunto, que usualmente es una línea privada, es compartida en tiempo real por dos o más nodos distantes. La conexión de los distintos nodos se efectúa por **agrupamiento**, cuando se conectan varios nodos a la línea en el mismo punto; por **derivaciones múltiples**, cuando se conectan nodos a la línea en puntos diferentes o por combinación de ambos métodos. Las señales transmitidas por la estación principal son recibidas por todos los nodos distantes o remotos. No obstante, cada mensaje será dirigido a un solo nodo

remoto, que será el único que aceptará efectivamente los datos. Asimismo, los nodos remotos utilizarán la línea por turno para transmitir los mensajes que tengan pendientes.

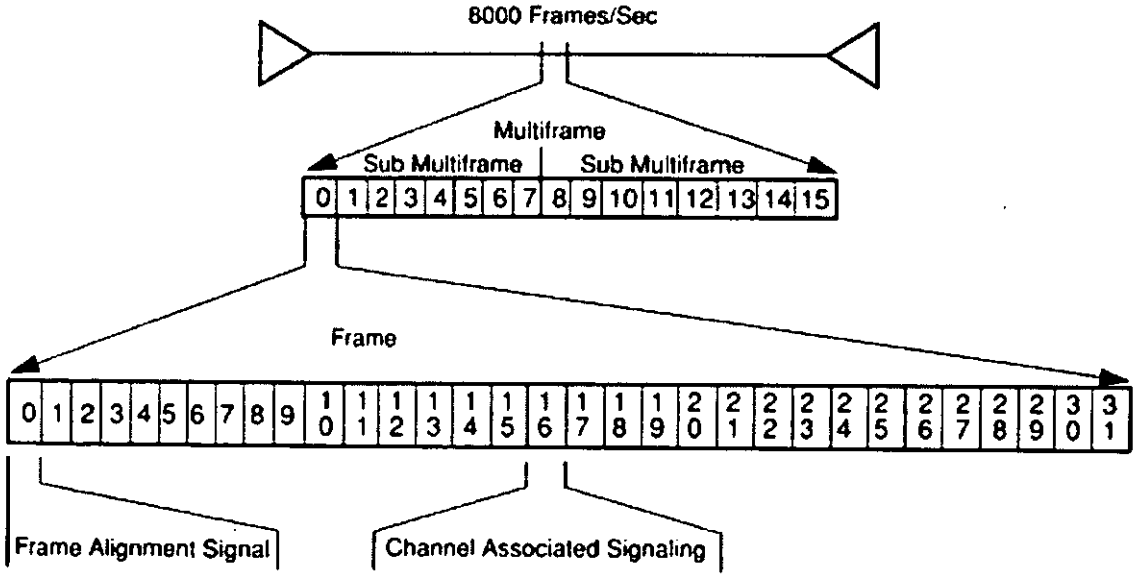
Ancho de Banda Un término muy utilizado en los sistemas de comunicación es el **ancho de banda** del medio de transmisión. El ancho de banda es el rango comprendido entre la menor y la mayor frecuencia que un medio puede transmitir. En un sistema digital, la velocidad de transmisión (expresada en bits por segundo) está íntimamente relacionada con el ancho de banda.

3.16 E1 Clear Channel

Es un sistema de 32 canales, de los cuales necesita uno de ellos para obtener sincronismo y otro para señalización, se deberá transmitir 32 intervalos elementales de tiempo. Un canal es muestreado 8,000 veces por segundo. Cada muestreo es transmitido como un valor de 8 bitios, esto significa que canales individuales tienen una velocidad de transmisión de 64 kbits/seg y que la velocidad total de transmisión para todos los 32 intervalos de tiempo en el sistema es de 2,048 kbits/seg. La estructura de trama está descrita en la recomendación G.704 del ITU.

Algunos de los canales son conectados directamente con un equipo digital, esto significa que la señal, en lugar de estar siendo reconvertida a la forma analógica, es transmitida como un flujo de bitios digital de 64kb/s. Para que la sincronización con este flujo de bitios se consiga, se deberá proveer de una señal de reloj. En la Recomendación G.703 el ITU especifica las interfaces de 64 kbits/seg.

Al sistema mencionado de 32 canales se le llama Sistema de Transmisión E1 Digital (tipo de trama), el cual multiplexa 30 muestras de 8 bits en una sola trama de E1, entonces una muestra ocupa un timeslot o un E0. Estas tramas, por razones administrativas son enviadas a través del medio físico agrupadas en una Multitrama, la cual contiene 16 tramas.



Timeslot 0 – Sincronización
Timeslot 1- 15 – Datos
Timeslot 16 – Señalización
Timeslot –17 – 31 – Datos

Figura 3.35 Trama de transmisión de datos E1

En total, hay 256 bits por trama E1; 240 bits de voz y datos (30 x 8), 8 bits para señalización y 8 bits para sincronismo.

El primer timeslot (timeslot 0) de la trama del E1 contiene el **Byte de Sincronía**. Este byte, para cualquier número de tramas E1 tiene el siguiente patrón, 1001101 (llamada internacional) o 00011011 (llamada normal).

El byte de Sincronía para tramas impares en una multitrama proporciona la sincronización de la trama y los reportes de alarmas. Cada uno de los 8 bits de este byte tiene la siguiente función:

BIT	FUNCION
1	Se utiliza para la trama de revisión CRC-4. Solo se puede usar para llamadas internacionales donde: 0 indica una llamada normal 1 indica una llamada internacional
2	Utilizado para la trama de sincronización. El valor binario del bit 2 alterna para las tramas E1 en una multitrama. Por ejemplo, el bit 2 de un byte de sincronismo para la primera trama E1 será 1; el bit 2 de un byte de sincronismo para la segunda trama E1 será 0 y así sucesivamente.
3	Utilizado para el Indicador de Alarmas Remotas (RAI), donde un valor binario de: 0 indica operación normal 1 indica pérdida de alineación de trama
4 – 8	Bits reservados utilizados para llevar mensajes propietarios.

La velocidad del E1 es de 2.048 Mbits/segundo o 2,048,000 bits/segundo, esto se determina por:
Muestreando a 8000 veces/seg x cada muestra de 8 bits = 64000 bits/seg

X 32 timeslots por trama
2,048,000 bits/seg.

3.17 Redes X.25

En los años 1970´s, cinco naciones planearon construir redes públicas de datos, estas naciones fueron Francia, Japón, Estados Unidos de América, Canadá e Inglaterra. Para que el desarrollo de una red de conmutación de paquetes fuera exitosa se necesitaba una interfase estándar entre el usuario y la red que cumpliera ciertos requerimientos básicos:

- ✓ Proveer una trayectoria de transmisión full duplex entre el usuario y la red.
- ✓ Asegurar la integridad y la exactitud de los datos transmitidos entre el usuario y la red.
- ✓ Proporcionar conexiones virtuales permanentes y conmutadas.
- ✓ Soportar eficientemente comunicaciones concurrentes de los dispositivos del usuario sobre un mismo circuito físico hacia la red.
- ✓ Permitir que el usuario y/o la red controlen el flujo de datos sobre el circuito de acceso, de modo que uno no afecte al otro.
- ✓ Proporcionar funciones de supervisión y control para administrar las llamadas satisfactoriamente.

Esta propuesta de interfase se puso a consideración del entonces CCITT (ahora ITU) y fue aprobada como la **recomendación X.25** en 1976. Esto proporcionó un conjunto de acuerdos en el formato, significado y tiempo relativo de intercambio de información entre dos dispositivos de

una red de conmutación de paquetes. La recomendación X.25 ha sido revisada en 1980, 1984, 1988, 1992 y así sucesivamente.

Esta recomendación está definida para los tres primeros niveles del modelo OSI: físico, de enlace de datos o tramas y de red o paquetes.

X.25 es el protocolo que debe utilizarse para la conexión de terminales que operan en modo paquete a una red pública de transmisión de datos con conmutación de paquetes (por ejemplo, TELEPAC). Las redes de área amplia actuales, deben usar la red pública para lograr la comunicación a larga distancia.
La recomendación X.25 maneja generalmente velocidades desde 1200 bps hasta 64 Kbps (en algunos países se ofrecen accesos a 2 Mbps), por lo que es muy utilizada en aplicaciones transaccionales y solicitudes de información de volumen moderado.

Debido a que la recomendación X.25 fue diseñada para soportar accesos analógicos por medio de par de cobre (Red Telefónica Pública Conmutada) contiene algoritmos de supervisión muy robustos.

3.17.1 Relación entre X.25 y el Modelo OSI

La recomendación X.25 define la interfase entre una computadora (host), al que el ITU generalmente llama **DTE** (Equipo terminal de datos), y el equipo del operador, conocido como **DCE** (Equipo terminal de circuito de datos). A un conmutador interno de la red se le nombra **DSE** (Equipo de conmutación de datos).

X.25 especifica el formato y significado de la información intercambiada a través de la **interfase DTE-DCE** para los protocolos de las capas 1, 2 y 3 del modelo OSI (fig. 3.36). Dado que mediante la interfase se separa el equipo del operador del equipo del usuario, es muy importante que la interfase quede cuidadosamente definida.

Es importante mencionar que X.25 es local para la interfase entre el DTE (host), y el DCE (nodo de la red). El procedimiento seguido entre los DCE´s se llama protocolo de red interno y depende de cada implementación de red. El protocolo de red interno no está especificado por el ITU, sin embargo, cada implementación de éste deberá mantener el significado y el formato de X.25 a través de la red.

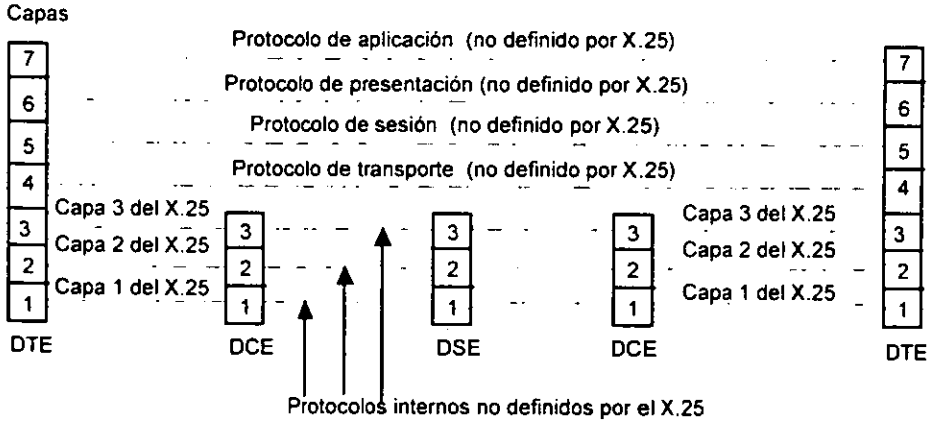


Fig. 3.36 Relación entre X.25 y el Modelo OSI.

La recomendación X.25, como se mencionó anteriormente, consiste de tres capas o niveles de procedimientos de control directamente relacionados con el modelo OSI:

Nivel físico.
Nivel de enlace de datos.
Nivel de paquete o red.

Cada capa es funcionalmente independiente de las otras capas, con la excepción de que una falla en una de las capas puede afectar la operación de las capas más altas.

Las capas actúan en áreas claramente definidas. Esto permite modificaciones en una capa sin alterar las otras. Estas tres capas proporcionan bases sólidas para el diseño de procedimientos en capas más altas para conexiones DTE-DTE.

3.17.2 Especificación X.21 y X.21 bis de la Capa Física

La capa 1 de la recomendación X.25 está relacionada con la interfase eléctrica, mecánica, funcional y de procedimiento entre el DTE y el DCE. En realidad, X.25 no define estos aspectos, sino más bien hace referencia a dos normas, la **X.21** y **X.21** ***bis***, las cuales definen a las interfases digital y analógica, respectivamente. El X.21 *bis* es una norma provisional, para ser utilizada en redes analógicas hasta que las redes digitales estén fácilmente disponibles. Es fundamentalmente el RS-232-C.

La interfase de señalización digital X.21 especifica la manera en que el equipo del cliente, el DTE, establece y libera las llamadas, mediante el intercambio de señales con el equipo del proveedor de servicios portadores, el DCE. En la figura 3.37, se dan los nombres y las funciones de los ocho circuitos definidos para la X.21. El conector físico tiene 15 pines, pero no todos se utilizan. El DTE utiliza las líneas *T* y *C* para transmitir los datos y controlar la información, respectivamente. La línea *C* es similar a la señal de colgar y descolgar de un teléfono. El DCE utiliza la línea *R* para transferir datos y la línea *I* para el control de llamadas. La línea *S* contiene la señal emitida por el DCE para proporcionar información de temporización, de tal forma que el DTE conozca el momento en que cada uno de los intervalos de bit comienza y termina. Como una opción del proveedor del servicio portador, se puede tener una línea *B* para agrupar los bits en tramas de 8.

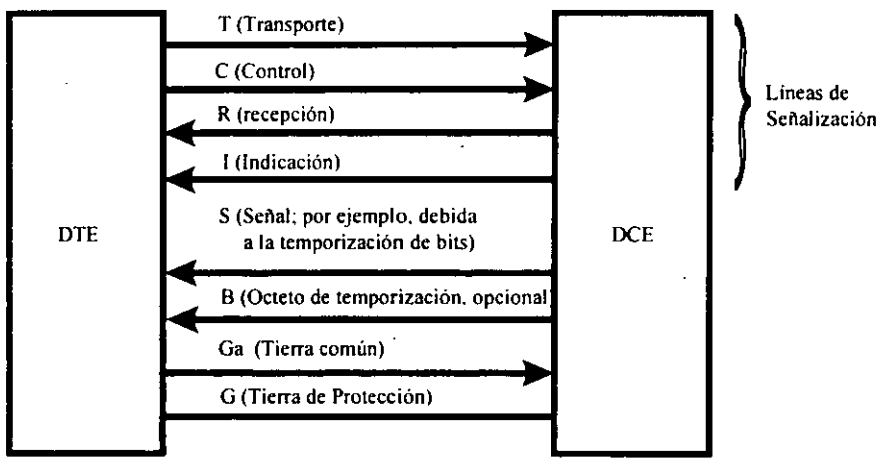


Fig. 3.37 Circuitos utilizados en X.21.

Las líneas *T, C, R* e *I* se denominan líneas de señalización. Estas líneas pueden tomar un valor de uno para indicar que están apagadas (estado off) o un valor de cero para expresar que están encendidas (estado on).

El protocolo de esta capa detalla, como se indicó antes, todos los pasos que se deben seguir para el establecimiento y liberación de llamadas, por ejemplo, define que cuando no hay ninguna llamada, las cuatro líneas de señalización deben estar a 1, cuando el DTE desea hacer una llamada debe poner *T* y *C* a cero (que es un procedimiento análogo al seguido por una persona que descuelga el teléfono para hacer una llamada), etc.

3.17.3 Protocolo LAPB de la Capa de Enlace de Datos

La tarea de la capa 2 consiste en asegurar que se lleve a cabo una comunicación fiable entre el DTE y el DCE, aún cuando éstos puedan estar conectados a través de una línea telefónica ruidosa. El protocolo que se utiliza es el **LAPB** (Procedimiento de acceso al enlace B). Este protocolo se deriva del protocolo desarrollado por IBM para la capa de enlace de datos de su arquitectura de red SNA (Arquitectura de red de sistema), conocido como **SDLC** (Control de enlace de datos síncrono).

IBM después de desarrollar este protocolo, lo envío al ANSI para que fuera aceptado como una norma en Estados Unidos de América y a la ISO para que lo fuera internacionalmente. La ANSI lo modificó para generar el **ADCCP** (Procedimiento de control de comunicación de datos avanzado); así mismo la ISO lo modificó para llegar a tener el **HDLC** (Control de alto nivel de enlace de datos). Posteriormente, el ITU adoptó y modificó el HDLC para dar lugar a su **LAP** (Procedimiento de acceso al enlace), como parte de la norma de interfase de la red X.25, pero más tarde lo modificó nuevamente para crear el LAPB, con objeto de hacerlo más compatible con la última versión del HDLC.

Todos estos protocolos están basados en los mismos principios. Todos están orientados a bit, pero hay diferencias que aunque son muy pequeñas se tienen que tomar muy en cuenta.

Una de las ventajas de los protocolos orientados a bit es la reducción del número de caracteres necesarios para control, ya que cada bit en un caracter de 8 bits puede tener significado diferente.

El protocolo LAPB, como todos los protocolos orientados a bit, utilizan la estructura de trama que se muestra en la figura 3.38.

Campo de Bandera
Cada trama comienza y termina con un patrón de bits para determinar su inicio y su terminación. El patrón de bits es un cero seguido por seis unos y un cero al final, es decir, 01111110.

Para que una trama sea válida, debe tener por lo menos 32 bits entre sus banderas, las tramas inválidas son descartadas.

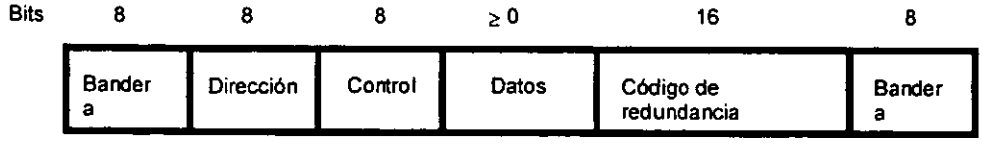


Fig. 3.38 Formato de la trama del protocolo LAPB.

Campo de Dirección
Cuando el receptor detecta una bandera, busca en el flujo de datos un campo de 8 bits con la dirección. En HDLC y SDLC este campo es utilizado para líneas multipunto, soportando hasta 256 estaciones. Como X.25 usa líneas punto a punto, el campo de dirección lo emplea algunas veces para distinguir los comandos de las respuestas.

Campo de Control
Identifica el tipo de trama y es usado para llevar los números de cada trama (secuencia), acuses de recibo, peticiones de retransmisión y otra información de control.

LAPB utiliza tres tipos distintos de tramas:

Tramas I de información
Tramas S de supervisión
Tramas U no numeradas

Trama I de Información
Únicamente las tramas I transportan datos a través del enlace. Estas tramas requieren números de secuencia. Los datos del usuario van contenidos en el campo de datos que sigue inmediatamente al campo de control en una trama I.

A cada trama I se le asigna un número de secuencia entre 0 y 7 en caso de utilizarse una ventana con módulo 8 (el concepto de ventana se define en el tema de control de flujo por técnica de ventaneo). Se usa un campo de 3 bits para especificar estos números de secuencia y se incrementa en uno por cada trama que se envía.

Tramas S de Supervisión
Son utilizadas para transportar información de control, como peticiones de retransmisión, acuses de recibo y peticiones de suspensión temporal de transmisión de tramas I. Por ejemplo, el comando Receive Ready es usado por el DTE o el DCE para indicar la disposición de recibir una trama I. Al presentarse una condición temporal de ocupado y la imposibilidad para aceptar más tramas I, es común enviar Receive Not Ready. El comando Reject (REJ) solicita la retransmisión de tramas I anteriores. Algunas tramas de supervisión tienen que manejar también los números de secuencia. Un ejemplo de esto es la trama del comando Reject.

Tramas U no Numeradas
Las tramas no numeradas derivan su nombre del hecho de que éstas nunca transportan números de secuencia.

Las tramas U proveen funciones de control adicionales, tales como inicialización y desconexión del enlace, reinicialización del mismo después de que ha ocurrido un error irrecuperable y rechazo de tramas no válidas.

LAPB considera iguales al DTE y DCE, es decir, no hay una relación de maestro-esclavo, por lo tanto, cualquier extremo puede comenzar la inicialización o desconexión del enlace.

Campo de Datos
Los datos del usuario se colocan en este campo por lo que puede contener información arbitraria. Puede ser arbitrariamente largo, aunque la eficiencia del código de redundancia decrecerá a medida que se aumente la longitud de la trama, debido a una mayor probabilidad de tener múltiples errores de grupo.

Campo de Código de Redundancia
El campo *Código de Redundancia* es una variante mínima del bien conocido código de redundancia cíclica, se utiliza el CRC-ITU como polinomio generador. Este código se utiliza para la detección de errores en las tramas transmitidas.

Las tres funciones básicas del LAPB se muestran en la siguiente figura:

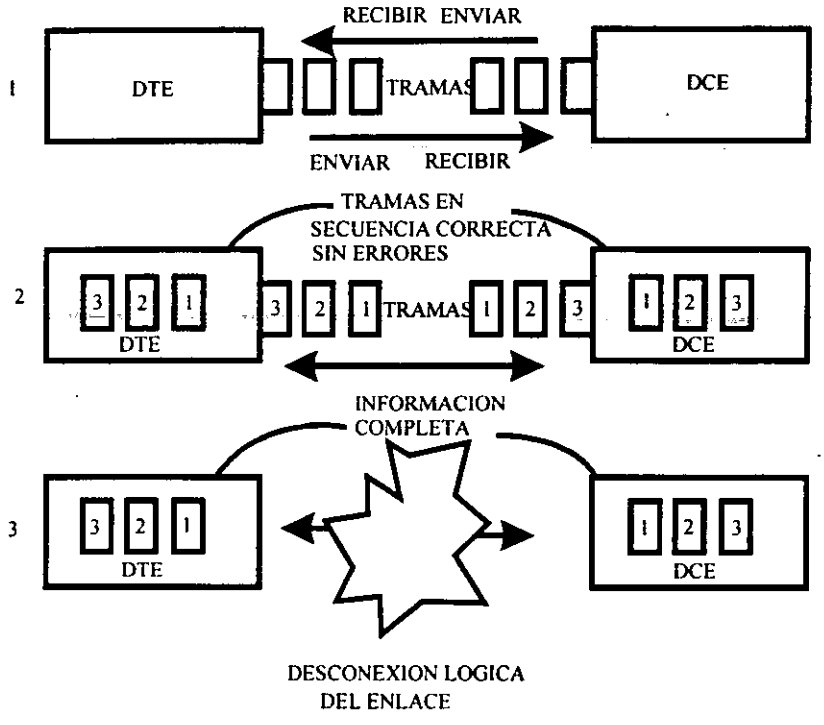


Fig. 3.39 Funciones básicas del LAPB.

3.17.4 Control de Flujo por Técnica de Ventaneo

Básicamente cuando el transmisor envía una trama necesita recibir un acuse de recibo por parte del receptor que le indique que la trama llegó correctamente, antes de transmitir la siguiente. X.25 proporciona un servicio orientado a conexión por lo cual todas las tramas deben llegar al receptor en la misma secuencia con la que fueron enviadas, para controlar el envío y la recepción de tramas se utiliza una **técnica** que se llama **de ventaneo** o **de ventana deslizante.**

En la técnica de ventaneo, cada una de las tramas de salida contiene un número de secuencia, cuyo valor se encuentra en un rango desde cero hasta un valor máximo. Por lo regular este máximo es 2^n-1, donde n es el número de bits que se utilizan para especificar el **número de secuencia.** Por ejemplo, si se utilizan 3 bits para representar este número de secuencia, se podrán tener tramas numeradas de 0 a 7. Debido a que se pueden tener 8 tramas numeradas se dice que son de módulo 8. El emisor mantiene siempre una lista de números consecutivos de secuencia, correspondientes a las tramas que puede enviar. Se dice que estas tramas caen dentro de la **ventana emisora.** Similarmente el receptor mantiene una **ventana receptora,** correspondiente a las tramas que está autorizado a aceptar.

La figura 3.40 muestra el caso de una ventana deslizante de tamaño 1, con un número de secuencia de 3 bits (módulo 8). Inicialmente, no hay tramas transmitiéndose, de tal forma que los bordes inferior y superior de la ventana del emisor son iguales, pero a medida que transcurre el tiempo, la situación progresa como se muestra en esta figura.

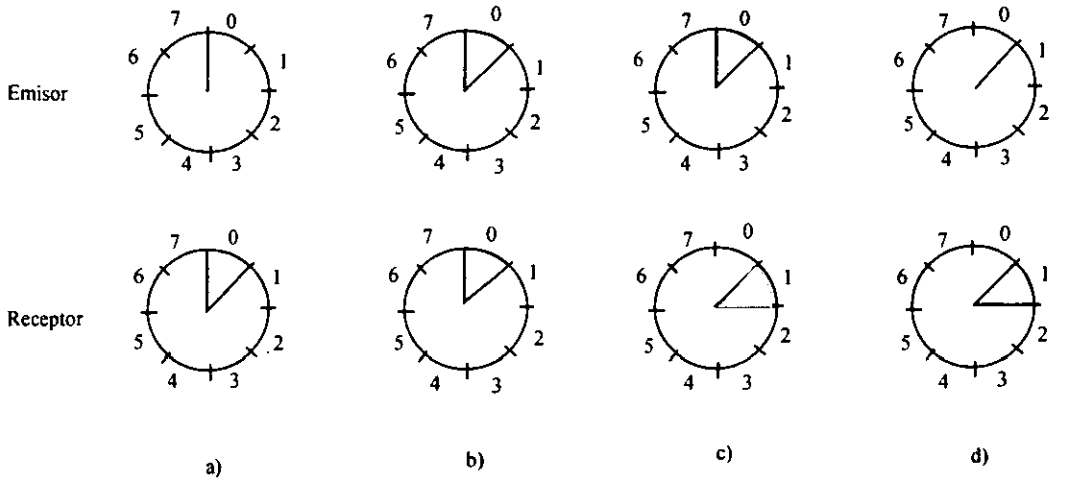


Fig. 3.40 Ventana deslizante de tamaño 1, con un número de secuencia de 3 bits.
a) Al principio,
b) Después de que se transmitió la primera trama.
c) Después de que se recibió la primera trama
d) Después de que se recibió el primer acuse de recibo.

El transmisor tiene un temporizador que pone a funcionar cuando envía una trama, si no le llega el acuse de recibo del receptor en un tiempo predeterminado vuelve a transmitir la trama.
Protocolo PLP (Packet Layer Protocol) de la Capa de Red

La capa de red o de paquetes es la más compleja de la recomendación X.25, gran parte de esta complejidad se debe a la flexibilidad y confiabilidad que por naturaleza debe tener un protocolo de este nivel. Al protocolo de esta capa se le conoce normalmente como **X.25 PLP** (Protocolo de la capa de paquetes).

Una de las funciones principales de la capa de paquetes de X.25 es el establecimiento de conexiones por medio de circuitos virtuales.

La capa de red de X.25 permite establecer varios circuitos virtuales sobre una misma conexión física.

Una red X.25 ofrece dos variedades de circuitos virtuales:

Circuito Virtual Conmutado

La conexión temporal sobre la red entre dos DTE's es definida por el ITU como una llamada virtual o circuito virtual conmutado (SVC). Los SVC's son análogos a las conexiones telefónicas convencionales. Para establecer una conexión SVC, se requieren tres fases separadas: el establecimiento de la llamada, la transferencia de datos y la desconexión de la llamada.

Circuito Virtual Permanente

Para las aplicaciones que requieren conexiones punto a punto a través de líneas dedicadas, una red X.25 soporta circuitos virtuales permanentes (PVC). A diferencia de los SVC's los PVC's tienen únicamente una fase: la transferencia de datos.

Los SVC's y PVC's se establecen por medio de números de canal lógico (LCN), que son asignados a través de la interfase DTE/DCE en ambos extremos de la conexión.

X.25 tiene una técnica estructurada para asignar los LCN's de manera eficiente. Esto es crítico para los SVC's ya que cada llamada que se establece, obtiene un número de canal lógico en forma dinámica. En un enlace X.25 puede haber hasta 4096 canales lógicos diferentes.

El canal lógico cero, LCN0, no está disponible para llamadas normales, debido a que esta reservado para uso futuro. La zona de circuitos virtuales permanentes comienza en el LCN1 y termina en un número predefinido LCNn. Después del último número de canal utilizado por los PVC's todos los LCN's que restan son usados por los SVC's. Si no hay PVC's definidos entonces a partir del LCN1 están disponibles para los SVC's.

Las conexiones (llamadas virtuales en la terminología del ITU) se llevan a cabo de la siguiente manera. En el momento en que un DTE quiere comunicarse con otro DTE, primero debe establecer una conexión. Para hacer esto, el DTE crea un paquete *SOLICITUD DE LLAMADA* y lo pasa a su DCE. La red, entonces, se encarga de entregar el paquete al DCE destinatario, quien a su vez lo pasa al DTE destino. Si finalmente desea éste aceptar la llamada, envía un paquete de vuelta con la instrucción *LLAMADA ACEPTADA.* Cuando el DTE fuente recibe el paquete *LLAMADA ACEPTADA* se establece el circuito virtual. En realidad, cuando un paquete llega al DTE fuente, a éste se le llama paquete *LLAMADA CONECTADA,* pero de hecho es igual al paquete *LLAMADA ACEPTADA* transmitido por el DTE remoto.

A partir de este momento, los dos DTE's pueden utilizar una conexión bilateral simultánea para intercambiar paquetes de datos. En el momento en que cualquiera de los dos lados decida terminar la transmisión, enviará un paquete de *SOLICITUD DE CANCELACION* al otro lado, el cual entonces procederá a enviar de vuelta un paquete *CONFIRMACION DE CANCELACION* como acuse de recibo. En la figura 3.48 se muestran las tres fases correspondientes de una conexión X.25.

El DTE fuente puede seleccionar cualquier número de canal lógico inactivo para identificar la conexión. Si este número de canal lógico se encuentra ocupado en el DTE destino, el DCE destinatario deberá reemplazarlo por un número que no esté siendo usado, antes de entregar el paquete. Por lo tanto, la selección del número de canal en las llamadas que salen, está determinada por el DTE y, para las llamadas que llegan, por el DCE. Podría llegar a presentarse una situación en donde los dos seleccionen simultáneamente el mismo número, generándose una **colisión de llamada.**

El X.25 especifica que si llega a presentarse una colisión de llamada, la llamada que sale sigue mientras que la de entrada se cancela. Muchas redes tratarán de establecer la llamada de entrada inmediatamente después, utilizando un número de canal lógico diferente. Para minimizar la posibilidad de tener una colisión de llamada, el DTE selecciona normalmente el identificador mayor que se encuentre disponible para las llamadas de salida y el DCE selecciona el identificador menor para las llamadas de entrada.

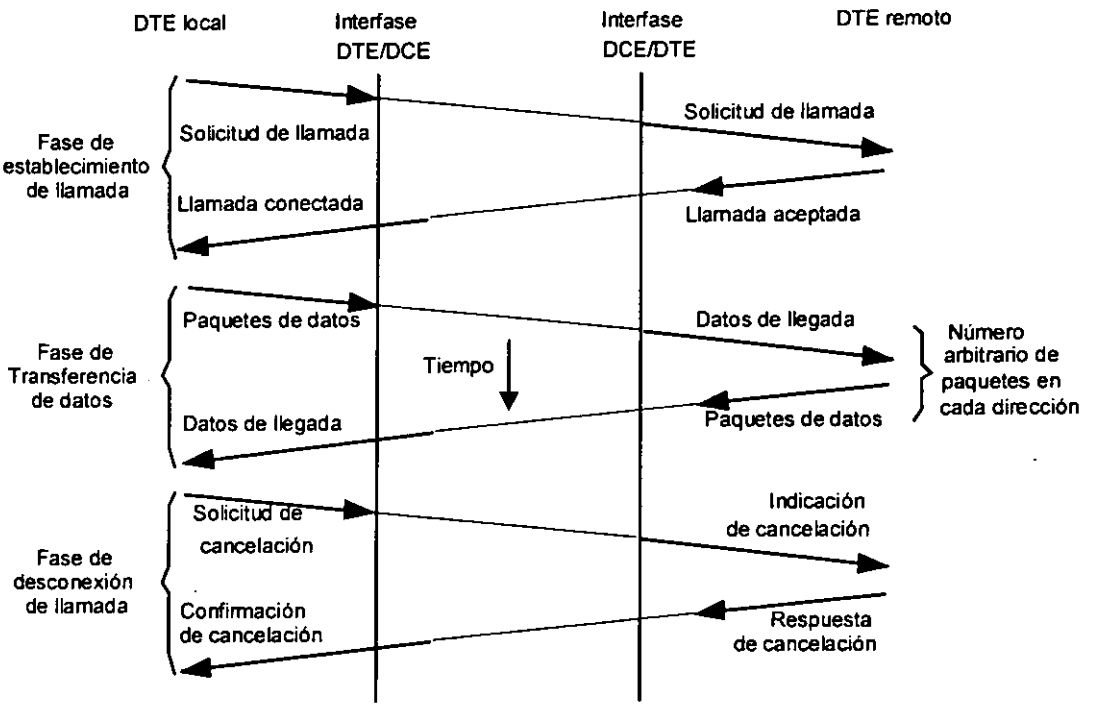


Fig. 3.41 Las tres fases de una conexión X.25.

Como ejemplo del formato de un paquete, la figura 3.49 muestra el paquete *SOLICITUD DE LLAMADA*.

Este paquete, así como los otros paquetes X.25 comienza con una cabecera de 3 octetos. El ITU llama **octetos** a los **bytes**.

Campos Grupo y Canal

Los campos correspondientes a *Grupo y Canal* forman un número de canal lógico (LCN) de 12 bits. El canal lógico 0, como se mencionó anteriormente, está reservado para uso futuro, por lo que en principio, un DTE puede llegar a tener hasta 4095 circuito virtuales simultáneamente abiertos. Los campos *Grupo y Canal,* desde el punto de vista individual, no tienen un significado particular.

Campo Tipo

En el paquete *SOLICITUD DE LLAMADA*, y en todos los otros paquetes de control, se encarga de identificar el tipo de paquete.

Campo Control

El bit del campo *Control* se fija con un valor de 1 en todos los paquetes de control y con un valor de 0 en todos los paquetes de datos. Al revisar primero este bit, el DTE puede saber si el paquete que acaba de llegar contiene información de datos o de control.

Campos Longitud de Direcciones y Direcciones del que Llama y del Llamado

Los tres campos siguientes contienen la longitud de la dirección del que llama, la longitud de la dirección del llamado y las direcciones de cada uno de ellos, respectivamente. Las dos direcciones están codificadas con 4 bits por cada dígito decimal.

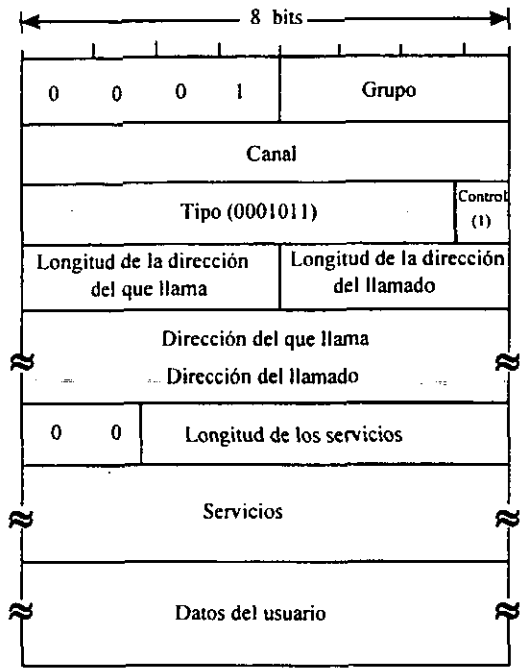


Figura. 3.42 Formato X.25 para el paquete SOLICITUD DE LLAMADA.

El **sistema de direccionamiento** que se utiliza X.25 está definido en la **recomendación X.121** del ITU. Este sistema es parecido a la Red Telefónica Pública Conmutada, con cada dispositivo (host) identificado por un número decimal que consta de un código del país, un código de la red y una dirección dentro de la misma específica para el host. La dirección completa puede llegar a constar de un máximo de 14 dígitos decimales, de los cuales los primeros tres indican el país, y los siguientes indican el número de la red y el host. Para aquellos países que esperan tener muchas redes públicas involucradas en el tráfico internacional, se han asignado múltiples códigos de país. Por ejemplo, a Estados Unidos de América se le ha asignado los códigos de país del 310 al 329, permitiéndole así tener hasta 200 redes (10 redes por cada código) con 10 billones de direcciones cada una.

Campos Longitud de Servicios y Servicios (de Conexión)

El campo *Longitud de Servicios o Facilidades* indica cuantos octetos ofrece el campo de servicios que sigue. El campo *Servicios* se utiliza para solicitar algunas características especiales para la conexión. Las características específicas que están a disposición pueden variar de red a red. Una posible característica es el cobro revertido del servicio (llamadas a cobro revertido). Este servicio, es especialmente importante para organizaciones con millares de terminales remotas, que inician llamadas hacia una computadora central. Si todas las terminales solicitaran siempre el cobro revertido, la organización solamente tendrá un recibo, en lugar de miles de ellos. Otra de las características es el hecho de tener un circuito virtual unidireccional, en lugar de uno bidireccional.

El DTE que llama, también puede especificar una longitud máxima de paquete, así como un tamaño de ventana, en lugar de utilizar los **valores por omisión** que constan de 128 octetos y dos paquetes, respectivamente. Si el DTE llamado no maneja la longitud máxima del paquete o el tamaño de la ventana propuestos, puede hacer una contrapropuesta en el campo de servicios del paquete *LLAMADA ACEPTADA*. La contrapropuesta sólo puede cambiar la original para acercarla a valores más próximos a los de omisión, y no más alejados. En la figura 3.50 se listan algunos de los servicios que comúnmente ofrecen muchas redes.

Algunos servicios pueden seleccionarse cuando el cliente se convierte en un suscriptor de la red, más que en base a cada llamada. Estos incluyen a **Grupos Cerrados de Usuarios (CUG)**, tamaños máximos de ventana que sean menores de siete (para terminales con espacio reducido de memoria temporal), velocidad de línea (por ejemplo, 2400, 4800, y 9600 bps), y la prohibición de llamadas de salida o de entrada (dispositivos que pueden aceptar llamadas, pero no hacerlas y viceversa).

A través del servicio de grupo cerrado de usuarios, los usuarios pueden configurar una o más **Redes Privadas Virtuales (VPN)** dentro de la red pública. Este servicio de grupos cerrados de usuarios permite al usuario reunir un determinado número de DTE's en un solo grupo lógico. El acceso a dicho grupo puede restringirse para recibir llamadas entrantes de la red, y también se pueden prohibir las llamadas salientes.

El número de CUG's depende de la red, un solo DTE puede pertenecer a uno o más CUG's. Normalmente, un número de dos dígitos identifica a un grupo cerrado de usuarios en su formato básico. Un formato ampliado para CUG's permite incluir hasta 10,000 CUG's utilizando un número de cuatro dígitos.

Campo Datos del Usuario

Permite que el DTE transmita hasta 16 octetos de datos junto con el paquete *SOLICITUD DE LLAMADA*. Los DTE's pueden decidir por sí solos qué hacer con esta información, por ejemplo, podrían enviar un password.

Números de secuencia de uso extendido (7 bits)
Fijación del tamaño de la ventana sin normalizar
Fijación del tamaño del paquete sin normalizar
Fijación de la clase de rendimiento (75 bps a 48 Kbps)
Solicitud de cobro revertido
Aceptación de cobro revertido
Selección de operador
Sólo datos de salida (sin que haya datos de entrada)
Sólo datos de entrada (sin que haya datos de salida)
Redireccionamiento de llamadas
Uso de selección rápida

Figura. 3.43 Ejemplo de servicios de X.25.

Aunque varias llamadas virtuales pueden compartir un mismo circuito físico, éstas mantienen su individualidad a través del uso de los LCN's. Los paquetes de datos subsecuentes al paquete *SOLICITUD DE LLAMADA* portan solamente el LCN para su identificación, no es necesario que contengan información de direcciones o servicios, ya que dicha información se almacena en la memoria del nodo de la red al inicio de la llamada y se asocia con ella hasta que se libera por medio del paquete *INDICACION DE CANCELACIÓN*.

Existe también la **recomendación X.75** que especifica procedimientos y formatos para la interconexión de redes públicas de paquetes X.25.

3.17.5 Dispositivo de Ensamblado/Desensamblado de Paquetes (PAD)

Dado que hay una gran cantidad de terminales, en todo el mundo, que todavía no hablan el protocolo X.25, se ha definido otro conjunto de normas que describen la forma en que un terminal simple (no inteligente) puede comunicarse con una red pública X.25. El usuario u operador de la red instala una "caja negra" a la cual se conectan las terminales. A esta caja negra se le conoce como **PAD** (Ensamblador/desensamblador de paquetes), cuyas funciones están descritas en una recomendación del CCITT que se conoce como **X.3**. Entre el terminal y el PAD se ha definido un protocolo normalizado denominado **X.28**. Otro protocolo, nombrado **X.29**, existe entre el PAD y el nodo destino (host). Estas tres recomendaciones en conjunto se conocen como **recomendaciones triple X**. La figura 3.44 muestra los intervalos de aplicación de cada una de estas recomendaciones.

3.17.6 Recomendaciones

X.3
Este documento define la operación y funcionamiento del PAD para el soporte de terminales asíncronas. El funcionamiento del PAD se basa en una serie de parámetros los cuales se fijan al momento de la contratación del servicio y pueden ser modificados ya sea por la terminal asíncrona o por la computadora remota (host) durante la llamada.

X.28
Esta define los procedimientos bajo los cuales la terminal asíncrona interactua con el PAD. Estos procedimientos administran el establecimiento de una conexión lógica, la inicialización del servicio, la modificación de los parámetros del PAD y el intercambio de información entre el PAD y la terminal.

X.29
Especifica la forma como el PAD y el nodo destino interactúan. Las funciones que realiza el PAD pueden agruparse en cuatro categorías esenciales:

Soporte de las interfaces de la terminal y del nodo destino.
Procedimientos para el establecimiento de la llamada virtual.
Procedimientos para la transferencia de datos.
Modificación de parámetros X.3.

Al inicio del servicio, es necesario definir el conjunto de parámetros X.3. Estos parámetros son utilizados por el PAD a fin de controlar el funcionamiento de la terminal asíncrona hasta el momento en que se desconecta la interfase.

En el caso de los procedimientos para el establecimiento de la llamada virtual, la recomendación X.28 define como se llevará a cabo la conexión lógica de la terminal y establece las señales que han de enviarse al PAD. También indica los procedimientos para la desconexión de la misma.

Para las funciones de transferencia de datos, los parámetros X.3 utilizados en el PAD administran el procedimiento a seguir en el caso de recepción de una señal de ruptura de comunicación y las condiciones para la transferencia de datos. La recomendación X.28 define el control de flujo entre el PAD y la terminal. Los procedimientos para el control de flujo entre el PAD y el host remoto se indican en la recomendación X.29.

Con respecto a la modificación de los parámetros X.3, estos procedimientos están indicados en las recomendaciones X.28 y X.29. En la recomendación X.28 se definen los procedimientos para que la terminal asíncrona modifique dichos parámetros mientras que la X.29 establece lo mismo pero por parte del host remoto.

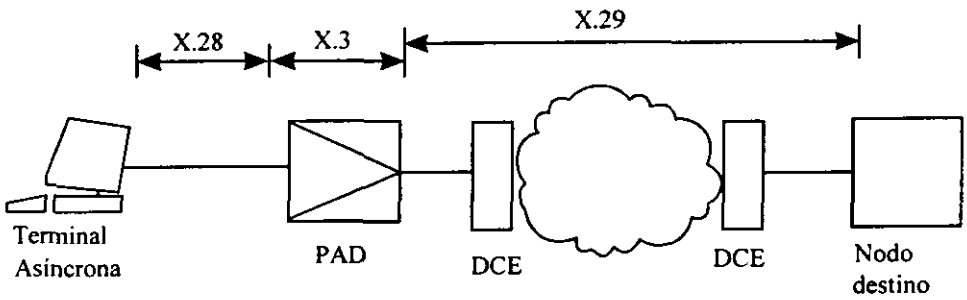


Figura. 3.44 Recomendaciones triple X empleadas cuando un PAD es conectado a una red de paquetes X.25.

3.18 Redes Frame Relay

Frame Relay es un estándar como X.25 que determina los procedimientos de comunicación entre DTE y DCE necesarios para accesar a una red de conmutación de paquetes. Combina la multicanalización estadística y la administración de los puertos de la conmutación de paquetes X.25 con la alta velocidad y bajo retardo de la conmutación de circuitos TDM.

Lo anterior se ha definido como un servicio modo paquete, esto significa que la información es organizada ahora individualmente y direccionada más que colocada en una ranura de tiempo, dando con ello características de multicanalización estadística y de administración de puertos. De una manera contraria a X.25, Frame Relay elimina por completo el procesamiento de nivel 3 y sólo usa parte de las funciones del nivel 2, las cuales incluyen la verificación del error. Todas las demás funciones, tales como supervisión, reconocimientos (ACK), secuencia de números, rotación de ventana, son eliminadas en esta tecnología, ganando con todo ello incrementar el caudal eficaz de la red (**Throughput**, que se puede definir como el número de tramas que pueden ser procesadas en un segundo para un costo dado de hardware) ya que las tramas no requieren de mucho procesamiento.

Una de las características de Frame Relay es que la estructura de la trama es de longitud variable quedando con un intervalo dinámico que va desde muy pocos hasta miles de caracteres. Frame Relay simplemente envuelve las tramas de información en su estado nativo. En la figura 3.45 se muestra la trama de Frame Relay en su forma más simple.

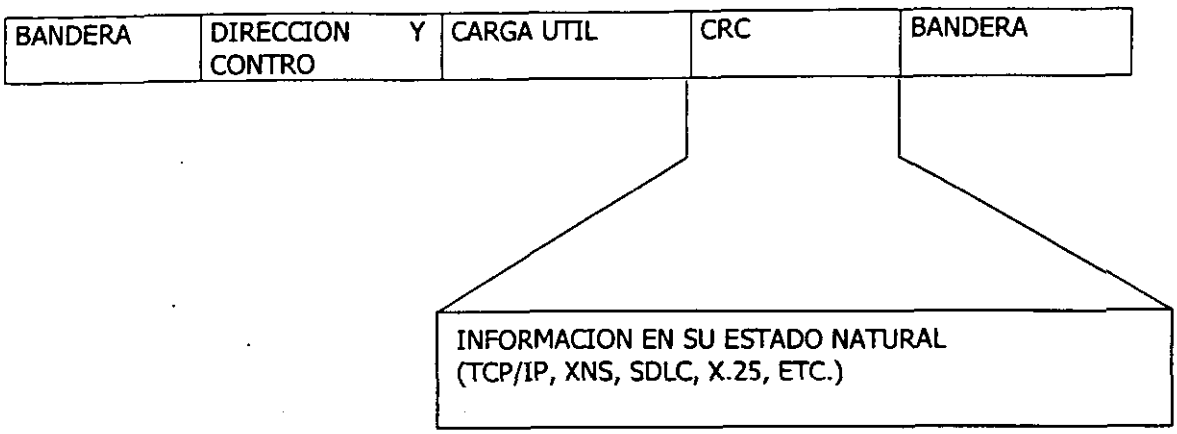


Figura. 3.45 Trama de Frame Relay

Frame Relay fue desarrollada como una nueva forma de conmutación modo paquete que tiene cuatro características importantes, alta velocidad, bajo retardo, comparte puertos y ancho de banda; las cuales son la solución ideal para el tráfico tipo ráfaga, encontrado en la interconexión de LANs y WANs.

Frame Relay requiere de tres condiciones:

- ✓ Los equipos terminales deberán soportar un protocolo inteligente de capas superiores.
- ✓ Líneas virtualmente limpias.
- ✓ La aplicación debe de tolerar un retardo variable.

Para un mejor estudio de la operación de Frame Relay conviene dividirlo en dos partes:

- ✓ Flujo básico de información en Frame relay
- ✓ Señalización en la interfase para proveer de control

Flujo Básico de Información

Generalmente la información es llevada a través de las líneas de comunicación en tramas basadas de una manera similar.

Frame Relay hace unos cambios pequeños en la estructura de la trama e incluye dos octetos (bytes) de encabezado de la trama o marco.

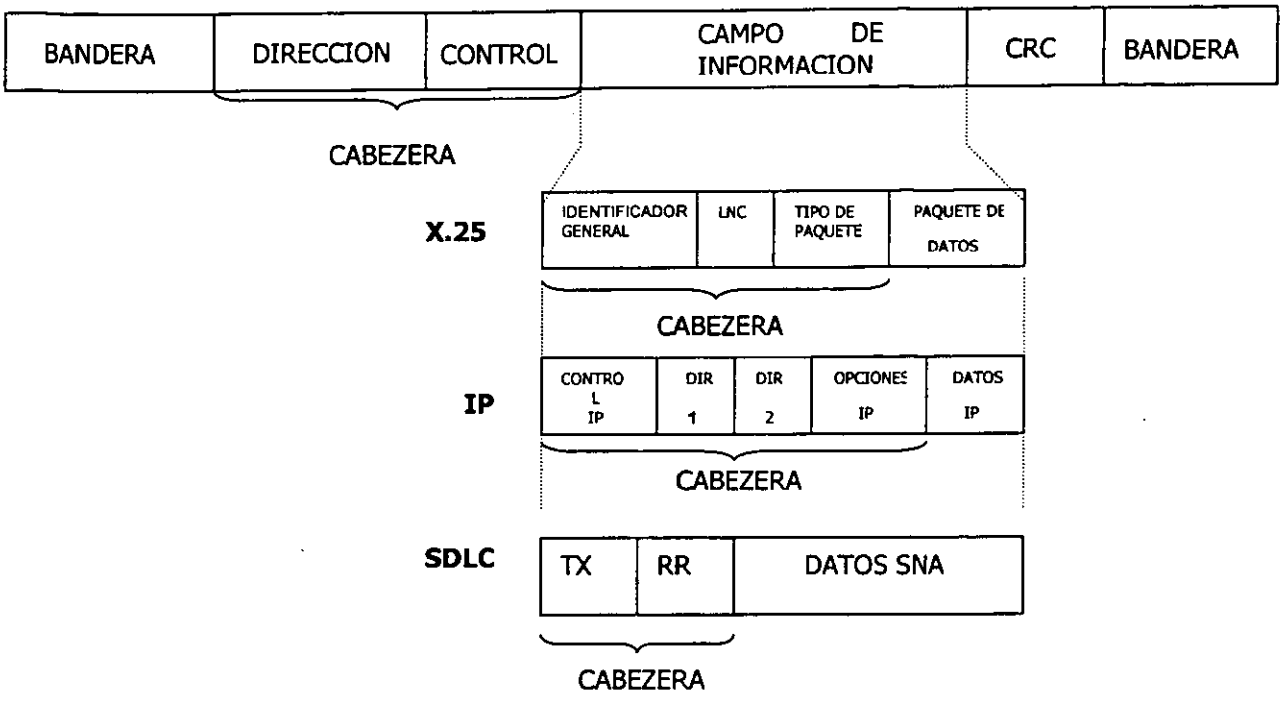


Fig. 3.46 Estructura Básica de la Trama.

3.18.1 Encabezado de Frame Relay

El encabezado de Frame Relay contiene un número de 10 bits, el **Identificador de Enlace de Datos (DLCI)**, el cual es el número de circuito virtual que corresponde a un destino en particular. En el caso de una interconexión RLD – RCA, el DLCI sería el puerto al cual la RDL está unido.

El DLCI permite a los datos entrar en la red de Frame Relay y ser enviados a través de ésta mediante un proceso que puede ser dividido en tres partes:

- ✓ Se revisa la integridad de la trama, si existe error, esta se descarta.
- ✓ Se revisa el DLCI con una tabla, si el DLCI no está definido para este enlace, la trama se descarta.
- ✓ La trama se entrega a su destino por el puerto troncal especificada en cada tabla.

A diferencia de X.25, Frame Relay no tiene tanto procesamiento nodal. Para poder mantener la simplicidad del mecanismo base de frame relay, se sigue una regla muy sencilla: si existe algún problema con la trama, simplemente se descarta. Las dos principales razones por las cuales se puede descartar una trama son la detección de errores en la información y por congestión. La razón por la que Frame Relay puede hacer esto, sin arruinar la integridad del enlace de comunicación, reside en la inteligencia de los dispositivos conectados a la red.

Lo anterior es posible debido a que Frame Relay soporta protocolos de capas superiores, los cuales se encargan de detectar errores y recobrar la información perdida.

La manera en que un protocolo de nivel superior puede recuperar una trama descartada, a partir de una secuencia de números de tramas enviadas o recibidas. En este proceso, se envían reconocimientos (ACK) para informar que la trama haya sido bien recibida. Si un número en la

secuencia se pierde, el nodo transmisor se espera un tiempo determinado antes de que el nodo destino envíe una petición de retransmisión.
Esta función es llevada a cabo en el nivel 4, o capa de transporte, tales protocolos son TCP/IP, OSI, XTP, todos de la clase 4, a diferencia de X.25 que ejecutaba estas operaciones en la capa 3 o nivel de red.

Resulta crítico el hecho de que durante la transmisión de descarte tramas, ya que con una sola trama perdida, se tendrán que retransmitir todas las tramas no reconocidas. Todo esto toma ciclos extra de máquina y de memoria en los dispositivos terminales, teniéndose por consecuencia grandes retardos debido a los tiempos fuera de los niveles superiores (tiempo de espera antes de declarar perdida la trama) y el tiempo de retransmisión.

Por lo tanto a pesar de que los protocolos de capas superiores pueden recobrar las tramas perdidas, el factor clave para mantener el correcto desempeño general de la red, es la habilidad de ésta para minimizar las tramas perdidas.

Tramas Descartadas Por Bits erróneos

Cuando un error ocurre en la trama, generalmente causado por ruido en la línea, esto podría ser detectado en la trama recibida por medio de la función de **Verificación de Secuencia de la Trama (FCS)**. Lo cual resulta ser totalmente diferente al protocolo X.25, el cual ejecuta la revisión de la integridad de los datos en cada nodo.

En la tecnología Frame Relay, todos los nodos por los cuales la trama pasa, simplemente la toman y la enrutan. La revisión de errores solo tiene lugar en el nodo destino, en el cual descansa la inteligencia que se encarga de solicitar la retransmisión de la trama que se descartó. Los grandes retrasos debido al hecho de tener una recuperación por medio de capas superiores, aunado al hecho de contar con líneas ruidosas, podrían tener un efecto desastroso en la eficiencia de la red. Por lo que ahora las dorsales en muchos países se basan en fibra óptica que tiene muy baja tasa de error, haciendo que la frecuencia de errores encontrados y la recuperación de tramas en los puntos terminales sea extremadamente baja.

Tramas Descartadas Por Congestión

La causa por la cual la mayoría de las tramas son descartadas es la congestión, más que por error en la red la congestión ocurre cuando en un nodo se reciben más tramas que las que éste pueda procesar (congestión por recepción), o bien, cuando se necesita enviar más tramas o marcos a través de una línea a una velocidad mayor que la que ésta permite o puede soportar (congestión en línea).

En el caso de que la memoria temporal (buffer) esté llena, se descartan las tramas que lleguen hasta que se vuelva a tener espacio disponible en la memoria. Debido a que en las redes locales de datos el tráfico es del tipo ráfaga, la probabilidad de congestionamiento es bastante alta. Es muy importante que la red Frame Relay tenga una excelente administración de la congestión, tanto para minimizar la ocurrencia de algún tipo de ésta, como para disminuir el efecto de las tramas descartadas cuando así se requiera.

3.18.2 Señalización De Interface Para el Control

Agregar mecanismos para el control vuelve un poco más compleja a la tecnología frame relay. El uso actual de todos esos mecanismos de señalización es opcional, pero se recomienda su utilización para mantener una alta eficiencia, tiempo de respuesta y desempeño de la red. Por lo anterior, es importante conocer como trabaja la señalización frame relay.

En congestión severa, se puede llegar hasta la caída total del sistema y la única manera de evitarlo es reduciendo el tráfico, es por eso que se han desarrollado mecanismos que notifican a los dispositivos de los usuarios que una congestión está ocurriendo y que deben reducir su tráfico o carga ofrecida. Así la red obtiene su punto óptimo para mantener su mejor eficiencia y desempeño.

3.18.3 Mecanismos de Alarma de Congestión

Notificación de Congestión Explícita **(ECN)**, este mecanismo utiliza dos bits en la cabecera de la trama o el bit de Notificación de Congestión Explícita Directa **(FECN)** y el bit de Notificación de Congestión Explícita Inversa **(BECN)**.

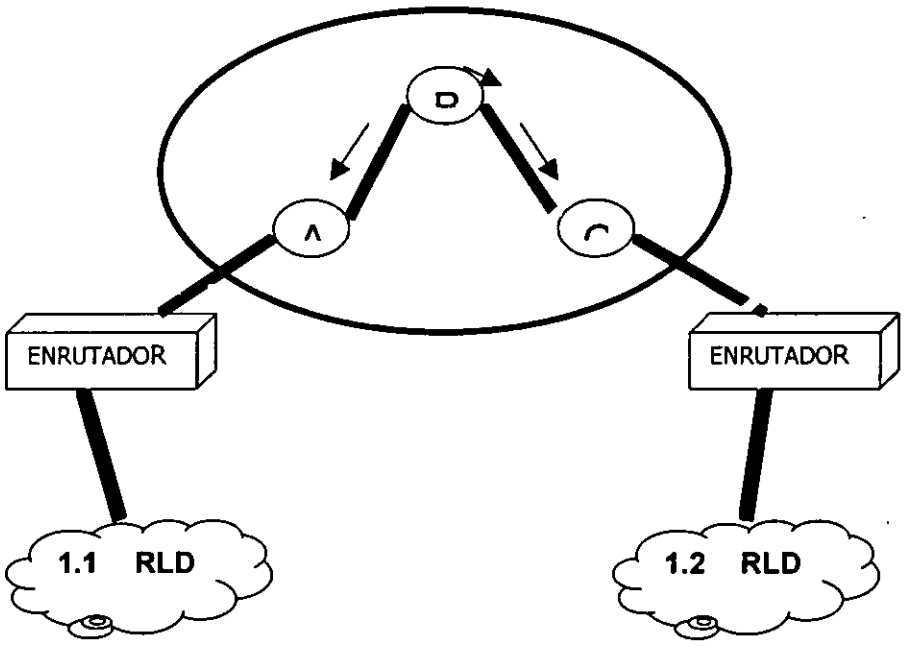


Fig. 3.47 Uso de los bits BECN y FECN.

El nodo B está bajo congestión, que pudo haber sido causada por un pico de tráfico entre B y C. El nodo B se da cuenta de que está bajo congestión, en base a mediciones de su memoria en uso o bien a través de la longitud de la cola de paquetes que exista, notificando de esto al nodo C (nodo siguiente de la trayectoria) por medio de un cambio en el bit FECN de 0 a 1. De este modo todos los nodos siguientes que están en la trayectoria destino sabrán que ocurrió una congestión en el DLCI afectado.

A veces es más conveniente notificar al nodo fuente que existe una congestión, de esta manera dicho nodo disminuiría la carga ofrecida hasta que la congestión desapareciera. Esto se hace cambiando el bit BECN de 0 a 1.

El proceso de FECN y BECN puede tomar lugar simultáneamente en múltiples DLCI, en respuesta a una congestión en una línea dada o nodo, de esta manera se notifica a las fuentes y destinos.

Administración Consolidada del Nivel de Enlace (CLLM)

Para poder usar el bit BECN se requiere que existan tramas que estén llegando de la fuente causando congestión, pero que sucede si no existen tramas en ese trayecto. Los estándares de Frame Relay no permiten que la misma red genere sus propias tramas con el DLCI del circuito virtual deseado.

Para este tipo de situaciones la ANSI ha definido otro mecanismo para señalización, llamado **Administración Consolidada del Nivel de Enlace (CLLM).**

Con la función de CLLM, uno de los DLCIs (el número 1023) en una interface frame relay se reserva para enviar mensajes de control del nivel de enlace de la red al equipo terminal.

El estándar ANSI (TI.618) define claramente el formato del mensaje CLLM que la red envía al usuario. Este mensaje contiene un código, el cual indica la causa de la congestión (tráfico excesivo, fallas en la línea) y lista todos los DLCIs que deben reducir la carga ofrecida para bajar la congestión. CLLM puede ser causado en lugar de, o en adición a los bits ECN para informar al usuario de la existencia de congestión, como se muestra en la figura 3.48.

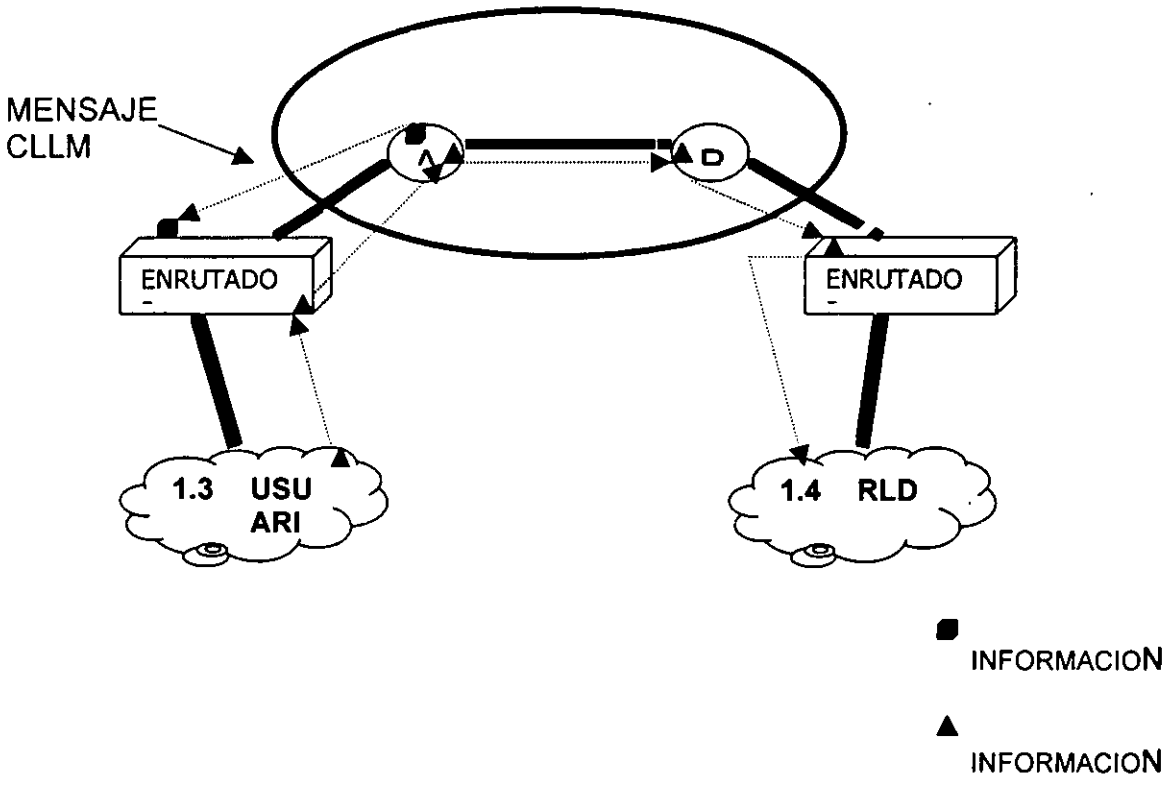


Fig. 3.48 Ejemplo de la función del CLLM

Notificación por Congestión Implícita

Algunos protocolos de transporte como el TCP/IP, que operan en los equipos terminales tienen una forma implícita de detectar la congestión. Este tipo de protocolos limita la tasa del tráfico que se está enviando a la red mediante "ventanas". Estas ventanas sólo permiten que un número determinado de tramas (tamaño de la ventana) sean enviadas antes del reconocimiento (ACK) sea recibido.

El protocolo puede darse cuenta de que existe congestión por parámetros como el tiempo de retardo total o por tramas perdidas (estas características del tráfico indican una congestión implícita). Si ocurre una congestión, el protocolo disminuirá el tamaño de la ventana, disminuyendo con esto la carga hasta que la congestión desaparezca. Después, se vuelve a incrementar gradualmente. Este ajuste en el tamaño de la ventana también es utilizado por el DTE cuando se recibe una señal ECN.

La ANSI especifica que la congestión explícita e implícita sin complementarias y deben de usarse en conjunto para mejores resultados. De aquí, surge la pregunta: ¿Cómo debe responder el dispositivo del usuario ante una alarma de congestión?

Los estatutos de los estándares indican que en caso de congestión el dispositivo del usuario debe de bajar la carga ofrecida, pero todas estas notificaciones solo son sugerencias; es decir, son recomendaciones de las acciones que el dispositivo terminal debe de tomar para incrementar o bajar el tráfico.

Sin embargo, el usuario puede hacer caso omiso de estas notificaciones simplemente ignorando las señales de congestión y seguir transmitiendo a la misma velocidad, aumentando con ello la congestión. En tal caso la manera en que la red se protege a sí misma es siguiendo la regla básica de frame relay: si la trama es un problema, se descarta. Afectando con esto la eficiencia del caudal de la red y el tiempo de retardo.

Muchas veces si la red es suficientemente inteligente eliminará las tramas preferentemente de aquellos usuarios que no están funcionando correctamente, para no afectar a los demás usuarios.

3.18.4 Necesidad de conocer El estado de las Conexiones

Existe otro mecanismo de señalización, el cual define como ambos lados de la interface frame relay pueden comunicarse entre sí, informándose del estado de la interface o de los PVC's en esta interface. Tal información puede resumirse en las siguientes necesidades:

- ✓ Saber si la interfaz está activa
- ✓ Los DLCIs válidos para esta interfaz
- ✓ El estado de cada PVC (congestionamiento o no)

La primera definición de la señalización acerca del estado del PVC fue la especificación LMI. Esta señalización tiene el DLCI 1023 (la señalización LMI y CLLM son dos formas de señalización mutuamente exclusivas, es decir, existe una o la otra pero no las dos).

El protocolo LMI se basa en un mensaje de "encuesta de estado" con el cual, el dispositivo del usuario puede informar a la red que continúa activo el enlace con el enrutador, o bien para preguntar el estado de los PVCs en ese puerto. La red responde con un mensaje de estado, el cual puede significar que se mantiene activo el enlace o un reporte acerca del estado de los PVCs.

Otro tipo de mensaje del de "actualización de estados" el cual habilita a la red para enviar un reporte acerca del estado de las PVCs a aquellos nodos que lo hayan solicitado.

La especificación LMI es asimétrica, es decir, solo el dispositivo del usuario puede preguntar acerca del estado y solo la red puede responder con un mensaje de estado.

A pesar de que es muy fácil de implementar, LMI tiene limitaciones en cuanto a su funcionalidad. Debido a su naturaleza no es útil para trabajar entre red y red. Esto es un problema en redes híbridas (privadas/públicas) en la que la red privada tendría una interface frame relay para accesar al mismo servicio de la red pública; por lo que la mejor alternativa es el CLLM.

3.19 Beneficios adicionales asociados a Frame Relay

El Foro de Frame Relay, una organización de no lucro de 300 compañías plus miembros dedicada a promover la aceptación e implementación de Frame Relay, junto con más de 10,000 usuarios mundiales, está dando testimonio de la evolución de Frame Relay de una tecnología del solo-aplicación a una con un ancho espectro de usos.

Gerentes de red constantemente están buscando nuevas maneras de que hacer su compañía sea más eficaz a través del uso de nuevos e innovadores servicios que están introduciéndose continuamente en el mercado. A menudo, ellos se enfrentan con la necesidad de conectar oficinas remotas al backbone corporativo para habilitar el acceso al e-mail corporativo, a la red de área local, a las computadoras del mainframe, y otros servicios corporativos. Frame Relay frecuentemente es la tecnología de opción satisfactoria para estas necesidades.

Inicialmente, Frame Relay ganó aceptación como un medio que proporciona una solución a los usuarios-finales para conexiones LAN-a-LAN y otros requisitos de conectividad de datos. Además de proporcionar mecanismos de transporte para datos flexibles y eficaces. Durante los últimos años ha habido una migración de tráfico legado como bisync y SNA de líneas privadas de baja velocidad hacia Frame Relay. La integración de este tráfico llamado legado con las necesidades de conectividad LAN-a-LAN de hoy les proporcionaron una red más eficaz, flexible, y muy rentable a los administradores de red. Más recientemente, los usos no-tradicionales están empezando a surgir. Debido a los adelantos en áreas como proceso de señales digitales, los usuarios finales están empezando a ver métodos viables que desarrollen aquel tráfico corporativo que no son datos, tal como vídeo y voz sobre Frame Relay.

La tecnología de Voz sobre Frame Relay (VoFR), ofrece la posibilidad a los administradores de red, de consolidar en un solo ancho de banda voz y datos (ejemplo: facsímil y los módem analógicos) con servicios de datos sobre Frame Relay. El Comité Técnico del Foro de Frame ha desarrollado un Acuerdo de Aplicación [FRF.11] para permitirles a vendedores interconectar su equipo VoFR. Se anticipa que este trabajo será el fundamento para el despliegue futuro de capacidades de VoFR en multi-vendedores y ambientes de redes públicas. Antes del desarrollo de este Acuerdo de Aplicación, muchos vendedores de equipo desarrollaron métodos propietarios para llevar a cabo voz sobre Frame Relay para así permitir al usuario final que transporten con éxito voz sobre Frame Relay en sus redes de Frame Relay.

Frame relay continuará viendo un crecimiento explosivo. La aceptación y uso de ATM (Modo del Traslado Asíncrono, una tecnología diseñada con la intención de transportar voz, datos, y vídeo) también aumentará. Tanto los usuarios finales como los proveedores de servicio de red encontrarán que Frame relay ATM no sólo coexisten cada vez más, sino que son complementarios; El acceso de ATM y Frame relay se ofrecen y son utilizados por usuarios finales. Además, los proveedores de servicio han empezado a emigrar sus redes Frame relay a los backbones basados en ATM. El uso continuo y la aceptación creciente de Frame relay y tecnologías de ATM traerán

mayor ancho de banda y la mejor actuación para conectar una red de computadoras a una variedad más amplia de aplicaciones de usuario.

Además de darle alguna visión al lector en cómo VoFR trabaja, esta sección proporcionará una apreciación global de unas de las aplicaciones potenciales de VoFR, algunas de las consideraciones enfrentados por usuarios, y una apreciación global del Acuerdo de Aplicación de la Voz sobre Frame [FRF.11]. La intención no es promover o disuadir a los usuarios de Frame relay de incorporar voz en sus redes, simplemente de proporcionar una perspectiva equilibrada e información para que los usuarios puedan tener más información para decidir acerca de sí ellos pueden beneficiarse de la voz sobre la tecnología de Frame Relay.

3.19.1 Voz sobre Frame Relay

Teoría de Operación

A través de los años, las redes de comunicaciones se han vuelto más confiables. Las conexiones analógicas más antiguas, de baja velocidad, y que a menudo son susceptibles a los errores inducidos por la red están reemplazándose con enlaces digitales de velocidad más alta que ofrecen actuar relativamente libre de error. Además, los dispositivos que comunican a los sitios se han vuelto más inteligentes permitiéndoles disminuir los retrasos de la red, recuperar y re-transmitir datos perdidos. Al contrario de la mayoría de las comunicaciones de datos que pueden tolerar retrasos, las comunicaciones de voz deben realizarse cerca del tiempo real. Esto significa que esa transmisión y eso retrasos de la red deberán permanecer tan pequeños que casi sean imperceptibles para el usuario. Hasta últimamente, la transmisión de paquetes de voz no era posible debido a los requisitos de ancho de banda de la voz, y a los retardos de transmisión asociados con redes de paquetes de datos.

Ahora es posible empaquetar la voz; menores proporciones de bits se logran analizando y procesando sólo los componentes esenciales de una muestra de la voz, en lugar de intentar digitalizar la muestra de la voz entera (con todas las pausas asociadas y los modelos repetitivos). La actual tecnología del procesamiento del discurso tiene varios pasos del procesamiento de digitalización de la voz además de los métodos convencionales de codificación.

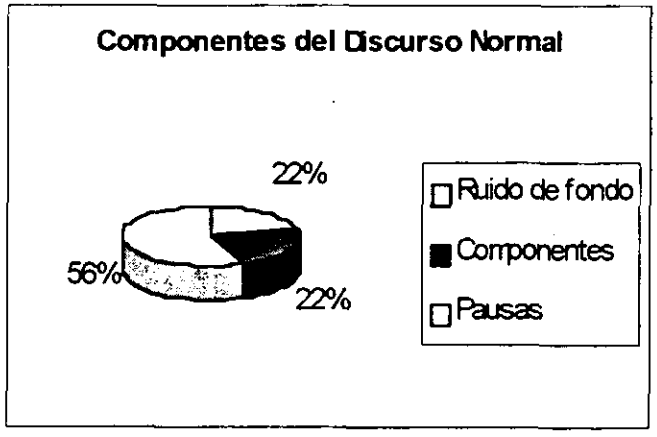


Fig. 3.49. Solamente el 22% del discurso normal necesita ser enviado para comunicaciones de voz de alta calidad.

El discurso humano se carga con una tremenda cantidad de información redundante que es necesario para que ocurran las comunicaciones en un ambiente natural, pero que no se necesitan para una conversación para llevada a cabo sobre una red de comunicaciones. El análisis de una muestra representativa demuestra que sólo el 22 por ciento de una conversación típica tiene componentes del discurso esenciales que necesitan ser transmitidos para una completa claridad de la voz (Figura 3.49). El equilibrio se compone de pausas, ruido de fondo, y los modelos repetitivos.

Remover los Sonidos Repetitivos del Discurso

Los sonidos repetitivos son inherentes en discurso humano, y es causado por vibración de los cordones vocales. Estos sonidos repetitivos (como la 's' en la palabra serpiente o un 'o' largo en la palabra préstamo), es fácilmente comprimible. Mientras viaja a través del ambiente natural, quizás sólo la mitad de lo que se habla alcanzará la oreja del oyente. Sin embargo, en una red de comunicaciones típica, todo el volumen del discurso se transmiten. La transmisión de estos sonidos idénticos no es necesaria; por lo que él suprimirlos puede aumentar eficazmente el ancho de banda.

Remover las Pausas (Supresión de Silencio)

Una persona hablando no proporciona un continuo flujo de información (sin tener en cuenta qué tan rápido hablan). Las pausas entre las palabras y frases, y los huecos que ocurren al final del periodo en el cual una persona habla antes de que el otro empiece; también pueden quitarse. Las pausas pueden representarse en forma comprimida y pueden recrearse en el lado destino de la llamada para mantener la calidad natural de la comunicación hablada. La supresión y re - movimiento de periodos silenciosos, también pueden mejorar significativamente la utilización del ancho de banda.

3.19.2 Formación de Trama de voz

El removimiento de períodos silenciosos y la información redundante a través de las técnicas avanzadas, permite a la voz ser eficazmente "comprimida". Después de remover los patrones repetitivos y los períodos silenciosos, la información restante del discurso puede digitalizarse entonces y puede ponerse en los paquetes de voz convenientes para la transmisión sobre una red de frame relay. Estos paquetes o tramas (se usan a menudo ambos términos) también tienden a ser más pequeños que el promedio de la trama de datos. El uso de pequeños paquetes de ayuda para reducir el retraso de la transmisión por una red de Frame relay. Los conceptos introducidos arriba proporcionan las bases para el uso eficiente de la menor cantidad del ancho de banda posible para la transmisión de la voz sobre una red de Frame relay.

3.19.3 Uso de la Voz sobre Frame Relay

Aplicaciones potenciales para usuarios finales

Administradores de las telecomunicaciones continúan explorando alternativas para obtener el uso más eficaz de sus recursos de la red corporativos. Muchos administradores han emigrado sus redes basadas en líneas privadas punto-a-punto (construídas en los 1980's con TDM - Multiplexores por División de Tiempo) a redes públicas y privadas de Frame Relay. Puesto que muchos de estos enlaces punto-a-punto transportan voz y datos, éstos administradores están interesados en no sólo satisfacer sus necesidades de comunicaciones de datos, sino también sus necesidades de comunicaciones de voz. VoFR (voz sobre Frame Relay) ofrece una alternativa potencial para transportar las comunicaciones de voz sobre una red de Frame relay para satisfacer estas necesidades de comunicaciones de inter-compañía. Los usuarios actuales de Frame relay podrían encontrar que tienen "exceso" de ancho de banda disponible incluso con la tremenda

expansión de aplicaciones y aumenta en tráfico de los datos. Incluso cuando existe ancho de banda utilizado eficazmente, algunos administradores de red podrían encontrar que el costo incremental para el ancho de banda de red Frame relay adicional que se necesitaría para transporte de la voz, es más rentable que algunos de los servicios de la voz normales ofrecidos por proveedores de telefonía de larga distancia y local. En otros casos, algunos usuarios podrían encontrar la VoFR como una opción viable para usarse en lugar de Off-Premises Extension (OPX) y líneas privadas Auto Ringdown (PLAR).

Por supuesto, la motivación detrás del interés en VoFR variará. VoFR tiene el potencial para proporcionarles mayor eficiencia a los usuarios en el uso del ancho de banda integrando funcionalmente voz, datos, y facsímil sobre un solo enlace. Además, VoFR tiene el potencial para proporcionarles una opción rentable a los usuarios para sus necesidades de transporte de tráfico de voz entre sus localidades.

Como ejemplo, un administrador de red, puede escoger entre integrar unos cuantos canales de voz y datos seriales sobre la conexión de Frame relay entre una oficina remota y la oficina principal. Transmitiendo el tráfico de la voz sobre la conexión de Frame relay que ya está llevando tráfico de datos (Figura 3.50), el usuario tiene el potencial para obtener a costo efectivo llamadas telefónicas y el uso eficaz del ancho de banda de la red.

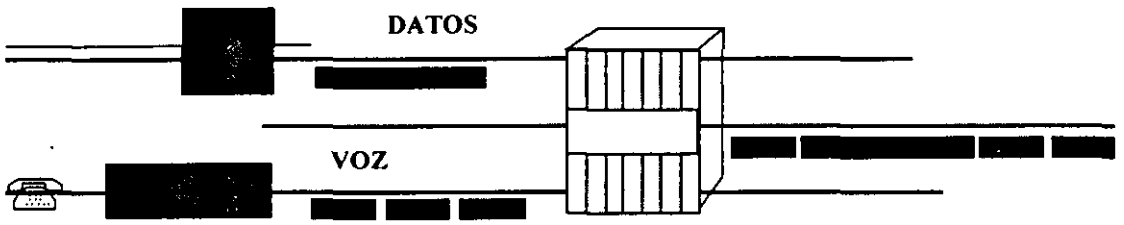


Figura 3.50 La Voz y datos integrados a través de equipo del cliente.

Los ejemplos proporcionados no necesariamente reflejan todas las posibilidades potenciales de VoFR. Hay muchas razones usadas, y las posibilidades exploradas por gerentes de la red en su esfuerzo por justificar capacidades de la gestión de redes más eficaces, flexibles, y rentables. VoFR representa uno de muchos posibles métodos que les permiten a los usuarios que aumentar la flexibilidad y eficacia de los recursos de la red de su compañía

Sin embargo, podrían existir algunos contras que se pueden enfrentar al llevar a cabo VoFR. Algunos significarían incluir alguna pérdida de la calidad asociada con la calidad del tráfico de voz, debido al uso de la compresión de voz en VoFR; la pérdida del control y administración dirección y los beneficios administrativos asociados con servicios de voz que brindan los proveedores (por ejemplo: la pérdida de la tarificación de los servicios de voz, y otras características avanzadas como Caller ID (Identificador de llamadas) y la contabilidad; Y la falta de normas que definen los niveles aceptables de calidad para transporte de la voz sobre Frame relay por los proveedores.

Además, los proveedores que ofrecen servicio de Frame relay público no siempre pueden garantizar la calidad o performance de voz transportadas en sus redes de Frame relay. En la ausencia de normas no hay características técnicas que definan la calidad de una conversación de la voz (ej. retardo, tono, etc.). Ya que la calidad de VoFR es subjetiva, es difícil para el proveedor garantizar la completa satisfacción del usuario.

Sin embargo, los significativos adelantos en procesadores digitales y algoritmos de compresión proporcionan a menudo mayor calidad de voz. Los proveedores de VoFR continúan agregando mejoras en cuestiones de administración. La industria buscará definir normas que definen niveles aceptables de calidad y métrica para mejor actuación del transporte de la voz a través de las redes de datos.

A algunos usuarios no les afectan las cuestiones de calidad; porque les interesa más una buena relación de costo-beneficio, entonces dependerá del cliente decidir.

3.19.4 Equipo para Voz sobre Frame Relay

Consideraciones comunes Enfrentadas Por fabricantes de Equipo

Los fabricantes que ofrecen equipo capaz de integrar tráfico de voz y datos sobre Frame relay deben considerar cómo dirigirán los problemas como compresión, cancelación de eco, retardo y variación de retardo, pérdida de trama, y priorización de tráfico. Estas, y otras consideraciones, pueden afectar calidad de la voz. Mientras que los fabricantes ofrecen equipos para voz sobre Frame relay pueden tener objetivos similares con respecto a la calidad y performance, cada fabricante puede conseguir estos objetivos a través del hardware y aplicaciones de software diferentes. Se presenta enseguida consideraciones comunes y unos de los muchos métodos potenciales utilizados para proporcionar voz sobre Frame relay.

Compresión de Voz

La compresión de voz es un resultado de remover los períodos silenciosos e información redundante encontrada en el discurso humano. Se usa compresión de la voz para reducir la cantidad de información necesitada para recrear la voz en el extremo del destino. La voz descomprimida y el facsímil requieren una cantidad grande de ancho de banda. Esto hace a menudo impráctico transmitir estas señales sobre los enlaces de acceso de baja velocidad. El uso de algoritmos de compresión de voz de bajo rango de bits, puede hacer posible proporcionar discursos de alta calidad mientras se usa el ancho de banda eficientemente.

Se usan varios algoritmos para muestrear modelos del discurso y reducir la información enviada intentando retener el posible nivel de calidad más alto de la voz. Un algoritmo ADPCM (Modulación Adaptable Delta de Código de Pulsos) relativamente simple puede reducir los datos del discurso a la mitad de PCM (Modulación de Código de Pulsos), una norma estándar de codificación de voz de la ITU consume 64 Kbps y se optimiza para la calidad del discurso. PCM es el algoritmo de la voz que normalmente se usa en redes de telefonía. ADPCM puede usarse en lugar de PCM, mientras se mantenga la misma calidad de la voz. Además de ADPCM, hay varios estándares de algoritmos de compresión de voz (ejemplo, ITU G.729), así como los algoritmos propietarios que corresponden a varios fabricantes y que proporcionan reducciones más significantes (ejemplo; a 10% o menos del de PCM) en la cantidad de información requerida para recrear el discurso al receptor.

Otros algoritmos de compresión de voz muestrean la voz más eficientemente (ejemplo, con menos bits) usando técnicas de predicción avanzadas. Estos algoritmos, además, reducen el ancho de banda requerido para mantener la buena calidad de la voz. La aplicación de estas técnicas de compresión avanzadas, y conociendo el proceso que implica, se hace posible por el uso de Procesadores de Señales Digitales (DSPs). Un DSP es un microprocesador que se diseña para procesar señales digitalizadas como aquéllas específicamente encontradas en la voz y las aplicaciones de vídeo. En los últimos diez años han ocurrido adelantos significativos en el diseño de DSPs. Este desarrollo les ha permitido a los fabricantes comercializar algoritmos de calidad de digitalización aun más altos y que consumen ancho de banda muy pequeño.

La función general de estas estrategias es escrutar la señal del discurso más cuidadosamente para eliminar las redundancias de la señal completamente, y para usar los bits disponibles para codificar las partes no-redundantes de la señal de una manera eficaz. Conforme rango de bits disponible se va reduciendo de 64 Kbps a 32, 16, 8, y 4 Kbps o debajo, las estrategias para quitar la redundancia y la posición de los bits, se va volviendo más sofisticada. El bajo costo de los procesadores de propósito general DSP y otros algoritmos de compresión avanzados permiten la posibilidad de lograr compresión de la voz dentro de los dispositivos VoFR a rangos de bits cada vez más bajos.

Cancelación de Eco

El eco es un fenómeno encontrado en redes de voz. El eco ocurre cuando la voz transmitida se refleja atrás del punto del que fue transmitida. En redes de voz, se usan dispositivos de cancelación de eco cuando la propagación del retardo aumenta al punto donde resulta el eco. La voz transmitida sobre una red de Frame Relay también enfrentará retardos de la propagación.

Cuando los aumentos de retardos de extremo-a-extremo, el eco se volverá muy notorio en el extremo-usuario si no se cancela. Si los proveedores de enlaces de acceso no usan equipo de cancelación de eco en sus redes de Frame relay, dependerá de los fabricantes suprimirlo dentro de sus equipos.

Retardo y Variación de Retardo

La naturaleza de la ráfaga y el tamaño de las tramas de Frame relay puede traer como resultado varios retardos entre paquetes consecutivos. La variación en la diferencia de tiempo entre cada paquete que va llegando se llama ***"Jitter".***

El Jitter puede impedir la habilidad del extremo receptor CPE a la fácil regeneración de la voz. Puesto que la voz es inherentemente una forma de onda continua, un hueco grande entre los paquetes de la voz regenerados podría producir un sonido distorsionado. Los fabricantes de equipo *pueden contribuir a la disminución del Jitter en la red; empleando fragmentación de paquetes* sobre los datos, para transmitir paquetes uniformes clasificados según el tamaño en la red. FRF.12 proporciona una técnica para fragmentación de datos anterior a su transmisión en una red de FR".

Para evitar perder muestras del discurso, los datos pueden almacenarse en memoria suficientemente en el decodificador del discurso para considerar el Jitter en el peor caso, a través de la red. Los fabricantes de equipo están incorporando esta característica dentro de su equipo.

Pérdida de Trama

La voz comprimida normalmente puede resistir mejor la frecuente pérdida de los paquetes al contrario de los datos. Si un paquete de la voz está perdido, será mejor que el usuario no lo note. Si ocurre la pérdida excesiva de la trama, es igualmente inaceptable para VoFR y para tráfico de los datos.

Integración de tráfico –Soporte de Facsímil y de Módem

Los Fabricantes que implementan tecnología de VoFR parecen estar imitando los servicios públicos de voz. Desde que el VoFR soporta facsímil y servicios de módem de datos también, los usuarios finales, quienes tienen altos volúmenes de tráfico de facsímil entre oficinas remotas y la oficina principal encontrarán esta característica muy provechosa.

Las señales en la banda para voz y del fax se demodulan en el equipo conectado localmente y se transmiten sobre la red como datos digitales en un paquete de formato estándar. En efecto, ***el FRAD (Dispositivo de Acceso Frame Relay)*** engaña a la máquina del facsímil haciéndolo pensar que se conecta a una máquina del facsímil remota por una red analógica. Sin embargo, es difícil de comprimir confiablemente las señales del facsímil y del módem de datos para lograr la utilización del ancho de banda cada vez que fuera necesario para la integración más eficaz sobre Frame relay. Algunos fabricantes han llevado a cabo esquemas donde la voz se comprime en un bajo rango de bits, pero desde el descubrimiento de un tono del facsímil, el ancho de banda se reasigna a un rango más alto para permitir la transmisión más rápida del facsímil.

Prioritización

La Voz, el Facsímil y algunos tipos de datos son sensibles al retardo. Esto significa que si el retardo de extremo - a - extremo o la variación del retardo excede un límite especificado, el nivel de servicio se degradará. Para minimizar el potencial de degradación de servicio, los fabricantes pueden emplear una variedad de mecanismos y técnicas.

Para minimizar el retardo de tráfico de voz, existe un mecanismo de prioritización que proporciona servicio al tráfico sensible al retardo. Los fabricantes que ofrecen equipo capaz de integrar voz y datos sobre Frame Relay pueden elegir entre usar una variedad de mecanismos propietarios para asegurar un equilibrio entre la transmisión de voz y la transmisión de datos. Aunque pueden diferir, el concepto permanece siendo esencialmente el mismo. Por ejemplo, cada tipo de tráfico de entrada puede configurarse en una de varias colas de prioridad. Pueden ponerse tráfico de voz y tráfico de facsímil en la cola de alta-prioridad, para la entrega urgente a la red. El tráfico de datos se puede configurar de baja-prioridad ya que puede ser almacenado en memoria hasta que los paquetes de alta-prioridad se envíen (Figura 3.51).

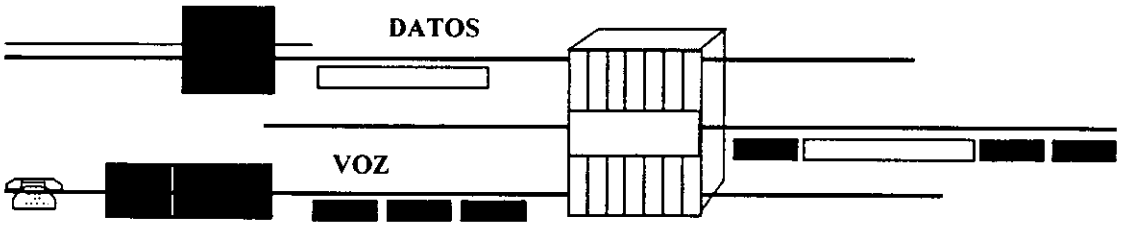


Figura 3.51 La prioritización pone el tráfico sensible al retardo, como la voz, delante de las transmisiones de datos de prioridad más baja.

Fragmentación

La fragmentación se usa para romper los bloques grandes de datos en tramas más pequeñas, creando tramas con menor retardo. Esto es otro medio para asegurar el nivel más alto posible de calidad de la voz. La fragmentación intenta asegurar un flujo igual de tramas de voz en la red y minimiza el Jitter a través de circuitos que llevan paquetes de voz y datos.

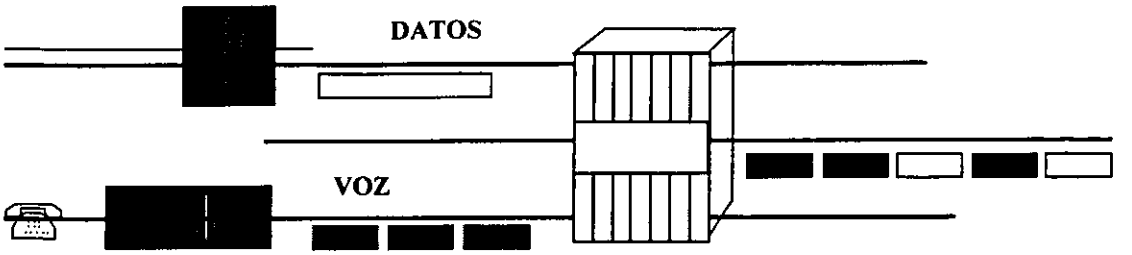


Figura 3.52. La fragmentación asegura ese tráfico de prioridad alto, como la voz no tiene que esperar para ser enviada. Pueden interrumpirse paquetes largos de datos para enviar un paquete de la voz.

La fragmentación involucra a menudo todos los datos en la red, para tener calidad de voz consistente. Esto es porque aún cuando la información de la voz se fragmenta, el retardo todavía ocurrirá si una trama de la voz se queda en el "medio" de la red, detrás de una trama de datos grande. Esta fragmentación de paquetes de datos (como se muestra en la Figura 3.52) asegura que los paquetes de voz y facsímil no se retrasen demasiado para que puedan ser aceptables cuando van detrás de paquetes de datos grandes. Adicionalmente, la fragmentación reduce el Jitter porque pueden enviarse paquetes de voz y pueden recibirse más regularmente. La Fragmentación, sobre todo cuando se usa con técnicas de prioritización, se utiliza para asegurar un flujo consistente de información de voz. El objetivo de esto y otras técnicas es permitir a la tecnología de VoFR proporcionar servicio que se acerque más a la calidad de la voz de una línea telefónica convencional. El Foro de Frame Relay recomienda el uso del Acuerdo de Aplicación de Fragmentación [FRF.12] cuando se utiliza fragmentación para VoFR.

Interpolación del Discurso digital

La interpolación del discurso digital se dirige hacia la supresión del silencio. La naturaleza de comunicación del discurso trae consigo pausas entre las palabras y frases. Los algoritmos de compresión de voz que identifican y quitan estos patrones redundantes, efectivamente reducen la cantidad de información del discurso a ser transmitido. DSI usa técnicas de procesamiento de voz avanzadas para detectar períodos de silencio y suprimir la transmisión de esta información. Aprovechándose de esta técnica, el consumo del ancho de banda que podría ser consumido muy fácilmente por este tipo de información no deseada.

Técnicas de Multiplexaje

Algunos fabricantes de equipos ***FRADs (Frame Relay Access Devices – Dispositivos de Acceso Frame Relay)***, utilizan diferentes técnicas de multiplexaje para la optimización del ancho de banda como Logical Link Multiplexing (Multiplexaje por Enlace Lógico) y Subchannel Multiplexing (Multiplexaje por Subcanal).
El Multiplexaje por Enlace Lógico permite a las tramas de voz y datos compartir el mismo PVC (Circuito Virtual Permanente). Esto puede ayudar a economizar los cargos del proveedor del PVC y aumenta la utilización del PVC.

Multiplexaje por canal es que una técnica utilizada para combinar varias conversaciones de voz dentro de la misma trama. Se reduce el overhead del paquete si se permite enviar la carga útil en la misma trama. Esto puede ofrecer entonces, aumentar el performance en los enlaces de baja velocidad. Esta técnica puede permitir conexiones de baja velocidad para transportar paquetes pequeños de voz eficazmente por la red de Frame relay.

Otras Consideraciones

Además de mantener servicios básicos como encapsulación de tráfico de datos para transporte sobre Frame relay, los FRADs son capaces de proporcionar conectividad entre PBXs y otros equipos de voz. Como resultado, el FRAD tendría que manejar diferentes tipos de tráfico y acomodar sus diferentes necesidades.

Cuando la voz se lleva sobre una red de Frame relay que emplea un Backbone ATM, no hay impacto debido al uso del backbone de ATM, ya que ATM funciona puramente como un medio de transporte.

3.19.5 Acuerdo de implementación de la Voz sobre Frame Relay (FRF.11)

Apreciación global

El Foro de Acuerdos de Implementación de Frame Relay, proporciona convenios y bases para los fabricantes y proveedores para desarrollar equipos y servicios que tengan interoperabilidad. En el caso de VoFR, como con muchas tecnologías que están surgiendo, los fabricantes pueden a menudo desarrollar y desplegar capacidades antes de que la industria y las organizaciones de usuarios logren acuerdos generales en las normas y aplicaciones.

FRF.11 proporciona entonces, un entorno para un acuerdo y bases para VoFR y para que las compañías puedan construir el equipo y servicios de la oferta que serán entre sí capaces de interoperar de manera funcional.

El IA se dirige a lo siguiente:

- El transporte de voz comprimida dentro de la carga útil de una trama Frame relay, vía el apoyo de un juego diverso de algoritmos de compresión de voz como CS-ACELP, LD CELP, MP-MLQ, PCM, etc.
- Utilización eficaz de las conexiones Frame relay de bajo rango de bits.
- Multiplexaje de hasta 255 canales subalternos en un sol DLCI Frame relay, tal que un solo DLCI puede contener tanto voz como carga útil de datos
- Soporte para carga de voz en el mismo o diferente canal(es) subalterno(s) dentro de una sola trama.

Modelo de la referencia

El modelo de la referencia para VoFR se muestra en la Figura 3.53. Usando la VoFR, se hace posible para cualquier tipo de VFRAD, como el que se muestra en el lado izquierdo de la Figura 3.53, intercambiar voz e información de señalización con cualquier tipo de VFRAD en el lado derecho de la Figura 3.53.

Se muestran tres tipos de dispositivos en la Figura 3.53. La capa de arriba muestra dispositivos sistemas terminales similares a teléfonos o máquinas facsímil; la capa media muestra dispositivos de multiplexaje transparente similares a bancos de canales; la capa de abajo muestra dispositivos de sistemas de conmutación similares a PBX.

Un VFRAD conecta los dispositivos vía las interfaces físicas como las definen en [FRF.1.1].

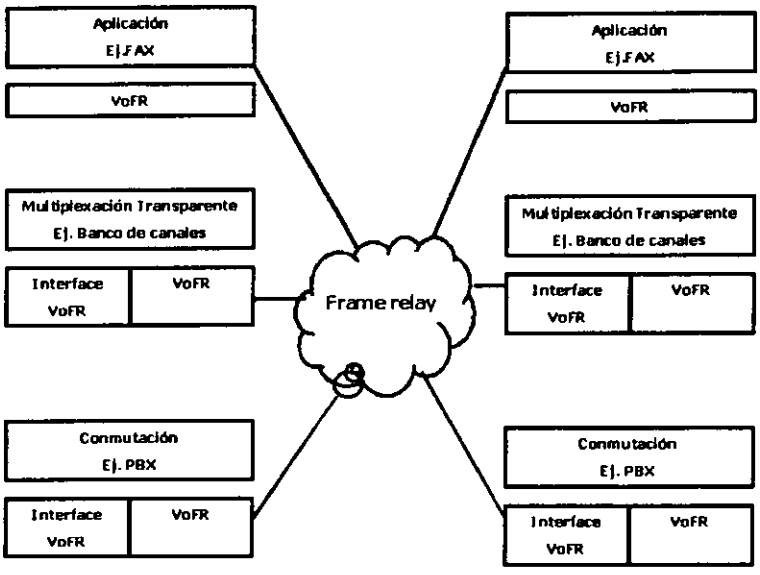


Figura 3.53. Modelo de Referencia Modelo de una Red de Voz Sobre Frame Relay

Resumen

Frame Relay está empezando a evolucionar de una sola, aplicación tecnológica a una tecnología con un espectro ancho de usos. La integración de voz y datos sobre Frame relay representa uno de muchas áreas prometedoras de desarrollo que no sólo podría beneficiar a los usuarios terminales, sino que podría continuar el crecimiento de servicios de Frame relay y aplicaciones.

La tecnología VoFR consolida voz y datos (ej. facsímil y los modems analógicos) con servicios de datos sobre la red de Frame relay. Tiene el potencial para proporcionarles mayor eficacia a los usuarios finales con el uso de ancho de banda y de acceso y proporcionarles transporte rentable de tráfico de voz a los usuarios finales para comunicaciones internas de la compañía.

3.20 Historia de ATM

En el desarrollo y definición de la tecnología ATM intervienen principalmente 2 tipos de organizaciones: los organismos de estandarización y los foros de la industria. Entre los primeros se encuentra el ITU-UT, el cual dio inicio con las especificaciones de ISDN en los 70's, para luego definir la BISDN en los 80's dentro del Libro Azul, incluyendo el ATM como una parte fundamental. Junto con el ITU-UT podemos mencionar al ANSI como el organismo de estandarización de Estados Unidos para ATM y la ETSI para Europa.

El Foro de ATM se formó en 1991 por cuatro compañías: Northern Telecom, Sprint, SUN Microsystems y DEC. En enero de 1992, la membresía se hizo extensiva para toda la industria, habiendo actualmente 3 categorías: principal, auditor y usuario. Sólo los miembros principales pueden participar en las reuniones del comité; los miembros auditores reciben copias de los documentos, mientras que los miembros en categoría del usuario participan en las juntas del la ***ENR (End User Roundtable – Mesa Redonda del Usuario Final).***

El ENR se formó en agosto de 1993 con el objetivo de hacer llegar a los comités del Foro los requerimientos de alto nivel.

En enero de 1994, el Foro tenía aproximadamente 150 miembros principales, 300 auditores y 25 miembros usuario.

3.20.1 Definición Modo de Transferencia Asíncrono

El Modo de Transferencia Asíncrono (ATM por sus siglas en inglés) se define como una tecnología para la transferencia de información entre redes de datos. Esta tecnología, relativamente nueva, tiene algunas características que hacen que se vislumbre como la tecnología del futuro; tecnología que ha de sustituir paulatinamente a las utilizadas actualmente a redes de cobertura amplia.

Pero, ¿es ATM realmente la panacea que viene a resolver los problemas de interconectividad con que no topamos actualmente? O ¿es sólo la tecnología de moda de la que todo el mundo habla y que después desaparece bajo la sombra de otra más nueva?

En el cuadro siguiente se analizan las características más importantes de ATM, considerando que el tipo de aplicación varía en función del software utilizado para determinar el ancho de banda requerido y la siguiente tabla es solo una muestra representativa.

TIPO DE APLICACION	FUNCIONES TIPICAS	AMPLITUD TIPICA DEL MENSAJE	TIEMPO DE RESPUESTA (SEG.)	ANCHO DE BANDA REQUERIDO
Automatización de oficina	Analizar y recuperar datos alfanuméricos	1.2 a 4.3 Kbytes	1 a 3	6 a 70 Kbps
Oficinas virtuales (para seguridad, estado real, etc.)	Analizar y escala de grises e imágenes a color para base de datos	Escala de grises: 30 a 60 Kbytes Color: 250 a 500 Kbytes	1 a 5	1 a 8 Mbps
Transmisión de imágenes (para publicidad)	Transmisión de fotografías	Más de 1 Mbytes	10	800 kbits a 5 Mbps
Médica o CAD/CAM	Transmisión de rayos X y otras imágenes a altas resoluciones	10 Mbytes	2	40 Mbps
Financiera	Transmisión a escala de grises	35 a 75 Kbytes por chequeo	0.025 por imagen	10 a 24 Mbps
Científica	Visualización	80 Kbytes a 3 Mbytes	0.03 a 1	600 Kbps a 800 Mbps

Tabla 3.6. Necesidades típicas de ancho de banda en aplicaciones cliente - servidor

3.20.2 Elementos de ATM

Celdas ATM. ATM funciona con base en la conmutación y multiplexaje de celdas; un método similar a la conmutación de paquetes en X.25 o conmutación de tramas en Frame Relay, analizados anteriormente. La celda es la unidad principal en ATM y ha sido definida con un tamaño fijo de 53 bytes (424 bits). Al igual que en otras tecnologías basadas en conmutación de paquetes existen celdas de propósito especial que dan lugar a la aparición de los distintos tipos de celdas que se mencionan a continuación.

- **Tipos de celdas ATM**

1. Celdas no utilizadas
   a) Ajuste de velocidad de transferencia del medio
   b) Sincronización del medio físico
   c) No pasan a la capa ATM

2. Celdas no asignadas
   a) Contienen VPI/VCI
   b) No soportan datos

3. Celdas VP/VC
   a) Datos del usuario
   b) Señalización de *broadband*
   c) VC OAM
   d) SMDS
   e) ILMI

Existen dos codificaciones estándar para la estructura de la celda: la UNI (Interface de Usuario a Red), que se muestra en la figura 3.54 y la NNI (Interface de Red a Red), que es similar a la que aparece en la figura excepto que no contiene GFC y el VPI ocupa 8 bits.
Ambas se detallan en las figuras 3.58 y 3.59.

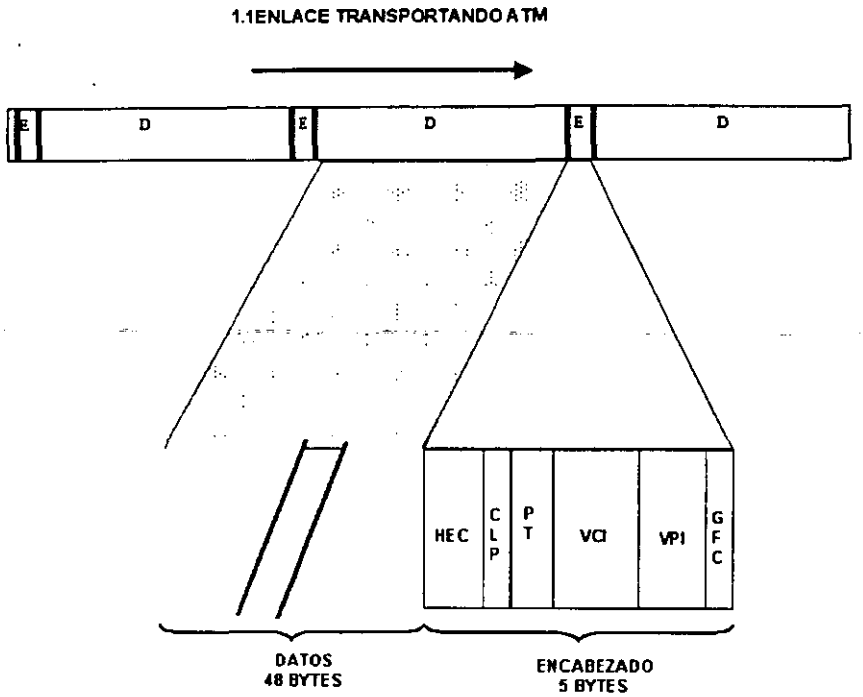


Fig.3.54 Estructura de una celda ATM.

Los nombres de los campos del encabezado de la celda son como sigue:

GFC Control Genérico de Flujo (Generic Flow Control)
VPI Identificador de Ruta Virtual (Virtual Path Identifier)
VCI Identificador de Canal Virtual (Virtual Channel Identifier)
PT Tipo de Información (Paiload Type)
CLP Prioridad de la Celda (Cell Loss Priority)
HEC Chequeo de Errores en Encabezado (Header Error Check)

Cualquier tipo de información que vaya a ser transportada en una red ATM se corta en "pedazos" de 48 bytes, y a cada uno de estos pedazos se le agrega un encabezado de 5 bytes (completando los 53 bytes reglamentarios), que incluye los campos mencionados, de modo que los nodos de conmutación de la red (*ATM switches*) sólo se encargan del manejo de estas celdas con base en la información que lleva su encabezado.

A diferencia de los paquetes X.25, en las celdas ATM sólo se verifican errores en el encabezado (mediante el campo HEC), dejando la detección y corrección de errores en la información a las capas más altas en los equipos de usuario.
Una vez que las celdas llegan a su destino, se les retira el encabezado anexo y se vuelven a reunir reconstruyendo de esta manera la información original.

Ahora que ya se tiene una idea de cómo funciona una red ATM, se analiza una red de dos nodos que maneja imágenes, voz y datos. En la figura 3.55 se muestra la operación TDM.

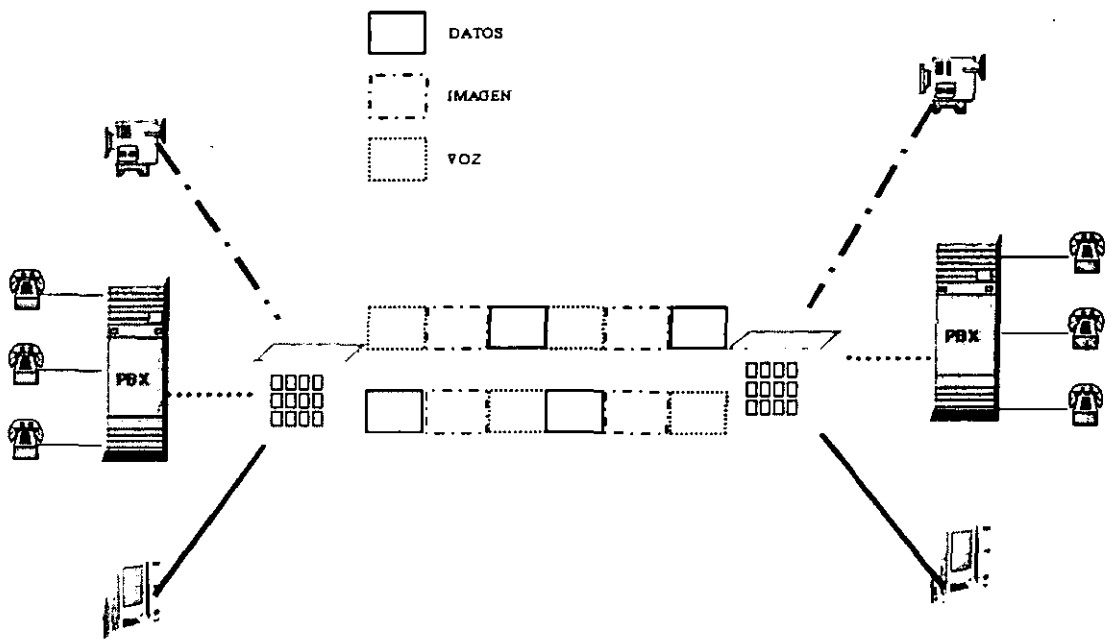


Fig. 3.55 Red con enlace TDM

En el enlace TDM del ejemplo se asigna una ranura de tiempo fija para el canal de imágenes, otra parte para el canal de voz y una última para el canal de datos. Estas ranuras permanecen fijas sin importar si se utiliza el canal o no. Por ejemplo, si en algún momento no se usa el canal de vídeo ni el de voz, el canal de datos seguirá disponiendo sólo del ancho de banda (entiéndase velocidad) que le fue asignado.

Se aprecia el comportamiento de la misma red pero con tecnología ATM tal como se muestra en la figura 3.56.

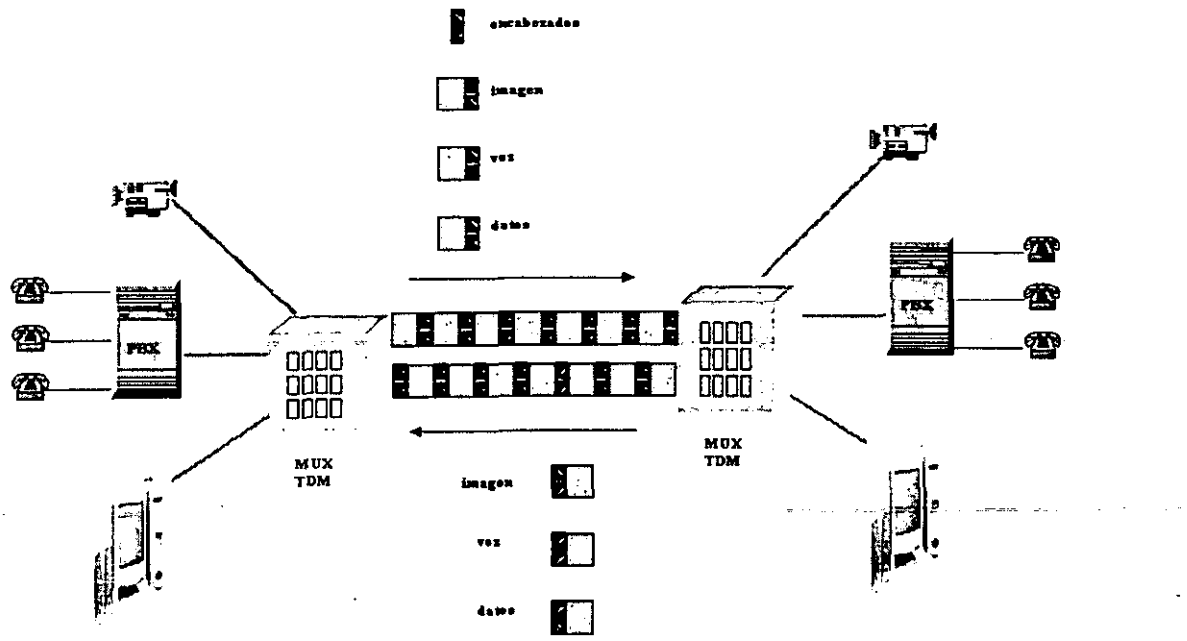


Fig. 3.56. Red con enlace ATM

En este caso, si dejan de utilizar el enlace las aplicaciones de voz y vídeo, las celdas ATM en el enlace son empleadas para transportar información del canal de datos, usando todo el ancho de banda del enlace para la aplicación de datos, optimizando de esta manera la utilización del mismo. Una vez que las aplicaciones de voz y vídeo vuelven a emplear el enlace, los datos regresarán a su velocidad normal.

Como se ve con este ejemplo, una de las principales ventajas de ATM comparada con TDM, es la mejor utilización del ancho de banda. Sin embargo, esto se logra haciendo más complejos los equipos de conmutación. En el caso de los multiplexores TDM, sólo se configuran al instalarse, asignando el ancho de banda disponible entre los circuitos o canales, repartiéndolo. Una vez que la red queda configurada estos equipos requieren muy poca atención. No así los equipos ATM, puesto que tienen que manejar las celdas correspondientes a los distintos canales con base en sus encabezados (dirección, prioridad, etc.). Además, tienen que implementar sistemas de control de flujo para corregir o recuperar estados de congestión en la red, todo esto incrementa la complejidad de los conmutadores ATM.

Se aprecia de manera sencilla para qué sirve cada uno de los campos del encabezado de las celdas.

Cada uno de los campos se describe bajo los siguientes encabezados con el nombre de la función que cumple la información en cada campo.

3.20.3 Direccionamiento

La dirección de la celda está contenida en los campos VPI y VCI (Identificador de Ruta e Identificador de Canal, respectivamente, por sus siglas en inglés); estos indican la dirección hacia donde se dirige la celda. Funcionan igual a los DLCIs (Identificadores de Conexión de Enlace en Frame Relay); es decir, cuando un conmutador ATM recibe una celda, el VPI y VCI dicen la procedencia de la celda, después se los cambia a la celda con base en una tabla de "conexiones" almacenada en su base de datos, y la envía por el siguiente enlace hacia el próximo nodo (conmutador o equipo de usuario). Es por esto, que los VPI, VCI en ATM tienen significado "local" solamente, dado que direccionan la celda hacia el nodo próximo, pero la ruta completa se establece con base en la configuración de las tablas de conexiones de los conmutadores.

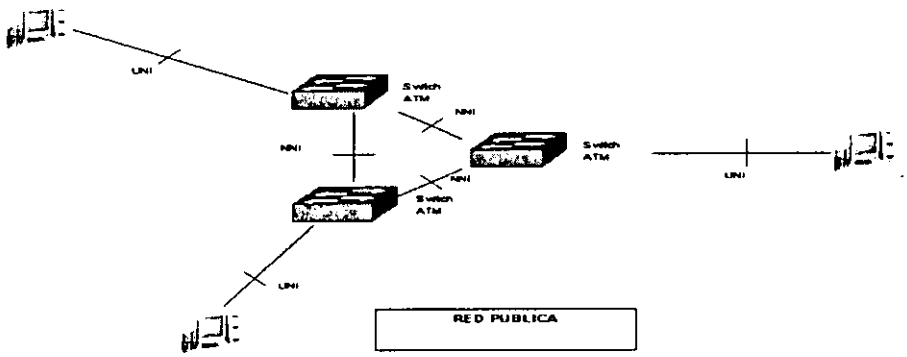


Fig. 3.57. Red Pública

En ATM están definidos dos tipos de interfaces, dependiendo si ésta conecta con un nodo de red NNI o con un nodo de usuario a red (UNI). La interface de UNI soporta hasta 256 rutas virtuales (VPIs), la interface de Red a Red (NNI) soporta hasta 4,096 rutas virtuales y cada ruta virtual UNI o NNI, puede contener hasta 65,536 canales virtuales (VCIs).

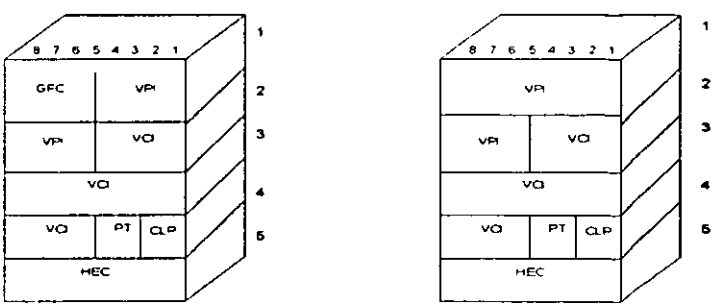


Figura 3.58 Formato de celda UNI y Fig.3.59 Formato de celda NNI.

Control de Flujo

El primer campo de la celda (GFC) le permite a un conmutador ATM controlar la velocidad de un equipo de usuario que va a comunicarse a través de la red de acuerdo a las condiciones de ésta; por ejemplo si está congestionada.

Tipo de Información

El campo PT le indica al conmutador la clase de información que forman los datos de la celda. Existen celdas con datos de usuario, de señalización y de mantenimiento.

Prioridad de la Celda

CLP es el bit de las celdas ATM que corresponde al bit DE en las tramas Frame Relay. Este le indica al conmutador si la celda es prioritaria o no, si tiene prioridad se descartará como última instancia en caso de congestión; las celdas sin prioridad son las primeras que se descartan durante los episodios de congestión.

Cada aplicación tiene diferentes requerimientos de comunicación. Por ejemplo, un enlace de voz o un enlace de videoconferencia requieren que la información llegue a su destino a una velocidad fija para operar correctamente, de ahí que se consideren aplicaciones de velocidad fija ***CBR (Constant Bit Rate Applications)***. El CBR funciona de manera similar al que funciona un canal asignado de un multiplexor TDM, en otras palabras, el canal es asignado se use o no. Si esto se cumple, no importa si se pierde uno que otro bit en el enlace ya que sólo se percibirá como una interferencia momentánea en la imagen o en la voz.

En cambio una aplicación de datos, el correo electrónico por ejemplo, requiere que la información llegue completa, no es aceptable la pérdida de un sólo bit en archivos de aplicaciones críticas de diseño o investigación científica, pero en este tipo de aplicación no importa si un archivo tarda dos segundos en llegar y el siguiente tarda diez. Estas se conocen como aplicaciones de velocidad variable ***VBR (Variable Bit Rate Applications).***

Transporte

Existen proveedores de switches ATM que pueden transportar voz y video mediante VBR optimizando aún más los anchos de banda.

Como ATM es una tecnología ideada para transportar cualquier tipo de información, tal y como se ve en el ejemplo, necesita contar con mecanismos que le permitan tratar de manera diferente a cada tipo de comunicación que viaje en la red.

El mecanismo con que cuenta ATM para diferenciar los tipos de información transportados es la Calidad de Servicio (QoS). ITU-T definió cuatro clases de servicios nominadas A, B, C y D con las siguientes características de calidad:

- Clase A: Servicio de Velocidad Constante (CBR), orientado a conexión con señal de reloj de extremo a extremo.
- Clase B: Servicio de Velocidad Variable (VBR), orientado a conexión con señal de reloj de fin a fin.
- Clase C: Servicio de Velocidad Variable, orientado a conexión sin señal de reloj requerida.
- Clase D: Servicio de Velocidad Variable, orientado a no conexión y sin señal de reloj requerida.

En una red ATM debe definirse una clase de servicio a cada circuito virtual, permanente o conmutado, para que la aplicación que utiliza determinado circuito se asegure de recibir la clase de servicio que demanda.

ATM tiene capas definidas para cada función, mismas que se muestran en la siguiente figura 3.60.

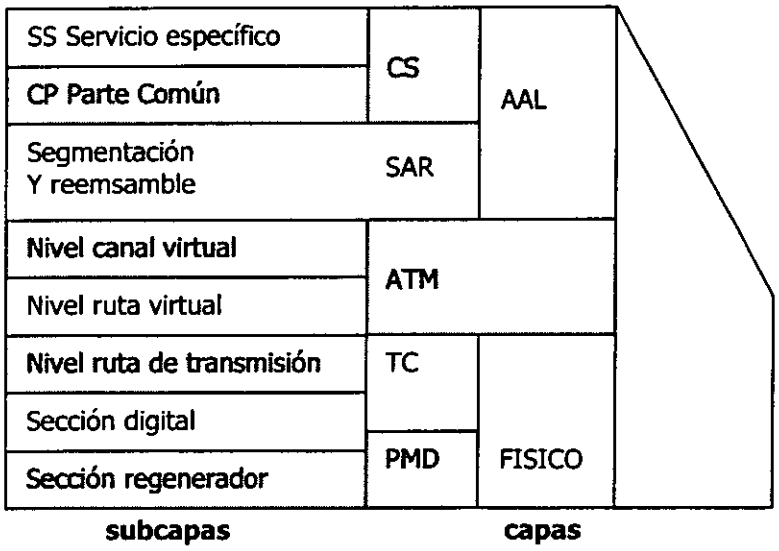


Fig. 3.60 Modelo de ATM.

El ITU-T, ANSI y Foro de ATM seleccionaron el modo de transferencia asíncrono como parte de las especificaciones de B-ISDN que provee la convergencia, la multiplexión y conmutación de celdas. En otras palabras, el ATM está basado en el modelo B-ISDN.

Modelo de niveles ATM

Nivel físico: la función en general del nivel físico de ATM es verter celdas ATM en el medio físico para enviarlas a otro nodo y recuperar las celdas recibidas desde otro nodo. El nivel físico se divide en dos partes***: PMD (Physical Medium Dependent)***, tren de bits encargado de generar la señal física inyectada al medio, también se define en este nivel el tipo de interface (E3, DS3, E4, etc.), así como la velocidad; y ***TC (Transmision Convergence)*** que se encarga de convertir las celdas ATM, provenientes del nivel superior, en una corriente estable de bits para entregarlo a PMD y de reagrupar en celdas ATM el tren de bits que recibe desde PMD, para entregarlas a la capa de ATM. Otra función importante realizada por TC es el desacoplamiento de velocidad según la recomendación I.321 de ITU-T; cuando se utiliza una interface cuya velocidad definida no es un múltiplo de 53 bytes se realiza el desacoplamiento de velocidad insertando celdas vacías y retirándolas durante la recepción. El foro de ATM asigna esta función a la capa ATM. Cuando se seleccione equipo ATM es recomendable que soporte ambos métodos para asegurar una mejor interoperabilidad.

Nivel ATM: La función básica de este nivel es mantener las rutas y canales virtuales (VPs y VCs) esto lo realiza interpretando y asignando los identificadores de ruta y de canal (VPIs y VCIs) a las celdas que pasan por él.

Nivel AAL (ATM Adaptation Layer): posiblemente se trate del nivel más importante de ATM dado que es el que permite ofrecer las diferentes clases de servicio (QoS) para soportar la conexión a la red ATM de los diferentes equipos que requieren una conexión, y comunicarse con otros equipos de su especie, por ejemplo: PBXs, ruteadores, equipos de videoconferencia, etc. Es en esta capa donde se reciben los datos de las capas superiores en forma de ***PDUs (Unidades de Datos de Protocolo).*** Normalmente un PDU es mucho mayor en tamaño que la parte de datos de una celda ATM, así que estas tramas se cortan en segmentos de 48 bytes para formar las celdas ATM que viajarán por la red. Cuando estas celdas lleguen a su destino se les retirarán los encabezados y se volverán a reunir para recuperar el PDU en su forma original. Existen AALs específicos para cada tipo de servicio. Por ejemplo, existe un Nivel de Adaptación ATM (AAL) para soportar el transporte de tramas TCP/IP sobre ATM, y ya hay definidos AALs para otros servicios.

El éxito de ATM en el futuro (el que llegue realmente a sustituir otros protocolos en uso actualmente) depende del desarrollo de AALs para el total de la gama de servicios que podrían aprovechar las bondades de ATM.

En una red ATM se distinguen dos tipo de nodo: los de ***Conmutación*** que sólo reciben celdas ATM en una interface y las conmutan entre otras interfaces de acuerdo a sus tablas, y los nodos ***Finales*** o de acceso, los cuales realizan funciones en la capa AAL al convertir la información de usuario en celdas ATM y viceversa.

Por último haremos una diferenciación entre VPs-VCs, VPIs-VCIs y VPCs-VCCs. Las Rutas Virtuales (VP) son rutas establecidas de fin a fin sin importar cuantos nodos haya en el medio, al igual que los Canales Virtuales (VC), solo que un canal virtual, transporta un sólo circuito dentro de una ruta, los Identificadores de Ruta Virtual (VPI) e Identificadores de Canal Virtual (VCI) son los campos en el encabezado de las celdas que contienen la información que indica a los nodos ATM hacia dónde enviarla. Por último, la Conexión de Ruta Virtual (VPC) es el tramo de una Ruta Virtual entre dos nodos solamente, y la Conexión de Canal Virtual es también la trama de un canal virtual que corre entre dos nodos de la red.

En el entorno ***CO (Oficina Central),*** la tecnología ATM se reduce a conmutadores con dimensiones y capacidades superiores a sus contrapartes diseñadas para ***CPE (Equipo Local del Cliente)*** o ***Ca (Campus).***

Los conmutadores para oficina central son el *backbone (espina dorsal)* de una red ATM, a menudo sólo manejan interfaces de ATM y requieren capacidades de conmutación superiores a 5 Gbps. A través de las interfaces ATM se reciben las solicitudes de establecimiento de llamada procedentes de los conmutadores ***CPE (Equipo Local del Cliente)*** existentes a lo largo de la red; es muy similar a la relación existente entre las centrales telefónicas y los PBX localizados en las instalaciones de una organización.

Este tipo de sistemas normalmente tienen la habilidad de expander su capacidad de procesamiento y puertos.

3.21 Aplicación de tecnología ATM a interconexión de redes

En esta sección del capítulo, trataremos los tipos de sistemas desarrollados por los distintos fabricantes de ATM y sus características. Se analizan aspectos de primordial importancia para los responsables de seleccionar los productos que integrarán la solución óptima de acuerdo a las necesidades de la red corporativa.

La tecnología ATM en general se enfoca principalmente al problema de la conmutación de celdas y a las funciones de adaptación. Los equipos ATM pueden agruparse de acuerdo al entorno de operación para el cual fueron diseñados, estos entornos son: ***Local del Cliente (Customer Premise Equipment o CPE)***, ***Campus (Ca)*** y ***Oficina Central (Central Office o CO)***.

Sistemas para las instalaciones del usuario final de una red ATM

La principal función de estos sistemas es proporcionar conectividad física y eléctrica entre los equipos que se encuentran en las instalaciones de la organización y la red ATM, así como efectuar la conversión del tráfico procedente de PBXs, PCs, LANs, multiplexores, ruteadores, etc. Al formato de la celda ATM.

Es indudable que una aplicación importante dentro de las instalaciones de una organización es su LAN, es por eso que primeramente se revisan los dispositivos ATM para aplicaciones LAN, continuando con el resto de los sistemas locales.

Hay casos en que la cantidad de usuarios y el poder de las aplicaciones corriendo sobre la LAN es tal, que el rendimiento de la tecnología Ethernet y Token Ring convencional no es suficiente. Como respuesta a esta situación se han desarrollado nuevas tecnologías LAN de alta velocidad.

La tecnología ATM es una de las opciones disponibles actualmente para implantar una LAN de alta velocidad (25 Mbps, 155 Mbps o más) con la ventaja adicional de poder integrarse a una WAN pública y/o privada de manera natural.

En este caso los concentradores, servidores y segmentos LAN se conectarán a conmutadores LAN con interfaces ATM mediante las cuales se comunicarán al conmutador ATM para trabajo en grupo. Las PCs, servidores y estaciones de trabajo en las que corren aplicaciones demandantes de ancho de banda, podrán conectarse directamente al conmutador ATM para trabajo en grupo a una velocidad de 25 Mbps, 155 Mbps mediante una Tarjeta de Interface de Red ATM (NIC ATM). A continuación se describen brevemente las características y funcionamiento de cada uno de los dispositivos mencionados.

Estos son algunos de los medios físicos de transporte en ATM:

1. Interface WAN DS3 a 45 Mbps.
2. SONET OC a 155 Mbps.
3. Multimodo a 100 Mbps (basado en FDDI).

Tarjeta de Interface de Red ATM

Las NIC cuentan con una interfaz física ATM y se instalan directamente en el bus de una poderosa PC, servidor o estación de trabajo; de esta manera pueden conectarse directamente al conmutador ATM.

En la PC, servidor o estación de trabajo, se requiere una API que permita la interoperabilidad entre el sistema operativo local y el sistema operativo de red con la NIC instalada en el bus. La NIC y la API, en conjunto, efectúan la función de conversión de los paquetes de datos en celdas ATM, adaptándolas para su transmisión sobre la interface física de la tarjeta de acuerdo a la recomendación UNI.[9.3].

Puente o conmutador LAN con soporte de ATM

Para la conexión de segmentos LAN (Ethernet por ejemplo) a algún tipo de dispositivo ATM, se requiere de un adaptador que soporte interfaces Ethernet (como 10 BaseT), interfaces ATM (como OC-3) y que efectúe, además, la conversión de tramas Ethernet al formato ATM.

En el mercado pueden encontrarse dispositivos que cuentan con una sola interfaz LAN y una sola interfaz ATM, por lo que su función es la de un *bridge*. Otros dispositivos son los conmutadores LAN (*LAN switches*) soportando una o más interfaces ATM, permitiendo que varios segmentos LAN conmutados tengan acceso a la red ATM.

Conmutador ATM para trabajo en grupo

Conocido también como *ATM Workgroup Switch*, este conmutador es por lo general pequeño, soporta exclusivamente interfaces ATM y se utiliza principalmente para aplicaciones LAN, recibe las conexiones de los *LAN switch/ATM* de la organización y de los sistemas de cómputo que cuentan con una NIC ATM. Como características principales figura que son sistemas limitados a 8 o 16 puertos por sistema, velocidad de conmutación de 1 o 2 Gbps y conmutación de celdas ATM. La función de adaptación de tráfico no ATM debe ser realizada por alguno (s) de los dispositivos mencionados anteriormente. Es utilizado principalmente en ambientes CPE y en algunos casos en Campus. En la figura 3.61 se muestra la manera en que se utilizarían los sistemas ya descritos en la integración de una LAN de alta velocidad con tecnología ATM.

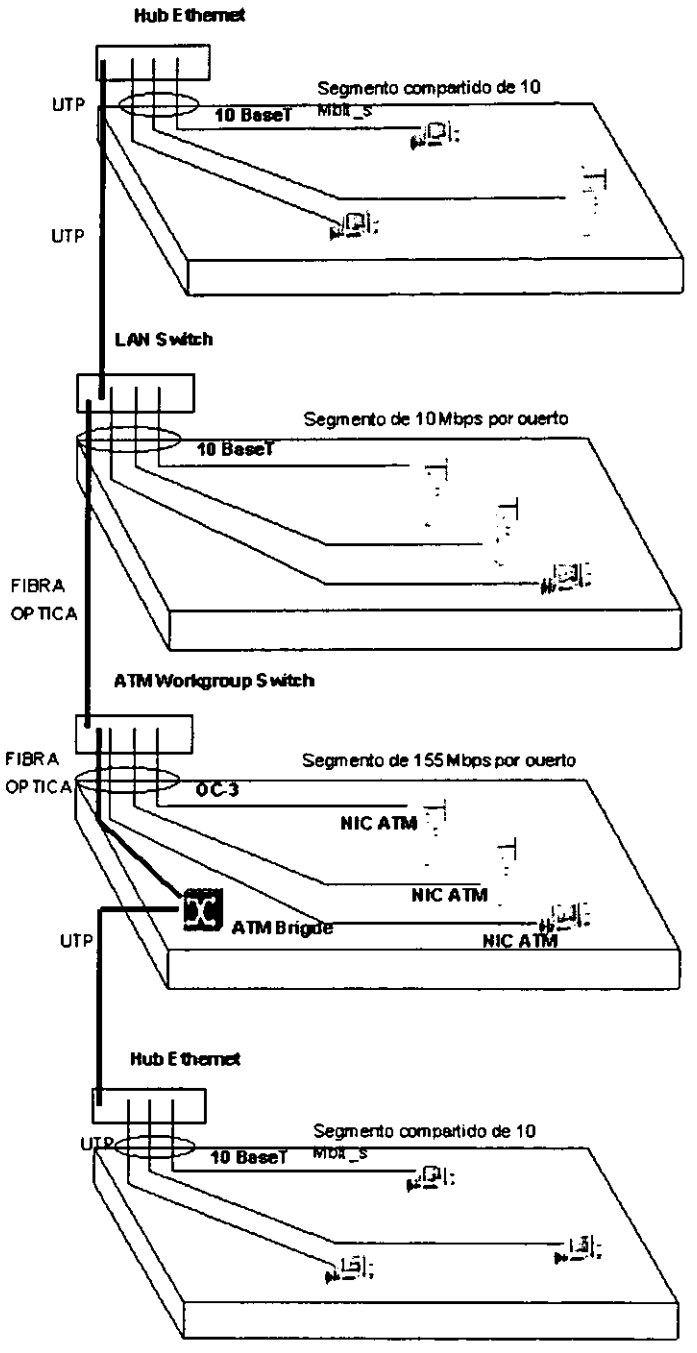


Figura 3.61 Aquí puede apreciarse como interactúan los distintos sistemas ATM para una aplicación LAN en un edificio corporativo.

3.21.1 El conmutador ATM integrador

Hasta este momento los conmutadores mencionados están limitados a aplicaciones LAN, ahora se trata de sistemas que efectúan un mayor número de funciones y soportan una variedad más amplia de interfaces, es por eso que reciben el nombre de integrador ya que simplifican el caos causado por la diversidad de equipos encontrados en las instalaciones de la organización. También se les denomina ***Enterprise Consolidators, Enterprise Network Switch, Network Consolidators o Adapting Switches***.

No sólo realizan la función de adaptación (AAL) al formato ATM de tráfico LAN, adicionalmente son capaces de adaptar tráfico CBR, como la voz y el vídeo digitalizados y soportan la conexión a troncales T1/E1procedentes de un PBX. Algunos fabricantes de *Enterprise Switches* soportan interfaces de vídeo que reciben la señal analógica de cámaras u otros generadores de imágenes, la digitalizan y la comprimen de acuerdo a un algoritmo de compresión como JPEG o MPEG. El resultado es la transmisión de vídeo de alta resolución. Así también soportan otras interfaces como: RS-232, V.35, 10BaseT, FDDI, T3/E3, OC-3/STM-1, E2, OC-12, etc. En la figura 3.62 se aprecia un ejemplo de este tipo de sistemas.

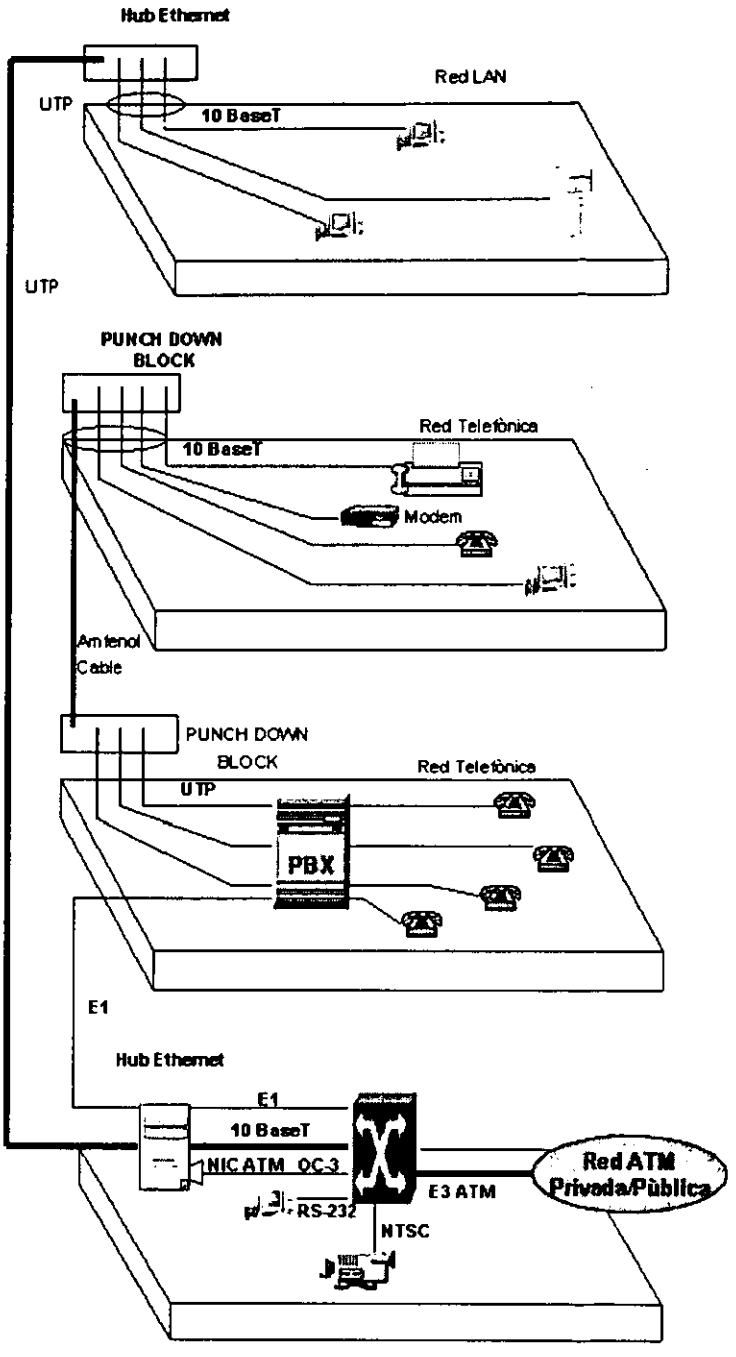


Figura 3.62 El tráfico de voz, datos y vídeo generado en un edificio corporativo se integra a un enlace ATM hacia la WAN.

3.21.2 Sistemas ATM para CAMPUS

En un ambiente de Campus, la tecnología ATM se reduce a conmutadores más pequeños que los de tipo CO y capacidades de conmutación normalmente inferiores a 5 Gbps. Por otro lado, cuentan con una variedad más amplia de interfaces como: LAN, MAN, SNA, X.25 y voz. En algunos casos, además, proveen la conversión de protocolos y emulación LAN.

Sistemas ATM para Oficina Central

En el entorno Oficinas Centrales (CO), la tecnología ATM se reduce a conmutadores con dimensiones y capacidades superiores a sus contrapartes diseñadas para ambientes CPE o Campus. Los conmutadores para Oficina Central son la espina dorsal de una red ATM, a menudo sólo manejan interfaces de ATM nativo y requieren capacidades de conmutación superiores a 5 Gbps.

A través de las interfaces ATM se reciben las solicitudes de establecimiento de llamada, procedentes de los conmutadores CPE existentes a lo largo de la red, esto es muy similar a la relación existente entre las centrales telefónicas y los PBX localizados en las instalaciones de una organización. En la figura 3.63 se ejemplifica la interconexión de los distintos tipos de conmutadores ATM.

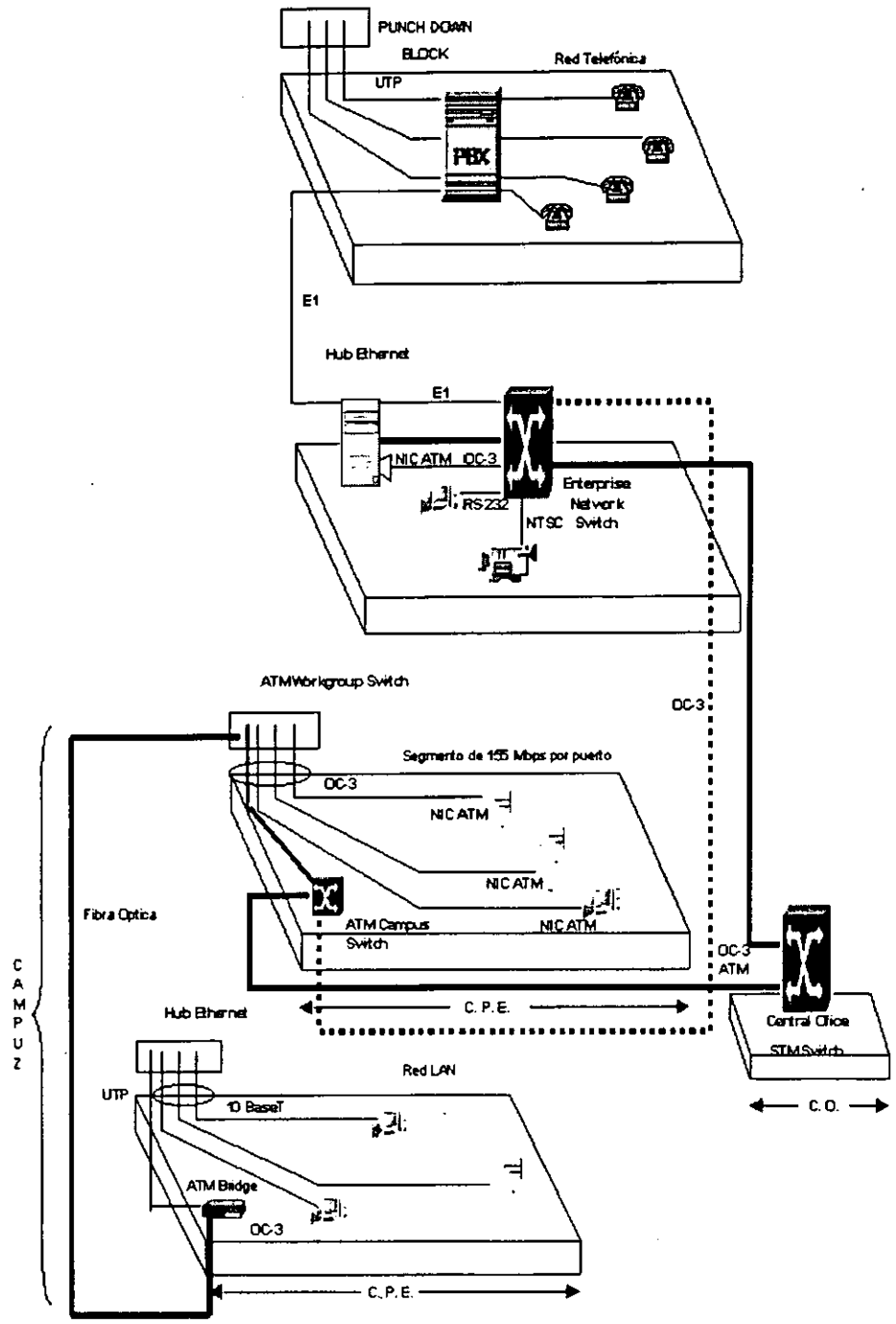


Figura 3.63 Esquema que muestra la interconexión de los distintos conmutadores y sistemas ATM para entornos CPE, Campus y CO.

3.21.3 EMULACION LAN (LANE)

Conforme más organizaciones están adoptando Modo de Transferencia Asíncrona (ATM) como parte de sus redes, requieren seguir soportando sus LANs Ethernet o Token Ring existentes. Primero, los usuarios quieren aplicaciones que corran sobre su red de manera transparente, ya sea que su red sea Ethernet, Token Ring o ATM LAN. Segundo, los administradores de red requieren más opciones para aumentar el funcionamiento de su red y asegurar la interoperabilidad protegiendo a la vez sus inversiones en infraestructuras LAN existentes.

Estas consideraciones las podemos encontrar en las funciones de conversión LAN-to-ATM (Red de Area Local a adoptando Modo de Transferencia Asíncrona), proporcionado por el Foro de ATM con el protocolo de EMULACION LAN (LANE), el cual permite a las aplicaciones correr transparentemente sobre una red ATM.

El protocolo LANE define cómo las estaciones en un extremo se comunican entre sí a través de una red ATM y cómo los servidores conectados a la red ATM se comunican con los dispositivos conectados en las LANs Ethernet o Token Ring.

LANE es un protocolo puente de capa 2 que hace que una conexión orientada de protocolos y aplicaciones de capas más altas en una red ATM parezcan un segmento más de la red Ethernet o Token Ring sin conexión. Como un servicio de capa 2, LANE puede manejar protocolos enrutables, tal como TCP/IP, Novell IPX y DECnet, también los no enrutables como NetBios y SNA.

Con LANE, las organizaciones pueden tomar ventaja de las velocidades más altas soportadas por ATM y dispositivos de acceso ATM sin reemplazar sus inversiones en Hardware, Software y Aplicaciones LAN. Las estaciones Ethernet, Token Ring o ATM continuarán comunicándose aún en la misma LAN utilizando los procedimientos estándares, ya que el backbone ATM es transparente para el usuario. Cada LAN emulada también representa una LAN virtual (VLAN) operando sobre la red LAN ATM, la cual da a las organizaciones aprovechamiento basado en los estándares al implementar VLANs.

Como trabaja la LANE

El protocolo LANE emula un segmento LAN proporcionando el servicio de broadcast que requieren los protocolos de capa de red sin necesidad de conexión. Este lleva a cabo la conversión de datos necesaria entre los paquetes LAN y las celdas ATM, y resuelve las direcciones de Control de Acceso al Medio (MAC) en direcciones ATM.

Sin embargo, el protocolo LANE no emula todos los protocolos MAC, por ejemplo, no soporta el Acceso Múltiple con Detección de Portadora con Detección de Colisión (CSMA/CD) para Ethernet o Token Ring.

Mientras que el actual estándar LANE define LANs emuladas separadas para Ethernet y Token Ring, no define explícitamente cómo conectar estos dos tipos de LANs directamente. Un ruteador equipado con ATM, con un procesador de interfaz ATM (AIP), actuando como un cliente en la LAN emulada, puede proporcionar esta conectividad permitiendo a la vez, que el administrador construya "Firewalls" (Paredes de fuego que restringen el paso de usuarios a la red local) o filtrar tráfico entre LANs emuladas.

El protocolo LANE no define la emulación de LAN tipo Interfaz de Datos de Fibra Distribuida (FDDI). Sin embargo, un ruteador o un switch puede puentear el tráfico FDDI en un servicio LANE ATM después de convertir los paquetes ya sean Ethernet o Token Ring.

Dos aplicaciones primarias que pueden utilizar el protocolo LANE para integrar redes incluyen:

Servidores centralizados y utilizando adaptadores ATM para conectarlos directamente a una red ATM. Los adaptadores ATM se interconectan con la red ATM, pero deberán presentar la interfaz de servicio LANE a los manejadores de protocolo de nivel más alto dentro del servidor conectado.
La integración de las LANs existentes sobre un backbone de transporte de alta velocidad ATM. Los administradores de red pueden cumplir con la integración de la LAN con ruteadores y con switches LAN, los cuales usan el protocolo LAN par implementar VLANs. Con LANE implementado en estos dispositivos de interconexión, no se necesitan cambios a los adaptadores de las estaciones de trabajo u otro hardware de estación remota.

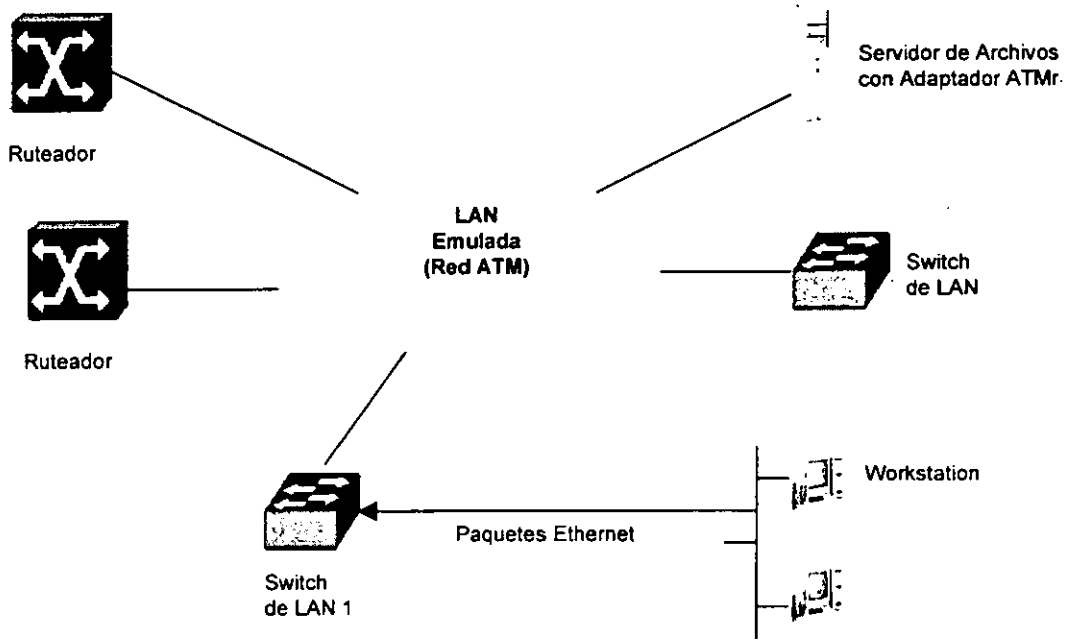


Figura 3.64 La Emulación conecta a las LANs transparentemente a través de las redes ATM.

En la figura 3.64 se muestran las condiciones en que un módulo LANE ATM en el switch 1 convierte los paquetes de ethernet transmitidos por un usuario en la estación de trabajo a celdas ATM. El Procesador de Interface ATM (AIP) en un ruteador proporciona el soporte para los componentes del servicio LANE: El **Servidor de Emulación LAN (LES)**, el **Servidor de Configuración (LECS)** y el **Servidor de No Reconocimiento y Broadcast (BUS)**.

Componentes LANE

LANE sigue un modelo cliente / servidor, en el cual varios clientes LANE (LECS) conectan a componentes de servicio LANE. Los LECS son típicamente implementados en dispositivos tales como adaptadores de estaciones de trabajo, ruteadores o switches LAN ATM.

Cuando se implementan varias LANs emuladas, los componentes de servicio pueden ser distribuidos a lo largo de diferentes ruteadores o switches a través de la red ATM.
LANE define tres diferentes tipos de componentes de servicio: El **Servidor de Emulación LAN (LES)**, el **Servidor de Configuración (LECS)** y el **Servidor de No Reconocimiento** y **Broadcast (BUS)**. Estos servidores proporcionan las siguientes funciones respectivamente:

El **Servidor de Emulación LAN (LES).** Resolver las direcciones MAC a direcciones ATM.
El **Servidor de No Reconocimiento** y **Broadcast (BUS).**
El **Servidor de Configuración (LECS)** y el **Servidor de No Reconocimiento.** Configurar LECS con la dirección del LES utilizada por la LAN emulada conectada.

CAPITULO CUARTO
MODELO DE RED

4.1 Antecedentes generales

La presente investigación se centra en el análisis de la infraestructura informática del **Servicio de Administración Tributaria SAT**; que hoy en día como Institución Pública necesita las ventajas que ofrecen los modernos sistemas de comunicación, en términos generales, el análisis se basa en la situación actual de las redes de área local de esta dependencia, cuya finalidad es brindar todo tipo de servicios referentes a consultas, almacenamiento, manipulación de la información, etc.; considerando la infraestructura con que cuenta dicha institución, (usuarios, software, hardware), a modo de ofrecer una optimización tecnológica en sus necesidades presentes y futuras.

Como parte del Servicio de Administración Tributaria SAT se encuentra la Administración General Jurídica de Ingresos AGJI que debido a sus actividades tiene la necesidad de cubrir servicios tales como correo electrónico (e-mail), aplicaciones cliente/ servidor y los antes mencionados e interactúa en forma constante con las otras Administraciones del SAT al compartir información y recursos; lo que nos obliga a examinar el funcionamiento del sistema administrativo de dicha dependencia para así conocer como un usuario accesará al sistema hasta él porque es necesaria la consulta de información la conclusión será proponer la optimización de los recursos con que cuenta actualmente el área de telecomunicaciones.

4.1.1 Antecedentes históricos del Servicio de Administración Tributaria

A partir del primero de julio de 1997 surge el Servicio de Administración Tributaria (SAT) como un órgano desconcentrado de la Secretaría de Hacienda y Crédito Público, con carácter de autoridad fiscal con atribuciones y facultades vinculadas con la determinación y recaudación de las contribuciones federales que hasta ahora ha ejercido la Subsecretaría de Ingresos, que tendrá por objeto recaudar los impuestos federales y otros conceptos destinados a cubrir los gastos previstos en el presupuesto de egresos de la Federación, para lo cual gozará de autonomía técnica para dictar sus resoluciones.

El SAT asume a partir del primero de julio las funciones que tenía encomendadas la Subsecretaría de Ingresos en lo relativo a la determinación, liquidación y recaudación de impuestos y demás contribuciones y sus accesorios, así como la vigilancia en el correcto cumplimiento de las obligaciones fiscales. En el desarrollo de esta función se destaca la necesidad de garantizar la aplicación correcta y oportuna de la legislación fiscal y aduanera de manera imparcial y transparente.

Recaudar con calidad y eficiencia las contribuciones federales necesarias para financiar el gasto público, garantizando la correcta y equitativa aplicación de la legislación fiscal y aduanera propiciando su cumplimiento voluntario y oportuno. Constituirse en una administración tributaria moderna, profesional, honesta y con una vocación de servicio, que acredite un alto grado de confianza en la sociedad.

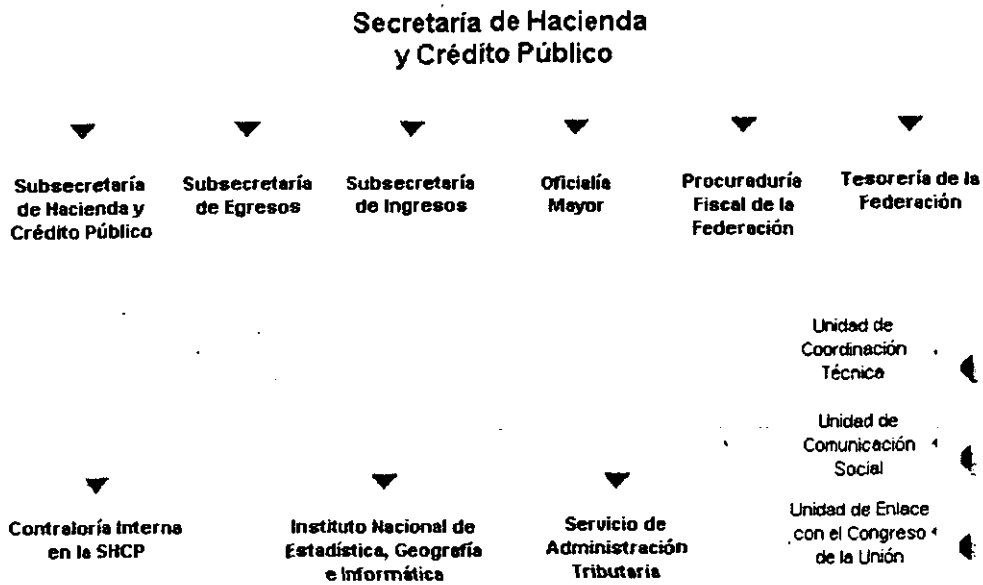


Figura 4.1 Estructura de Secretaría de Hacienda y Crédito Público

Funciones del SAT

El SAT está integrado por una Junta de Gobierno que constituye su órgano principal de dirección, por las Unidades Administrativas que lo conforman y por un Presidente que será nombrado y removido por el Presidente de la República. El Presidente del SAT será el enlace entre el SAT y las demás entidades gubernamentales a nivel federal, estatal y municipal y de los sectores social y privado, en las funciones encomendadas al propio Servicio de Administración Tributaria.

Por su parte, la Junta de Gobierno del SAT está configurada por el titular de la Secretaría de Hacienda que funge como presidente, así como dos representantes de la propia dependencia, el presidente del SAT y dos funcionarios del mismo organismo. Entre sus principales atribuciones está la de establecer medidas de política fiscal y aduanera necesarias para la formulación y ejecución del Plan Nacional de Desarrollo y de los programas sectoriales.

El patrimonio del SAT se conforma con los recursos financieros y materiales, así como con los ingresos que actualmente tiene asignados la Subsecretaría de Ingresos. Adicionalmente, el SAT recibirá recursos en proporción a sus esfuerzos de productividad y eficiencia.

La entrada en vigor del SAT no significa la creación de nuevas oficinas, por lo que se mantendrá el funcionamiento de las Administraciones Generales, Regionales y Locales de Auditoría Fiscal, de Recaudación, Jurídica de Ingresos y Aduanas.

Por lo que se refiere a las gestiones que actualmente realizan los contribuyentes ante las diversas instancias de lo que anteriormente era la Subsecretaría de Ingresos, éstas se continuarán tramitando ante las mismas oficinas como es el caso de la inscripción al Registro Federal de Contribuyentes, la solicitud de cédulas de identificación fiscal, así como la presentación de declaraciones y avisos que se llevarán a cabo en las formas fiscales aprobados con anterioridad, o en su caso, se efectuarán con los documentos o formatos que se expidan o aprueben con el funcionamiento del SAT.

4.2 Consideraciones para la estructura de una red

Requerimientos Informáticos

Para realizar sus funciones la AGJI, aprovecha los beneficios que el ambiente de red proporciona y así utilizar los medios informático de acuerdo a sus necesidades:

- Almacenar datos y crear bases de datos.
- Almacenamiento de software y herramientas manipuladoras de datos.
- Permitir acceso de usuarios a los dispositivos de entrada y salida.
- Comunicación, administración y control de software.
- Transferencia y correo electrónico
- Compartir recursos (memoria impresoras).
- Arquitectura abierta, etcétera.

4.2.1 Organización del SAT en el conjunto Hidalgo

El Servicio de Administración Tributaria SAT, se compone de diversas administraciones cuyas funciones dependen de las tareas que se les hayan encomendado. No obstante, de tener actividades específicas, la interacción entre ellas es frecuente, y por ende, la necesidad de compartir recursos.

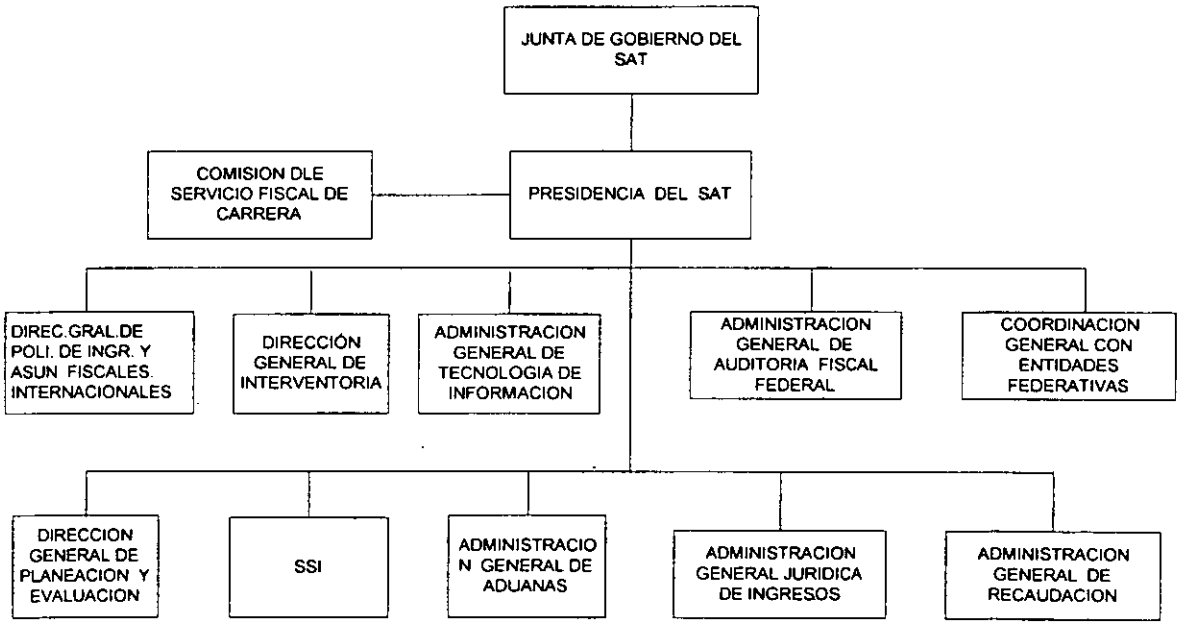


figura 4.2 Organización administrativa del SAT

Las funciones generales de estas administraciones son las siguientes:

- Proyectar y calcular los ingresos de la federación, del Departamento del Distrito Federal (D.D.F.) y las entidades paraestatales.
- Estudiar y formular los proyectos de leyes y disposiciones fiscales, de las leyes

de ingresos de la federación y del D.D.F.

- Dirigir la política monetaria y crediticia.
- Planear, coordinar, evaluar y vigilar el sistema bancario del país, que comprende el banco central, la banca nacional de desarrollo y las demás instituciones encargadas de prestar el servicio de banca y crédito.
- Formular la cuenta anual de la Hacienda Pública Federal.
- Cobrar impuestos, derechos y aprovechamientos federales en los términos legales.
- Definir los estímulos fiscales y estimar sus efectos en los ingresos de la federación.
- Establecer y revisar los precios y tarifas de los bienes y servicios de la administración pública federal.
- Dirigir los servicios aduanales y de inspección y la política fiscal de la federación.
- Proyectar y calcular los egresos del gobierno federal y de la administración pública federal.
- Formular el programa del gasto público federal y el proyecto de presupuesto de egresos de la federación y presentarlos junto con el del D.D.F. a la consideración del Presidente de la República.
- Evaluar y autorizar los programas de inversión pública de las dependencias y entidades de la administración pública federal.
- Dictaminar las modificaciones a la estructura orgánica básica de las dependencias y entidades de la administración pública federal.

Vigilar el cumplimiento de las obligaciones derivadas de las disposiciones en materia de planeación nacional, así como de programación, presupuestación, contabilidad y evaluación.

4.2.2 Administración, políticas, seguridad, recursos, usuarios y funciones

Se puede establecer una organización lógica de la red del Conjunto Hidalgo, que debe considerar aspectos de tipo administrativo, de política, de seguridad, de recursos, de número de usuarios, de funciones, etc. A continuación se explica de manera breve:

- Administrativo.- cada una de las administraciones dispone de centros de cómputo con una estructura muy particular, manejados por personal informático adscritos a ellas, que cuentan con procedimientos y estándares de trabajo bien definidos. Sin dejar de respetar sus mecanismos de trabajo, se les debe integrar al trabajo conjunto en red en el Conjunto Hidalgo.

- Política.- a pesar de que el trabajo entre administraciones suele ser frecuente, cada una de ellas se rige por políticas que pueden ser muy particulares. Políticas que involucran aspectos como horarios, métodos, y en general decisiones de cómo llevar a cabo las actividades. El acceso a la red debe cubrir sus expectativas en cuanto a los criterios ya mencionados.

- Seguridad.- cada una de las diferentes administraciones vigila el que la información que maneja, por ser la mayoría de carácter confidencial, esté a buen resguardo y sea consultada sólo por el personal autorizado. La forma en que se almacena y consulta la información por medios electrónicos, debe estar bajo constante supervisión y auditoría. Cualquier violación a la integridad y confidencialidad puede ser considerada delito federal.

- Recursos.- por el tipo de funciones que realizan, las administraciones cuentan con recursos diferentes, tanto materiales como humanos y de logística. Mientras que algunas para el desempeño de sus labores se apoyan más en el factor humano, otras han demandado más el recurso tecnológico. Para todas ellas sin embargo, la comunicación interna y externa es importante, por lo que el acceder a la red es un aspecto que cada vez adquiere mayor relevancia.

- Número de usuarios.- dentro del SAT existen tanto administraciones como direcciones, sin ser una regla, es común que las administraciones dispongan de un número bastante mayor de personal que las direcciones. Sin embargo, a todos los usuarios sin importar donde estén adscritos, debe facilitárseles el acceso a la red. El planear la manera en que debe organizarse para atenderlos a todos ellos es un aspecto muy importante para lograr un buen funcionamiento.

- Funciones.- las actividades realizadas por cada una de las administraciones responden a las funciones para las cuales fueron creadas. El esquema lógico de la red debe considerar el no entorpecerlas para no constituir un obstáculo en las tareas que por ley, están obligadas a desarrollar.

4.3 Esquema lógico de la red

Considerando los requerimientos de comunicación y las funciones administrativas para el establecimiento de la red lógica es necesario conocer la herramienta con que se administra una red, para así comenzar la arquitectura[1] de red; el de software de red, que se utiliza es WindowsNT4.0 de Microsoft; , al analizar esta herramienta podemos definir conceptos necesarios para adentrarnos en los protocolos de comunicación.

4.3.1 Software para red

Windows NT de Microsoft es un verdadero sistema operativo de 32 bits muy poderoso, que está disponible en versiones cliente y servidor. Entre las características clave de NT está la multitarea prioritaria, procesos de multilectura o hebras, portabilidad y soporte para multiprocesamiento simétrico. La multitarea prioritaria permite la realización de múltiples tareas preferentes y subordinadas. Es NT y no los programas específicos quien determina cuando deberá interrumpirse un programa y empezar a ejecutar otro. Procesos de lectura múltiple o hebras, es un término que en NT, se refiere a los hilos que funcionan como agentes de ejecución. Tener hebras de ejecución múltiple dentro de un mismo proceso, significa que un proceso ejecuta, de manera simultánea, diferentes partes de un programa en diferentes procesadores. El multiprocesamiento simétrico permite que los requerimientos de sistema y aplicación se distribuyan de manera uniforme entre todos los procesadores disponibles, haciendo que todo funcione mucho más rápido. Windows NT

[1] Arquitectura, ver capítulo II

emplea el sistema de archivos NT (NTFS). Este sistema de archivos soporta nombres de archivo de hasta 256 caracteres. También permite el rastreo de transacciones. Esto significa que si el sistema falla, NT regresa los datos al estado inmediato anterior a la caída del sistema. Microsoft diseñó Windows NT para que fuera portátil. Está compuesto de un kernel o núcleo, así como de diferentes subsistemas del sistema. Hay subsistemas disponibles para aplicaciones que ejecutan programas basados en OS/2 y POSIX. Un procesador DOS virtual (VDM) ejecuta MS-DOS y aplicaciones Windows de 16 bits. NT incluye software de red de punto a punto para que los usuarios de NT puedan compartir archivos y aplicaciones con otros usuarios que ejecuten NT o Windows para Trabajo en Grupo.

Ejecución de NT con otros sistemas operativos de red

Windows NT Server ofrece compartición de archivos integrada, capacidad de compartición de impresoras para la computación en grupos de trabajo y una interfaz de sistema de red abierto, que incluye soporte integrado para IPX/IPX, TCP/IP, NetBEUI y otros transportes. NT Server es compatible con redes existentes como VINES, NetWare, UNIX, LAN Manager2.x y Windows para Trabajo en Grupo. Windows NT incluye interfaces de programación de aplicación (API) que permiten que los fabricantes de sistemas operativos de red (NOS) escriban software de cliente para que sus productos puedan ejecutarse con éste. NT da soporte a clientes Macintosh y los trata de la misma manera como usuarios de la red, dando soporte al protocolo de archivo AppleTalk. Los usuarios de Macintosh pueden accesar el servidor NT Server como si se tratara de un servidor AppleShare.

Windows NT Server 4.0

La integración de la interfaz de usuario de Windows 95 en NT 4.0, proporciona una visión consistente a través del escritorio y el servidor, resultando en un menor tiempo de entrenamiento y un más rápido desenvolvimiento del nuevo sistema operativo de red. Herramientas como el administrador de tareas y el monitor de red simplifican la administración del servidor. El administrador de tareas ofrece información extensa de las aplicaciones e indicaciones gráficas del CPU y de la memoria, que permiten a los administradores un control del comportamiento del sistema. El monitor de red tiene la habilidad de vigilar el tráfico de la red, permitiendo prevenir problemas en el desempeño de la misma. El directorio de servicios de Windows NT (NTDS) soporta a 25,000 usuarios por dominio y cientos o miles por empresa. Sin importar lo centralizado o descentralizado de un negocio, NTDS permite instalar un directorio en la organización capaz de proveer un manejo completo de recursos, servicios y aplicaciones. NTDS es un directorio de servicios que presenta seguridad, arquitectura confiable, interfaz gráfica para la administración e interoperabilidad abierta con Novell NetWare.

NT 4.0 incluye un programa de diagnósticos que proporciona información acerca de los drivers y del uso de la red, minimizando los posibles errores del sistema. Esta información se presenta en forma gráfica que puede ser utilizada desde un sistema NT remoto. El desempeño y la escalabilidad del servidor se han mejorado, así como la compartición e impresión de archivos y el desempeño del servidor de Internet. Windows NT 4.0 trabaja con sistemas como NetWare, UNIX e IBM. Tiene soporte para más de 5,000 plataformas de hardware, siendo compatible para los protocolos de red más utilizados como TCP/IP, IPX/SPX, NetBEUI, AppleTalk, control de enlace de datos (Data Link Control, DLC), HTTP, arquitectura de redes de sistemas (Systems Network Architecture, SNA), PPP Y protocolo de punto a punto por medio de túnel (Point to Point Tunneling Protocol, PPTP). NT 4.0 es compatible para una gran variedad de sistemas clientes como Windows 3.x, Windows 95, Windows NT Workstation, IBM OS/2 y Macintosh.

Dominios

Un dominio es un conjunto de ordenadores (servidores + estaciones de trabajo) que comparten características comunes en cuanto a accesos. Un usuario registrado en un dominio con un nombre de usuario y una palabra de paso, automáticamente es capaz de acceder a todos los servidores de dicho dominio utilizando el mismo nombre y la misma palabra de paso.

Dentro de los servidores de un dominio existen dos jerarquías: el servidor PDC (Primary Domain Controller) y los servidores BDC (Backup Domain Controller). Por cada dominio ha de haber un PDC y sólo uno, y posiblemente varios BDC. Cuando el administrador del dominio da de alta un nuevo usuario, lo hace sobre el PDC. Los datos sobre los usuarios se guardan en una base de datos llamada SAM, que la tiene cualquier servidor. El PDC se encarga de copiar esa base de datos de usuarios a todos los BDCs de su dominio de manera periódica. Notemos la liberación de trabajo que esto supone para un administrador de red. Con sólo dar de alta un usuario en el PDC, ese usuario automáticamente puede acceder a cualquier servidor del dominio y, además, usando el mismo nombre de usuario y la misma palabra de paso. Este proceso de copia periódica de la SAM se denomina replicación.

Relaciones de confianza

Windows NT Server viene preparado con los protocolos adecuados para soportar diversos tipos de clientes: MS-DOS, Windows para Trabajo en Grupo, OS/2, Windows95. Ahora que tenemos la idea intuitiva de lo que es un dominio, pasemos a ver cómo se relacionan los dominios de una red mediante el concepto de Trust o Relación de Confianza. Se dice que un dominio A confía en otro B, o que hay establecida una relación de confianza desde A hacia B, cuando cualquier usuario autorizado en el dominio B puede entrar sin más en el dominio A. Un grupo local es un grupo de usuarios, de manera que cualquier usuario del grupo puede entrar y acceder a los recursos del servidor PDC del dominio al que pertenece el grupo. Un grupo local se define como perteneciente a un dominio.n grupo global es igual que el anterior excepto en que puede ser visto también por todos los dominios que confían en el dominio al que pertenece el grupo. La diferencia entre local y global es, pues, el ámbito de visibilidad. Si A confía en B, y definimos en B un grupo global, entonces ese grupo también se puede utilizar en A.

El Dominio Master

Una organización distinta sería la del dominio master. Supongamos que tenemos un dominio donde almacenamos todas las cuentas de los usuarios de la red (dominio master). En él definimos varios grupos globales, por ejemplo uno por departamento. Creamos ahora tantos dominios como departamentos hay, y hacemos que todos esos dominios confíen en el master. Ahora, en el dominio del departamento X, creamos un grupo local donde meteremos todos los globales del master cuyos usuarios nos interese que accedan a los recursos de las máquinas de X. Por tanto, en el dominio X bastará dar permisos de acceso al grupo local definido y, automáticamente heredarán esos permisos los usuarios de los globales metidos en ese local. Un mismo grupo global puede estar metido en varios locales de varios dominios. Repetiremos esta operación para cada departamento. Esto da lugar a una administración centralizada.

Otro modelo es el de múltiples masters. Un dominio en general puede albergar hasta 15000 cuentas de usuario. Cuando necesitamos más, podemos definir varios masters. Entre los masters definiremos relaciones de confianza en ambos sentidos (por ejemplo, si tenemos dos masters M1 y M2, haremos que M1 confíe en M2 y M2 confíe en M1). Si ahora hacemos que todos los restantes dominios confíen en M1 y en M2, habremos conseguido lo mismo que en el modelo de master único pero ampliando el número de cuentas de usuario hasta 30000.

Grupos De Trabajo

Para terminar me gustaría señalar la diferencia de los dominios con los grupos de trabajo de Windows para trabajo en grupo. Un grupo de trabajo es un conjunto de ordenadores en el que cada uno puede funcionar tanto como cliente como servidor, o ambos a la vez. El administrador tiene la responsabilidad de mantener la base de datos de usuarios en cada ordenador del grupo. Además, un usuario de un ordenador podría fácilmente dañarlo y echar abajo los servicios.

Cuentas de usuarios y grupos

Es muy importante planificar cuidadosamente la administración de las cuentas de usuario y grupos, no obstante disponemos de sencillas y potentes herramientas para llevarlo a la práctica.

El mantenimiento de los permisos y derechos de un grupo es más sencillo que el de varias cuentas de usuario, generalmente usaremos los grupos para administrar el acceso a los recursos (puestos, archivos, impresoras, etc.).

Es obvio que sobre el directorio personal de un usuario aplicaremos permisos específicos para dicho usuario, pero si necesitamos que varios usuarios de distintos o de un mismo grupo accedan al mismo recurso es recomendable crear un nuevo grupo para tal fin, ya que un usuario puede pertenecer a varios grupos.

Muchas veces creamos grupos utilizando el mismo esquema de nuestra empresa u organización, sin embargo, debemos pensar en los grupos de usuarios en función de los recursos que van a necesitar. Cambiaremos los permisos proporcionados a un conjunto de usuarios utilizando la cuenta de grupo pero no modificaremos cada cuenta. Intentaremos aprovechar los grupos predefinidos de Windows NT, a los que se han asignado útiles conjuntos de derechos y capacidades. En un dominio de Windows NT Server se pueden mantener dos tipos de grupos: grupos locales y grupos globales, para comprender la utilidad de cada uno hemos hecho un pequeño extracto de los manuales de ayuda.

Grupos globales

Un grupo global contiene una serie de cuentas de usuario de un dominio; que están agrupadas bajo un nombre de cuenta de grupo. Un grupo global sólo puede contener cuentas de usuario del dominio donde se creó el grupo global. Una vez que se crea un grupo global, se le puede asignar permisos y derechos en su propio dominio sobre estaciones de trabajo o servidores miembro, o sobre dominios que 9confían. Sin embargo, lo mejor es asignar derechos y permisos a grupos locales, y usar el grupo global como método para agregar usuarios a grupos locales. Los grupos globales se pueden agregar a grupos locales del mismo dominio, en dominios que confían en dicho dominio, o en servidores miembro o equipos que ejecuten Windows NT Workstation en el mismo dominio o en uno que confía. Los grupos globales sólo contienen cuentas de usuario de dominio. No puede crear un grupo global en un equipo que ejecute Windows NT Workstation o en un equipo que ejecute Windows NT Server como servidor miembro.

La palabra "globales" en "grupos globales" indica que el grupo está disponible para recibir derechos y permisos en múltiples dominios (globales). Un grupo global sólo puede contener cuentas de usuario; no puede contener grupos locales ni otros grupos globales.

Grupos locales.

Un grupo local contiene cuentas de usuario y cuentas de grupo globales de uno o más dominios, agrupados bajo un nombre de cuenta de grupo. Los usuarios y los grupos globales de fuera del

dominio local sólo se pueden agregar al grupo local si pertenecen a un dominio que confía. Los grupos locales hacen posible la rápida asignación de derechos y permisos sobre los recursos de un dominio (es decir, el dominio local) a usuarios y grupos de dicho dominio y otros dominios que confíen en él. Los grupos locales también existen en servidores miembro y equipos que ejecutan Windows NT Workstation, y pueden contener cuentas de usuario y grupos globales. La palabra "locales" de "grupos locales" indica que el grupo está disponible para recibir derechos y permisos en un dominio único (local). Un grupo local no puede contener otros grupos locales. Estrategias para utilizar grupos locales y globales. Un grupo local es una entidad de seguridad única a la que se puede conceder acceso a muchos objetos de una única ubicación (un dominio, una estación de trabajo o un servidor miembro) en vez de tener que editar los permisos sobre todos esos objetos de forma independiente.

Con los grupos globales se pueden agrupar las cuentas de usuario a las que se podrían conceder permisos para usar objetos en múltiples dominios y estaciones de trabajo. Por ejemplo, en una configuración de múltiples dominios, puede pensar en los grupos globales como medio para agregar usuarios a los grupos locales de dominios que confían. Para extender los derechos y permisos de los usuarios a recursos de otros dominios, agregue sus cuentas a un grupo global de su dominio y después agregue el grupo global a un grupo local de un dominio que confía. Incluso en un dominio único, si recuerda que puede agregar dominios adicionales en el futuro, puede usar grupos globales agregados a grupos locales para conceder todos los derechos y permisos.

Posteriormente, si se crea otro dominio, los derechos y permisos asignados a sus grupos locales pueden extenderse a los usuarios del dominio nuevo creando una relación de confianza y agregando 9grupos globales del dominio nuevo a sus grupos locales. De la misma manera, si el dominio nuevo confía en su dominio, sus grupos globales se pueden agregar a los grupos locales del dominio nuevo. Los grupos globales de dominio también se pueden usar para propósitos administrativos en equipos con Windows NT Workstation o en servidores miembro con Windows NT Server. Por ejemplo, el grupo local Administradores de dominio se agrega de forma predeterminada al grupo local incorporado Administradores en todas las estaciones de trabajo o servidores miembro que se unen a un dominio existente. La pertenencia al grupo local Administradores de una estación de trabajo o servidor miembro permite que el administrador de red administre el equipo de forma remota creando grupos de programas, instalando software y solucionando los problemas del equipo.

4.3.2 Arquitectura de dominios del SAT

Para la arquitectura lógica de la red se ha planeado el trabajar bajo un esquema de 3 niveles de dominios NT:

- ✓ Dominio administrativo (primer nivel)
- ✓ Dominio de control de recursos y cuentas (segundo nivel)
- ✓ Dominios de aplicaciones (tercer nivel)

Dominio Administrativo.- este dominio cumple básicamente con la función de controlar los dominios de segundo nivel. Está manejado por la Administración General de Tecnología de la Información y no es accesible al resto de los usuarios de la red. Para cumplir su labor de administración, mantiene relaciones bidireccionales de confianza con el dominio de segundo nivel.

Dominio de Control de Recursos y Cuentas.- este dominio tiene la función de controlar tanto los recursos de que se dispone en la red (correo electrónico, software de aplicaciones de propósito específico para la AGJI, etc.), como las cuentas de usuario para el personal del SAT con acceso a la red. Está manejado por la Administración General de Tecnología de la Información y no es

accesible al resto de los usuarios de la red. Para cumplir su labor, mantiene relaciones de confianza bidireccionales con el dominio de primer nivel.

Dominios de Aplicaciones.- estos dominios corresponden a las diferentes administraciones y direcciones que conforman el SAT. Están manejados por cada una de ellas y no son accesibles a los usuarios de las otras administraciones. En principio, no mantienen relaciones de confianza más que con el dominio de segundo nivel en el cual confían. Debido a que son las propias áreas las que administran sus propios dominios, el establecer otro tipo de relaciones queda bajo su criterio y riesgo. La intención de la existencia de estos dominios es que cada administración trabaje con libertad los sistemas y aplicaciones con los que llevan a cabo sus labores, sin dejar de operar en un ambiente común de red.

El esquema de dominios de conjunto Hidalgo, presta atención a las consideraciones antes mencionadas, estableciendo la siguiente arquitectura de dominios que lo identifican dentro de la red de acuerdo al origen que tiene.

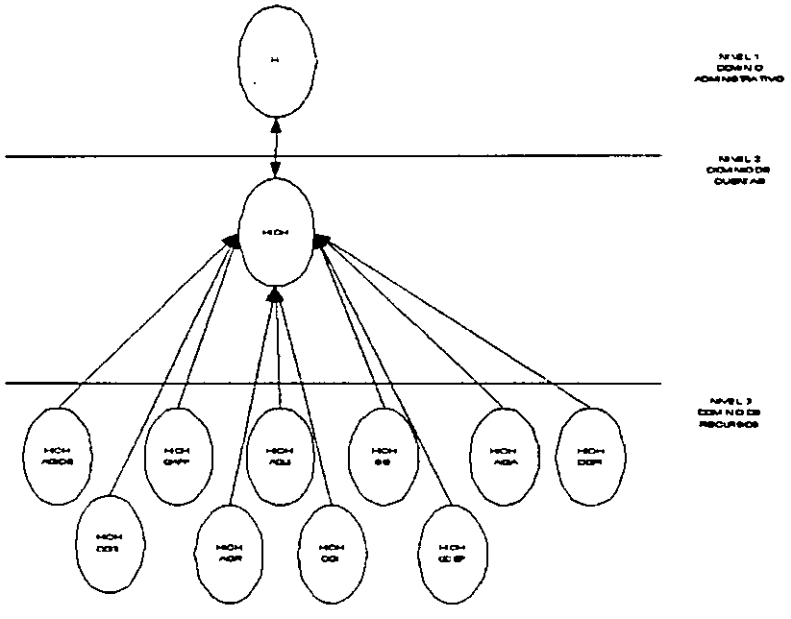


Figura 4.3 Arquitectura de dominios de Windows NT

- ✓ El dominio administrativo nivel 1 esta identificado por HI que representa Hacienda Ingresos.
- ✓ El dominio de cuentas nivel 2 esta identificado por HICH que representa a Hacienda Ingresos Conjunto Hidalgo.
- ✓ El dominio de recursos nivel 3 cuenta con 10 nombres de dominio en los que cada uno representa a las administraciones que forman el conjunto hidalgo siendo los siguientes.

NOMBRE DE LA ADMINISTRACIÓN	SIGLAS DE ID	NOMBRE DEL DOMINO
DIRECCION GENERAL DE POLITICAS DE INGRESOS Y ASUNTOS FISCALES INTERNACIONALES.	DGPI	HICHDGPI
DIRECCION GENERAL DE INTERVENTORIA	DGI	HICHDGI
ADMINISTRACION GENERAL DE AUDITORIA FISCAL FEDERAL	AGAFF	HICHGAFF
COORDINACION GENERAL CON ENTIDADES FEDERATIVAS	DGCEF	HICHDGCEF
ADMINISTRACION GENERAL DE ADUANAS	AGA	HICHAGA
ADMINISTRACION GENERAL JURIDICA DE INGRESOS	AGJI	HICHAGJI
ADMINISTRACION GENERAL DE RECAUDACION	AGR	HICHAGR
ADMINISTRACION GENERAL DE TECNOLOGIA DE LA INFORMACION	AGTI	HICHDGTI
ADMINISTRACION GENERAL DE EVALUACION	AGIDE	HICHAGIDE
SUBSECRETARIA DE INGRESOS	SSI	HICHSSI

Por ejemplo, en la Administración General Jurídica de Ingresos AGJI sus usuarios y recursos están representados por el nombre de domino HICHAGJI que dentro de la red global de la SHCP puede definirse como:

- ✓ **HI** SHCP es decir parte de **H**acienda que pertenece a la subsecretaría de **I**ngresos
- ✓ **CH** Identificación del SAT en su ubicación física dentro de las instalaciones de **C**onjunto **H**idalgo
- ✓ **AGJI** que representa a la **A**dministración **G**eneral **J**urídica de **I**ngresos

Siendo el mismo esquema para las otras administraciones.

4.3.3 Relaciones de Confianza del SAT

De acuerdo a la figura 4.3 Arquitectura de Dominios de Windows NT, observamos que se presentan las relaciones de confianza de acuerdo al nivel de seguridad requerido por cada nivel, cabe mencionar que la Administración de tecnología de la Información es la que se encarga de administrar en materia de informática a las demás administraciones.

4.3.4 Usuarios

Las instalaciones de Conjunto Hidalgo cuenta con 8 edificios (módulos de ahora en adelante) dentro de los que se ubican aproximadamente 4510 usuarios del Servicio de Administración Tributaria SAT que de acuerdo a la capacidad del inmueble, se agruparon de la siguiente forma:

MODULOS	USUARIOS
1	167
2	527
3	700
4	1139
5	552
6	681
7	556
8	187

4.4 Esquema físico de la red del SAT

4.4.1 Características de Hardware

La infraestructura principal de la red del SAT se encuentra en la ciudad de México distribuida en 8 módulos, además, tiene oficinas regionales en el interior de la República (Puebla, Monterrey, Guadalajara, Querétaro y Yucatán). Los módulos 2 y 4 concentran los equipos principales que realizan la interconexión a los otros módulos.

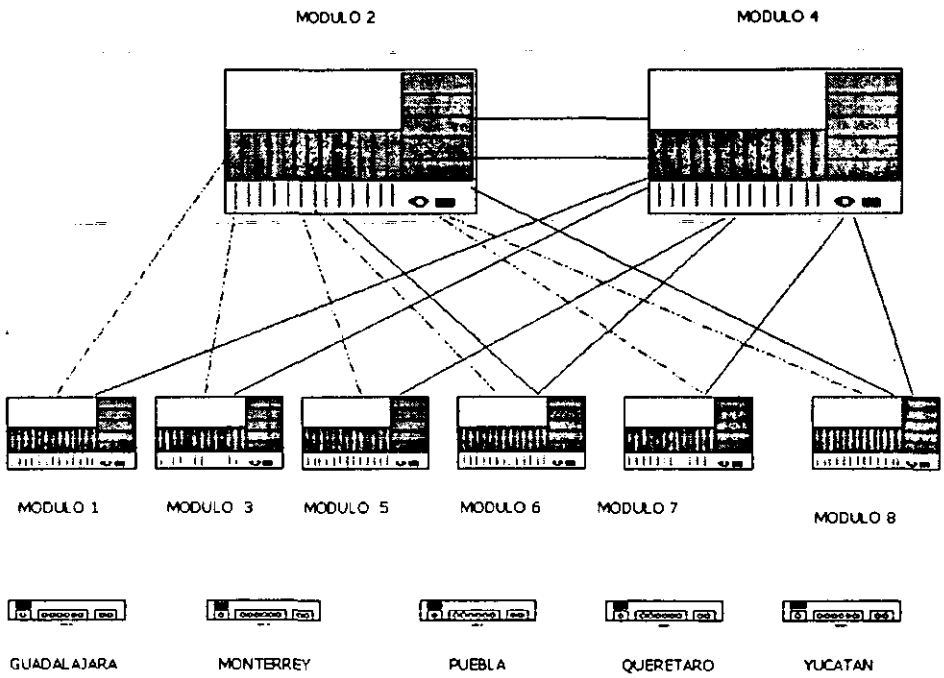


Figura 4.4 Esquema de conexión entre módulos

Los detalles de los equipos de los módulos se muestran en el Apéndice E (Inventario Red SAT).

4.4.2 Ambiente operativo en el SAT

Es en esta sección en donde se ejemplificará tomando el caso de Jurídica. Es importante describir como es el proceso de operación de un usuario, por ejemplo una secretaria. Lo relevante es que muestres como se loguean con su cuenta que está en un dominio de segundo nivel, y como interactúan con sus aplicaciones que están en el tercer nivel (correo electrónico y Control de Gestión). El por que para el usuario es transparente el concepto de esquema de dominios, es decir, el usuario ni sabe que existe ni tiene por que saberlo.

Un usuario mediante sus aplicaciones busca el comunicarse con otros usuarios, el transporte de su información a través de la red es transparente para él y en cuestión de segundos busca el recibir respuesta.

Las siguientes laminas presentan la forma en que la información viaja hasta su destino.

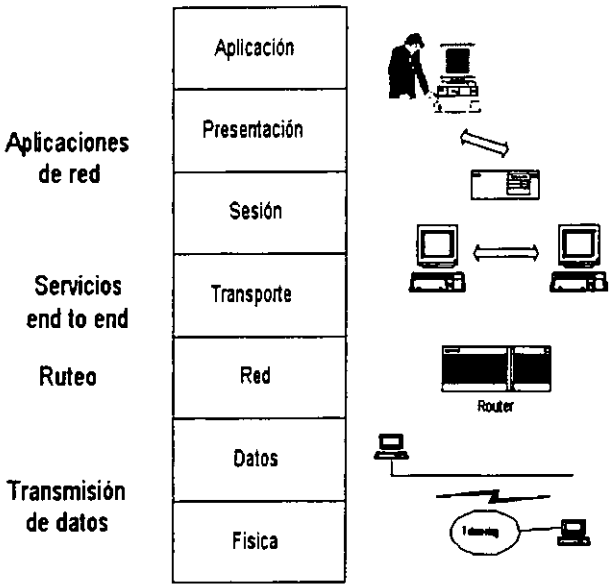


Figura 4.5 Funcionalidad de cada una de las capas del Modelo de Red

Aplicaciones, Presentación y Sesión

Aplicación

Un usuario al solicitar los servicios de comunicación utiliza también las aplicaciones de red para poder soportar sus aplicaciones de escritorio:

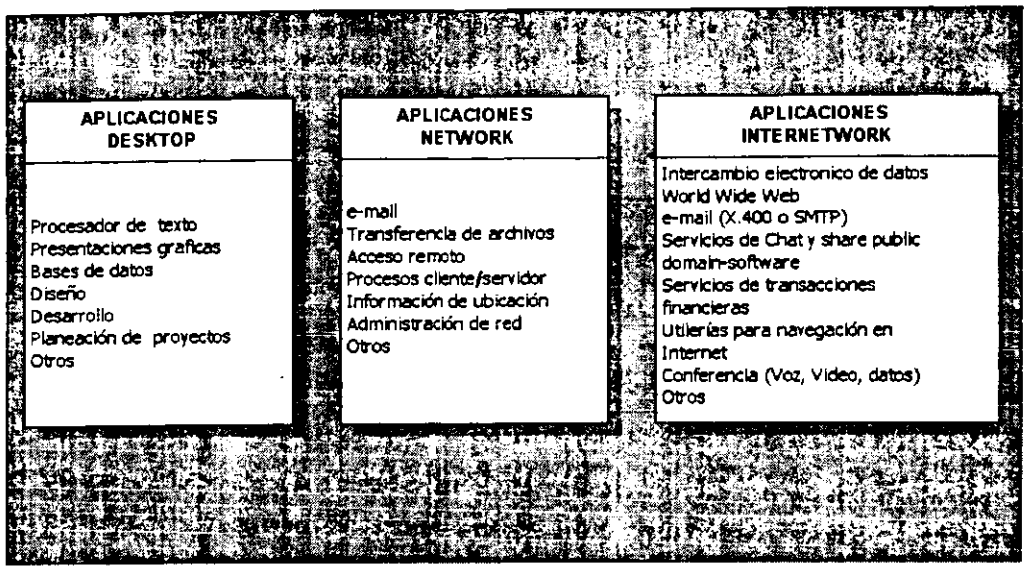


Figura 4.6 Aplicaciones usuario/red/Internet

Presentación

Se encarga de proporcionar formato y conversión de código para las aplicaciones, es decir, es responsable de la conversión de sintaxis entre sistemas que tienen diferentes representaciones de caracteres de texto y datos, tales como EBCDIC Y ASCII incluye también la encriptación de datos; que es un proceso de conversión el cual permite que los datos puedan ser transmitidos protegidos para en caso de recepciones no autorizada que estos no puedan ser descifrados. Otras rutinas comprimen el texto o convierten imágenes gráficas en tramas de bits (bit stream) para transmitirlos a través de la red.

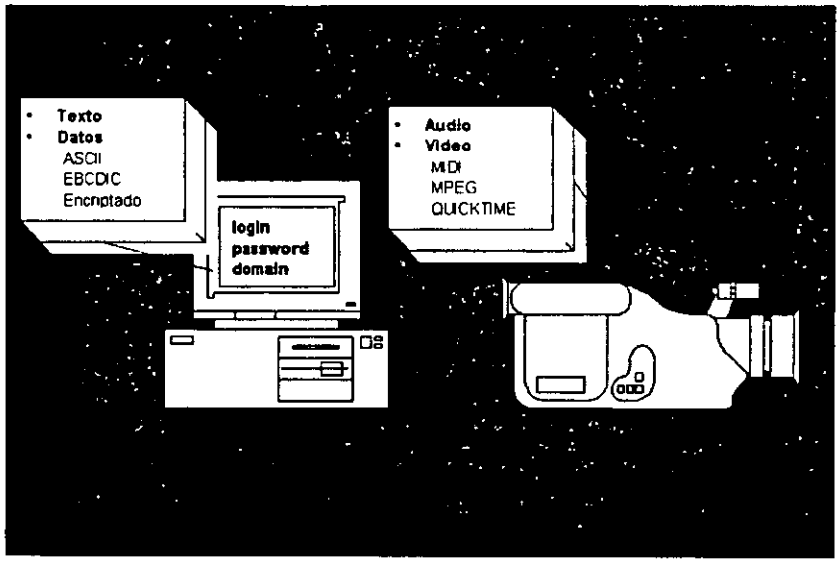


Figura 4.7 Presentación (Conversión para las aplicaciones)

Sesión

Establece, administra y termina sesiones entre aplicaciones. Esencialmente coordina los servicios de solicitud y respuesta que ocurren cuando las aplicaciones se comunican entre diferentes hosts.

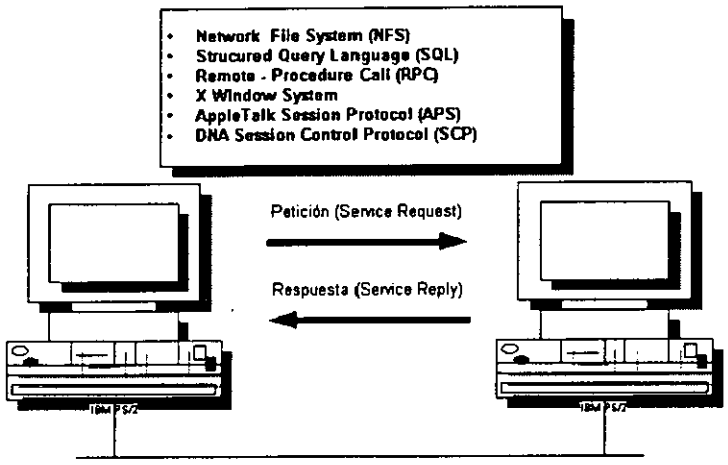


Figura 4.8 Sesión (Coordina como interactúan las aplicaciones sobre diferentes hosts)

Transporte

Los servicios de transporte permiten a los usuarios el segmentar y reensamblar múltiples aplicaciones de la capa superior dentro de la misma trama de datos de la capa de transporte.
Así mismo, la trama de datos suministra servicios de transporte end to end. Lo cual permite establecer un a conexión lógica entre los puntos finales de la Internetwork: El host origen o remitente y el host destinatario o receptor.

En esta etapa también se puede asegurar la integridad de los datos, pues el control de flujo evita el problema de que en un lado de la comunicación el hosts sobrecargué la conexión del buffer en el host del otro lado. El sobre flujo puede ocasionar la perdida de datos.

Los servicios de transporte también permiten a los usuarios hacer peticiones seguras en el transporte de datos entre sistemas y comunicaciones. El transporte seguro utiliza una relación de conexión orientada entre comunicaciones y sistemas para realizar lo siguiente:

- ✓ Asegurar que los segmentos entregados serán reconocidos de vuelta al remitente.
- ✓ Proporcionar la retransmisión de cualquier segmento que no sea conocido.
- ✓ Colocar los segmentos de regreso dentro de su correcta secuencia de destino.
- ✓ Evitar la congestión.

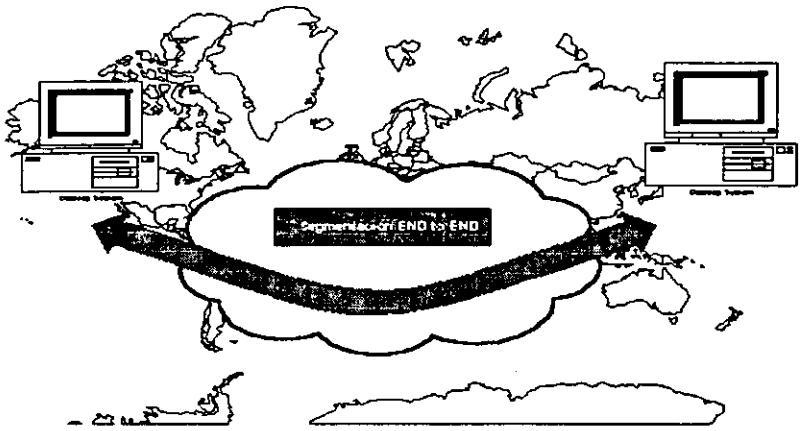
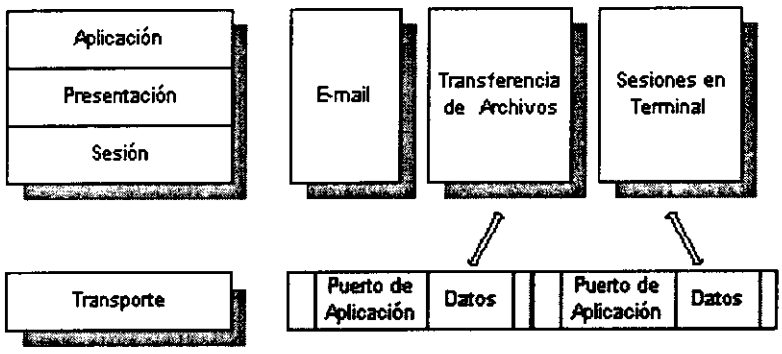


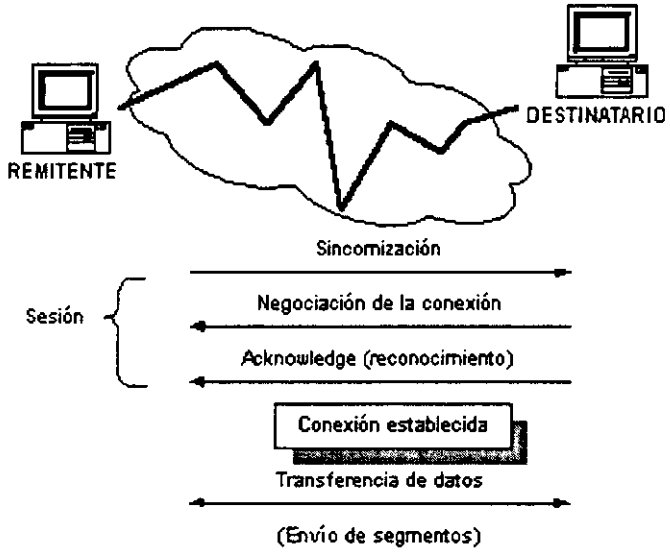
Figura 4.9 Transporte (Segmentación y reensamble de datos provenientes de las capas superiores)

El siguiente esquema plantea los diferentes procesos del transporte de datos.

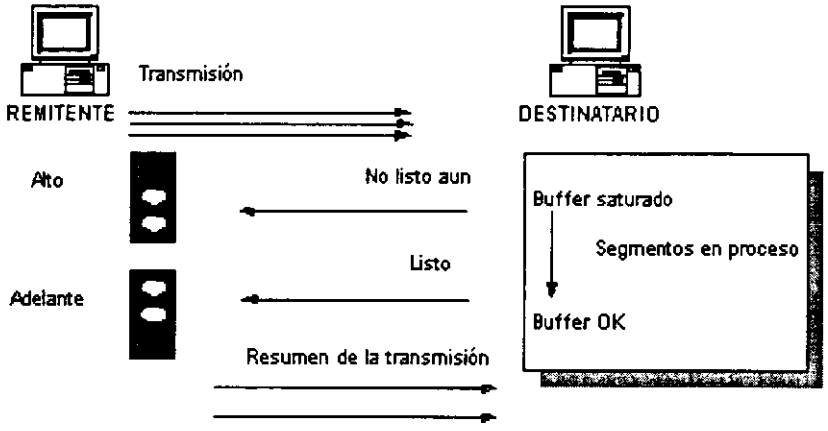
Segmentación de las aplicaciones superiores

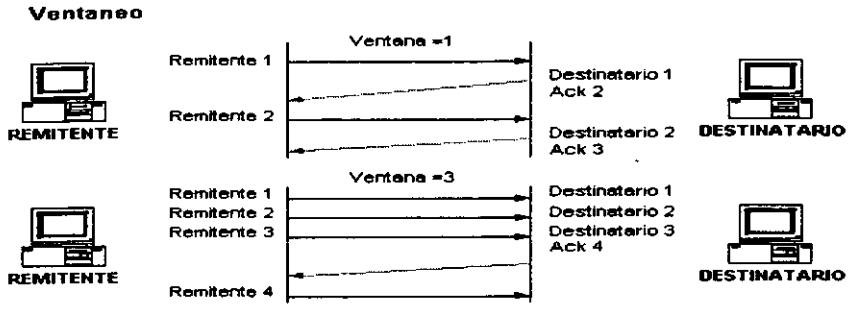


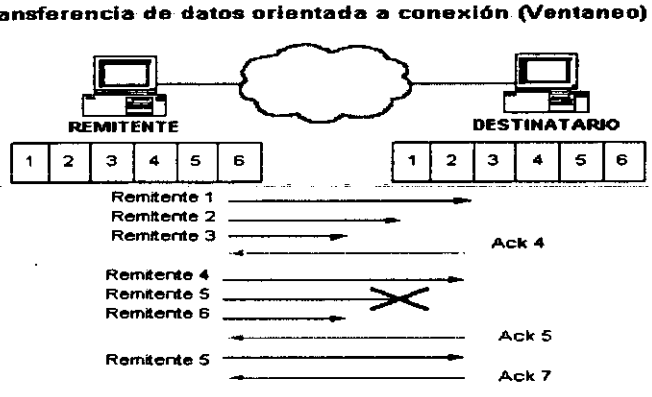
Estableciendo Conexión



Envío de segmentos con control de flujo







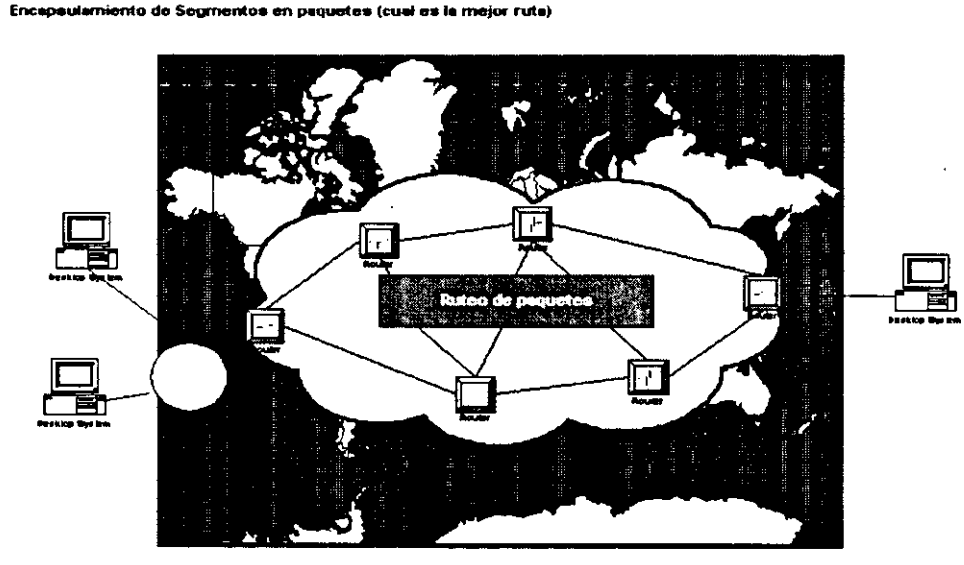
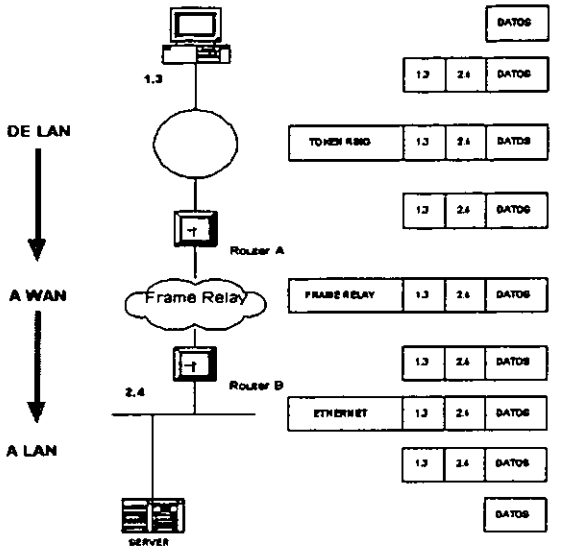


Figura 4.10 Proceso de Transporte de Datos

Red

En la figura anterior surge la pregunta ¿cuál camino elegir? Es aquí donde la determinación de la mejor ruta habilita al ruteador para evaluar y establecer el mejor manejo de los paquetes de datos hacia su destino.
El direccionamiento puede variar de acuerdo al protocolo utilizado, formado por el campo de red y él numero de host.



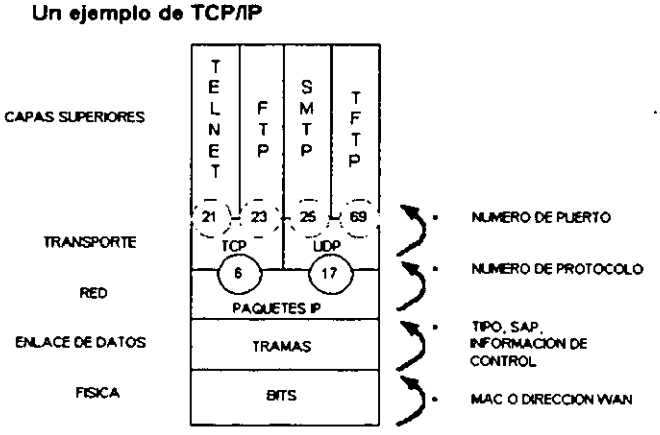


Figura 4.11 Ejemplo de TCP/IP

Datos y Capa física

Proporciona el transporte de datos a través de la capa física, manejando direcciones físicas, topologías de red, notificación de errores, entrega ordenada de tramas y opcionalmente control de flujo.

La capa física especifica requerimientos mecánicos, eléctricos y funcionales para activar, mantener y desactivar la capa física entre los sistemas terminales. Los protocolos LAN se encargan se ubican en la base estas dos capas y mediante el LLC (Logical Link control) y la MAC (Media Access Control) siendo la primera la que suministra el ambiente que necesita el servicio de conexión orientada en el enlace de datos(Funciones de Software hacia capas superiores); y la segunda que proporciona el acceso a los medios de la LAN de una forma ordenada (funciones de hardware hacia capas inferiores).

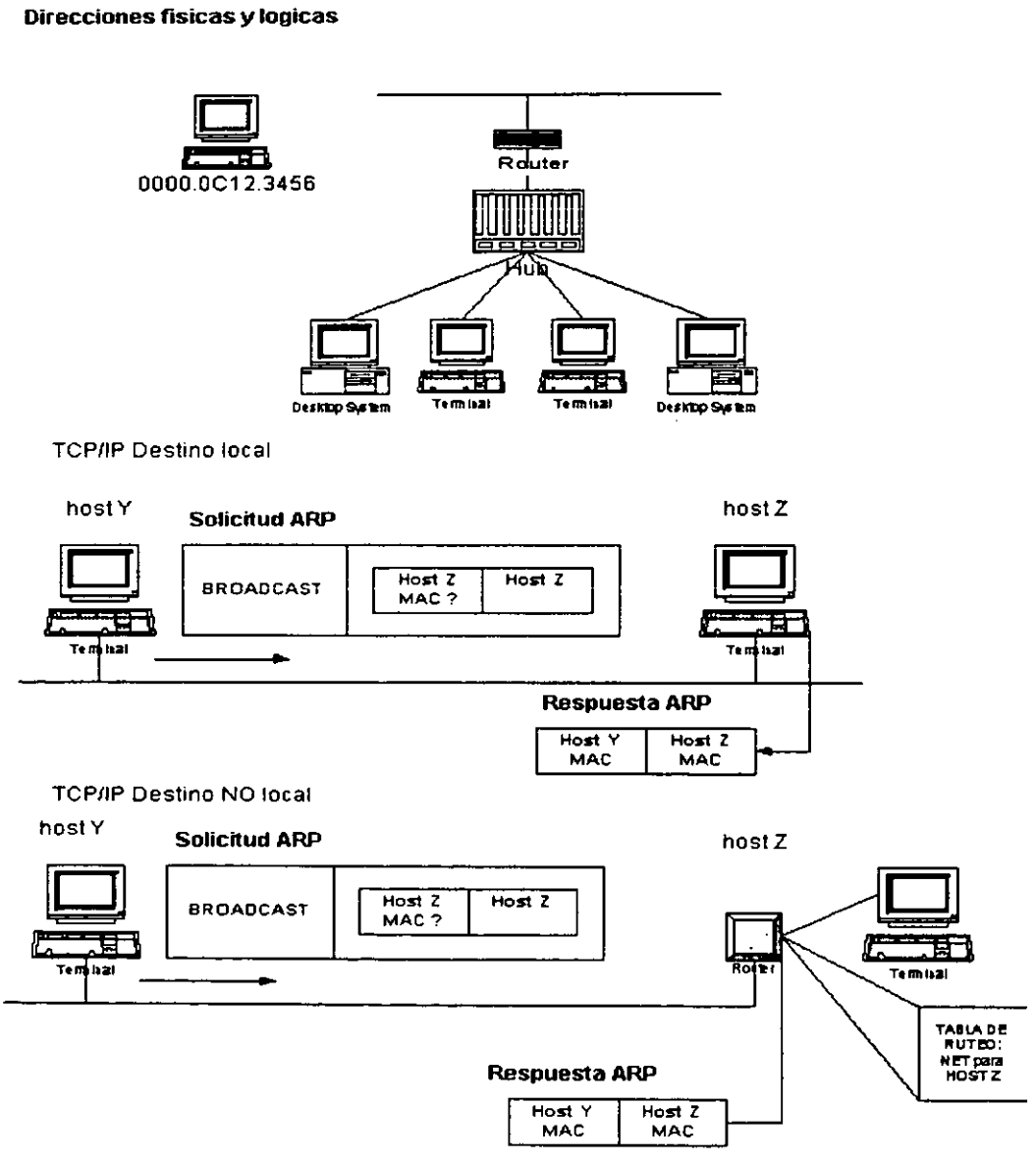


Figura 4.12 Direcciones Físicas y Lógicas

CAPITULO QUINTO
ANALISIS DE LA RED DEL SAT

Una vez presentadas las nuevas tecnologías de Frame Relay, protocolos LAN y protocolos de transporte, los cuales en conjunto proporcionan una red rápida de comunicaciones para la transmisión de datos, y por otro lado, analizando el estado actual de la red de comunicaciones del SAT, el siguiente punto, será correlacionar ambos aspectos, es decir, determinar la factibilidad de hacer del SAT una red de conmutación rápida, con capacidad de manejar aplicaciones como la de interconectividad de redes locales con voz y datos.

5.1 Integración de Servicios de Voz y Datos

La telefonía es una de las tecnologías más expandidas, particularmente en los negocios: Cada día los negocios hacen literalmente miles de llamadas y pensando en una llamada en particular, el costo es bajo, pero el costo acumulado en el negocio es bastante significativo.

Para la mayoría de los negocios, una parte de ese gasto puede evitarse. La telefonía pública tradicional es una parte compleja de tarifas y subsidios, normalmente resultando en situaciones donde la llamada de A a B cuesta una fracción de la parte desde B a A. Las compañías tienen grandes cuentas en redes de líneas privadas para pasar los cargos de telefonía pública, pero las tarifas de las líneas dedicadas también son altas. Varios han estado buscando otras estrategias y alternativas.

Conforme se van desarrollando las tecnologías, se están generando nuevas necesidades de comunicación y por lo tanto se vuelven posibles nuevas soluciones, los costos se reducen y la calidad aumenta como resultado en las nuevas tecnologías como Voz sobre Frame Relay (refiérase al capítulo 3) que permite nuevas soluciones de negocio tal como el transporte de la voz sobre una red pública de frame relay y reducciones dramáticas de los costos de llamadas de larga distancia.

Las redes de datos y las redes telefónicas han sido diseñadas con objetivos diferentes. Una red de datos se diseña para alta utilización y es tolerable a retardos pequeños, pero es intolerable a errores.

En la transmisión de voz el retardo es intolerable. Las palabras dichas llevan solamente una parte del significado. Aunque el mensaje se lleva también en la entonación, es decir, una breve pausa tiene mucho significado en una frase y se deberá preservar dicha pausa. Las redes de voz se deben diseñar para repetir la conversación confiablemente y en sincronización lo más apegado a lo original.

Las tecnologías de interconectividad que están basadas en voz paquetizada dan ciertas alternativas que pueden aplicarse para resolver estos problemas. Lo más importante es que la voz paquetizada no se distingue de los paquetes de datos, así que pueden ser transportados sobre redes normalmente reservadas para datos, donde los costos son normalmente más bajos.

Se intenta en esta sección reducir los costos de interconectividad y hacer más eficientes los servicios en una red de datos, asimismo, incluir servicios que den un valor agregado. Por lo anterior se hace referencia a capítulos anteriores donde se analizan las características de las tecnologías consideradas para la integración de los servicios mencionados.

Cada red debe llevar a cabo las actividades de direccionamiento, enrutamiento y señalización para establecer sus conexiones de una manera óptima. El direccionamiento, como ya se mencionó en el

capítulo 2 y 3, se requiere para identificar la llamada en sus puntos origen y destino, también se utiliza para asociar clases de servicios en la parte correcta. El enrutamiento busca el "mejor" camino del origen al destino y lleva la información a través de la red de la manera más eficiente posible de acuerdo al diseño de la red. La señalización alerta a las estaciones terminales y elementos de red del estado de ésta y de sus responsabilidades inmediatas para establecer una conexión.

En el diseño de una red integrada de voz y datos, debemos tener en cuenta las similitudes que tienen las redes de voz con las redes de datos, sobre todo cuando en las redes de voz como en las de datos están tratando de establecer una sesión de extremo a extremo entre dos usuarios. Es por esto que, los conceptos de señalización, enrutamiento y direccionamiento son similares.

Básicamente se debe seguir una secuencia para poder integrar y mejorar servicios en las redes de comunicaciones del SAT, como es una evaluación de la red actual contando los recursos con que ya cuenta, dicha información se plantea en el capítulo 3 y 4 de este documento. Establecer objetivos generales para integrar la red. Evaluar la tecnología existente y la disponible, hacer un análisis financiero para evaluar el factor costo-beneficio.

Una ventaja de las redes informáticas es la capacidad de compartir recursos, siendo que en las redes de voz esto no es posible. Por lo tanto, la integración de servicios de voz y datos permite la reducción de costos.

5.1.1 Inventario

En el capítulo 4 se obtuvo el inventario general de los recursos con los que cuenta la red del SAT, es decir, revisamos el equipo existente y evaluamos su capacidad de operación. Se ha determinado también la necesidad de la transmisión de voz, datos, facsímil y vídeo.

Se ha hecho también un estudio del tráfico a través de la red para implementar servicios de valor agregado y mejorar la calidad en el servicio de transmisión de datos. En este caso se modificará la red y tal vez sea necesario quitar algunos enlaces mientras que otros pueden crecer, y de acuerdo al análisis financiero se tomará la opción de compra o arrendamiento para que el factor costo-beneficio sea lo más óptimo posible.

5.1.2 Objetivos para la Red

Una vez que tenemos la información de todos los recursos de nuestra red actual y el planteamiento de nuestras necesidades actuales y próximas, el siguiente paso es plantear los objetivos de nuestra red que en este caso es la integración de nuevos servicios y el mejoramiento de la transmisión de datos.

Determinaremos el tipo de tráfico predominante en la red actual y cual es el que la red está capacitada para soportar, ya que debemos incluir el transporte de voz, datos y vídeo a través de la red WAN para comunicar a las diferentes oficinas remotas que existen en esta entidad, así como las facilidades de conexión que se prestarán a los usuarios de esta red.

5.1.3 Revisión de Tecnologías y Servicios

A continuación se evaluarán las tecnologías y servicios disponibles para seleccionar el modelo y la tecnología que más nos ayude a cumplir con los objetivos planteados.

Todos los sistemas de paquetes de voz siguen un modelo común. La red de transporte de paquetes de voz, la cual puede estar basada en las tradicionales "nubes" de IP, Frame Relay, ATM. En los extremos de estas nubes hay dispositivos que se pueden llamar "agentes de voz". La misión de estos dispositivos es de cambiar la información de la voz desde su forma telefónica tradicional a una forma capaz de ser transmitida en paquetes. Entonces la red podrá enviar los paquetes de datos a un agente de voz que esté sirviendo para llevarlo a su destino o a la parte llamada.

La integración de las redes de voz y datos debe incluir una evaluación de estas tres tecnologías:

- ✓ Voz sobre ATM (VoATM)
- ✓ Voz sobre Frame Relay (VoFR)
- ✓ Voz sobre IP (VoIP)

Existen dos modelos básicos para la integración de voz sobre una red de datos, Transporte vs. Traducción.

Transporte es el soporte transparente de la voz sobre la red de datos existente. Un ejemplo es la simulación de líneas dedicadas sobre ATM usando la emulación de circuitos.

Traducción se refiere, como su nombre lo indica, a la traducción de las funciones tradicionales de voz por la infraestructura de datos. Un ejemplo podría ser la interpretación de la señalización de voz y la creación de SVCs en ATM. Las redes de Traducción son más complejas que las redes de transporte y su implementación es todavía punto de discusión con las instituciones encargadas de estandarizar las tecnologías.

Se deberá evaluar y seleccionar el modelo más apropiado basado en la disponibilidad, costo y consideraciones técnicas.

Enseguida se presenta un resumen de las tres alternativas en tecnologías que mencionamos arriba.

ATM es orientado-a-conexión. Fue diseñado para manejar tráfico sensible al tiempo, tal como la voz. Su señalización, direccionamiento y enrutamiento, nos permitirá construir una red que siga el modelo de Traducción. La función de enrutamiento en particular robusto, permitiendo hacer conexiones basándose en encontrar un cierto retardo y variaciones de retardos.

Frame Relay tiene facilidades para especificar que tiene voz, en el campo que especifica el tipo de información. También es relativamente bajo en costo y muy común en muchas partes del mundo. Los servicios de Frame Relay pueden proporcionar SVC's (Circuito Virtual Conmutado), PVC's (Circuito Virtual Privado) y QoS (Calidad de Servicio), pero por su sencilla señalización, su funcionalidad de enrutamiento y direccionamiento previene de ir mas allá del modelo de transporte hacia la construcción del modelo de traducción.

IP es una tecnología no orientada a conexión, se desarrolla en áreas de prioritización, reservación del recurso y fragmentación de paquetes, todos relativamente nuevos. IP como ATM tienen señalización robusta, funcionalidad de enrutamiento y direccionamiento, lo cual hacen una posibilidad para el modelo de traducción. Otros incentivos para IP es su facilidad de integración con las actuales aplicaciones de datos y su ubiquidad.

Después de evaluar las tecnologías y servicios de voz sobre una red de datos, se deben cubrir ciertas consideraciones, tal como factores que pueden impactar potencialmente la calidad de la voz. Lo primero a considerar son los métodos de codificación y compresión de voz (referirse al capítulo 3). También debemos considerar como otro factor potencial el retardo y la variación de

retardo, más comúnmente mencionados como Jitter digital. El retardo puede provocar en primera instancia, si es muy largo, que el segundo conversador empiece a hablar antes de que el primero termine, y en segunda instancia, el retardo puede provocar eco, lo cual es el reflejo de la señal original que regresa al transmisor y esto provoca distracción en la conversación. Estas características provocan que la calidad de la transmisión de voz en una red principalmente hecha para transmitir datos, se degrade un poco, sin embargo, al utilizar los algoritmos de compresión de voz, podremos obtener un ahorro de ancho de banda, lo cual trae como consecuencia reducción de costos. Aunado a esto, el utilizar una única red para transmitir voz y datos, así como otras aplicaciones, nos generará ahorros significativos en costos de larga distancia.

5.1.4 Planeación de Capacidades

El aprovisionamiento de líneas troncales se lleva a cabo estableciendo el número de troncales que habrá del PBX hacia la red de voz y datos. Después de establecer las troncales, el siguiente paso es trasladar ese número al ancho de banda requerido en la red.

El número correcto de sistemas de troncales se determinará por el volumen y flujo de tráfico y otros objetivos específicos de la red. Se tiene la opción de simplemente mover las troncales de la red actual a la red integrada o se puede aprovechar la oportunidad rehacer la ingeniería de tráfico y actualizar este estudio de acuerdo a las nuevas aplicaciones de datos.

El uso del modelo de transporte o del modelo de traducción puede tener un gran impacto en el número de troncales simuladas por la red. El modelo de red de transporte es de acuerdo a una conexión virtual para una línea privada en base a Una-por-Una. Para la ingeniería de voz, realmente no cambia nada. De cualquier forma, el modelo de traducción utiliza la red para simular un PBX tandem, de ahí que se reducen potencialmente el número de troncales requeridas. El enrutamiento de llamadas sobre grupos específicos de troncales en el cual un grupo podría ser la red de voz y datos integrada, es manejada por la ingeniería de voz, es decir que, un ingeniero tiene la opción de elegir utilizar la red como primera opción, mientras que otros pueden tenerlo como la última opción.

Entonces, basándose en el diseño de red propuesto y el número de troncales requeridas entre localidades, se podrá calcular el ancho de banda requerido. Estos cálculos deben basarse en la compresión utilizada, overhead y utilización, cada uno de estos variará dependiendo de la tecnología de voz sobre una red de datos que se va a utilizar. Después se calcula la matriz de retardos entre locaciones y asegurarse de que los cálculos de estos retardos están dentro de los límites requeridos. Si no es así, se deberá ajustar el ancho de banda o seleccionar una tecnología de voz sobre una red de datos diferente.

5.1.5 Análisis Financiero

Una vez que se han planteado los objetivos, la tecnología o tecnologías de voz paquetizada elegidas, completado el plan de capacidad y el dimensionamiento apropiado de las troncales para soportar el tráfico adicional en base al estudio de retardo. Ahora la pregunta que se debe plantear es si el costo de la red es justificable.

En el caso que estamos presentando en esta Tesis, tratándose de una compañía de cobertura nacional y en donde se pretende utilizar un servicio público de Frame Relay, así como, determinar la factibilidad de hacer del SAT una red de conmutación rápida, con capacidad de manejar aplicaciones como la interconectividad de redes locales de datos o aquellas que requieran amplio ancho de banda, como el procesamiento de imágenes y gráficas, grandes transferencias de archivos entre computadoras, además de la integración del servicio de voz sobre la misma red de

datos, como valor agregado. Para llevar a cabo lo anterior, conviene recordar aquí los tres requerimientos mínimos para la aplicación de la tecnología de frame relay:

- ✓ El empleo de dispositivos terminales con mayor inteligencia y con capacidad de manejo de protocolos de capas superiores.
- ✓ El empleo de líneas de transmisión virtualmente libres de error (tal como la fibra óptica)
- ✓ El empleo de dispositivos terminales con mayor inteligencia y con capacidad de manejo de prioridades.

Por otro lado, una de las características importantes de Frame Relay y que ofrece una ventaja muy favorable para el caso de la red del SAT, es su capacidad de coexistir en un ambiente híbrido, es decir, seguir manejando tecnologías como X.25 o ATM en aquellos lugares y/o trayectorias que así lo requieran, y aplicar la tecnología de Frame relay en aquellos enlaces con suficiente demanda y que reúnan la calidad de línea requerida por Frame Relay. Lo anterior da como resultado que la red del SAT pueda de manera gradual ir alcanzando la calidad antes mencionada, de acuerdo a sus propias características de crecimiento, así como permitir agregar servicios.

Esta posibilidad de migración a una red de tipo Frame Relay se puede hacer modificando o agregando software y hardware en cada uno de los nodos de la dorsal. Para lo cual se ha planteado en el capítulo cuarto el equipo de acceso asociado a la red (CPE o Customer Premise Equipment), el equipo de conmutación dentro de la dorsal, el medio físico en las trayectorias, así como la topología de la propia red, estableciendo también una serie de planteamiento relacionados con la administración de la red.

Equipo de Acceso a la Red de Frame Relay

El equipo terminal (DTE) tiene como responsabilidad asegurar una transmisión de datos terminal a terminal libre de error. Afortunadamente, cada día los dispositivos terminales, especialmente aquellos que, asociados a las redes locales de datos tienen la suficiente inteligencia y potencia de procesamiento para efectuar dichas funciones. Por su parte, los equipos de acceso a una red de frame relay pueden ser puentes, enrutadores gateways, frads o bien, interfaces que ya vienen contenidas dentro del equipo de cómputo.

El equipo de comunicaciones (DCE), o de acceso a la red, lo más usado es el enrutador (router), estos dispositivos soportan la mayoría de los protocolos, por ejemplo X.25, FR, TCP/IP, RIP, FTP, SNMP, IPX, NetBios, etc. En suma, se puede decir que el equipo de usuario (CPE) debe de tener la inteligencia suficiente para reconocer y retransmitir paquetes que no estén libres de error, además de enrutar el direccionamiento de cada paquete de acuerdo al destino especificado.

Para el caso de la red del SAT, será necesario que los usuarios conectados a la misma, cuenten con la interfaz frame relay provista por un enrutador.

Equipo de Conmutación Asociado a la Dorsal de Frame Relay

Dadas las características de una red de frame relay, de procesamiento nodal, sólo entre puntos terminales de la red, se requiere que el equipo de conmutación Frame Relay asociado a la dorsal de alta velocidad cumpla con las siguientes características:

- ✓ Manejar altas velocidades de transmisión (2 a 34 Mbps)
- ✓ Ser eficiente en el manejo de tráfico tipo ráfaga (característico de las redes locales de datos)
- ✓ Capaz de asignar el ancho de banda dinámicamente

- ✓ Alto desempeño (típico de 4000 paquetes por segundo)
- ✓ Bajo retardo de conmutación (menor de 3 mseg)

Todo lo anterior trae como beneficio una mejora sustancial en el desempeño y tiempo de respuesta de la red, que al emplear Frame Relay, presenta una reducción considerable en su complejidad, ya que mediante un solo tipo de acceso es capaz de manejar diferentes tipos de tráfico. Una gran ventaja es que tipo de equipos presentan un desarrollo comercial muy fuerte soportando estándares y con más de 50 fabricantes de equipo.

Una vez definido el equipo terminal, así como el de comunicaciones, queda la tarea de establecer la dorsal, como primera fase se ha pensado en una red frame relay con posibilidad, en su segunda fase, de emigrar fácilmente a una red de banda amplia (ATM). Es importante remarcar que esto implicaría el hecho de sólo agregar nuevos módulos al equipo de conmutación, no la compra de otro equipo, manteniéndose la idea de un cambio gradual y la del aprovechamiento de la plataforma existente.

En general la topología se basa en el arreglo ya existente, salvo algunos cambios que se consideran importantes para un mejor desempeño de la red y para poder adicionar servicios en la misma.

El medio de transmisión que se utilizará en la dorsal (troncales entre nodos) serán troncales E1 a una velocidad de 2.048 Mbps. La red SAT de alta velocidad se constituirá con equipo Frame Relay no existente en la red (enrutadores y conmutadores – FRADs). En cada uno de los nodos principales de la dorsal de frame relay existirá un conmutador frame relay. Este equipo se divide básicamente en dos partes: el lado de red y el lado del usuario, tal como se muestra en la figura.

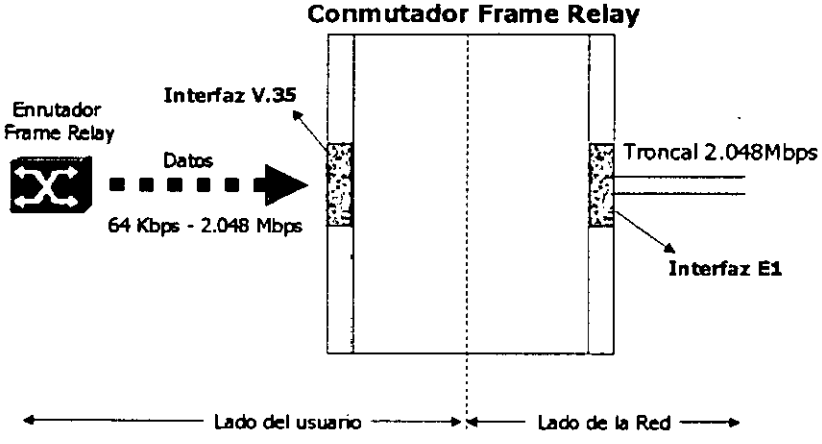


Figura 5.1 Conmutador Frame Relay

En el lado de la red se tendrán líneas con interfaces E1 (2.048Mbps) por las cuales llegarán o se transmitirán paquetes con información local o de tránsito. En el lado del usuario existirán módulos frame relay con interfaces V.35, las cuales recibirán el tráfico SNA, TCP/IP, Voz, Vídeo, Ethernet, etc. A velocidades de acceso de 64kbps hasta 2.048Mbps.

La información que tenga que entrar a la dorsal, será pasada por un frad (frame relay access device), el cual se encargará de empaquetar esta información en frame relay para transportarla a su destino correspondiente, tal como se explica en el capítulo tres.

Administración de la red

El sistema de control de la red debe cumplir con las siguientes funciones de supervisión y monitoreo de:

- ✓ Fallas
- ✓ Configuración
- ✓ Rendimiento
- ✓ Contabilidad
- ✓ Seguridad

Para la red frame relay, la supervisión y el monitoreo es relativamente sencillo, ya que los elementos de red son dispositivos inteligentes con capacidad para realizar la mayoría de las funciones de monitoreo autónomamente como el auto-restablecimiento de fallas, auto-diagnóstico, creación de mensajes, los cuales son enviados al equipo de cómputo conformado éste por una estación de trabajo (workstation), con sus respectivos periféricos y un software propietario del fabricante de los elementos de red, que por lo regular tiene la capacidad y características para poder monitorear otros elementos de red que no correspondan al mismo fabricante. Aquí se procesa la información recibida desde los elementos de red para la generación de bases de datos, reportes de contabilidad, análisis de la configuración de la red, estado de las troncales y enlaces, además de desplegar la topología de la dorsal en tiempo real, monitorear simultáneamente múltiples puntos de la red.

Se recomienda tener un sistema de monitoreo y administración centralizado y tener sólo un sistema de respaldo en otro nodo. Una opción más que presentan estos elementos, es la de proveer un monitoreo parcial a través de una terminal VT100. Este tipo de monitor se podría tener en cada nodo de la dorsal, para una mejor supervisión del sistema.

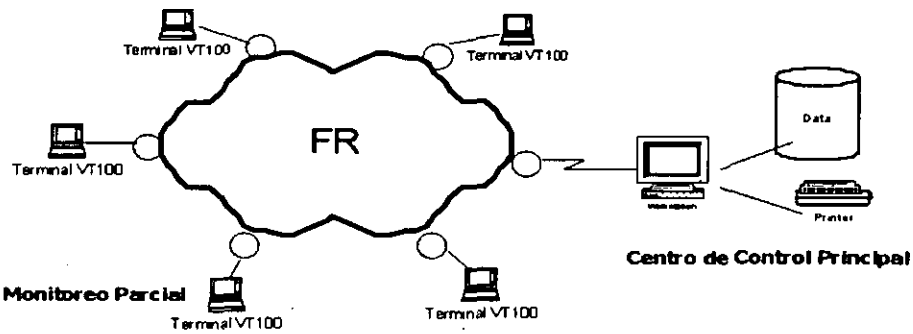


Figura 5.2 Configuración de la administración de la dorsal Frame Relay

El SAT tiene sus oficinas principales en la República Mexicana, están en las ciudades de México, Guadalajara, Monterrey, Puebla, Querétaro, y Yucatán.

La mayoría de las llamadas son entre los empleados de la red en la misma ciudad y clientes locales. Solamente alrededor del 20% del volumen total de llamadas es entre empleados del distintas ciudades. A pesar de que este último volumen mencionado es el pequeño, también es el más costoso en base al minuto por llamada, puesto que es facturado como llamada de larga distancia. Como resultado de estas llamadas, el SAT paga alrededor de $15,000.00 mensuales en cada nodo.

Los servicios de voz se proporcionan por pequeños PBXs conectados a la Red Telefónica Pública Conmutada (PSTN). Para asegurar un análisis financiero conservador, asumiremos que el volumen de llamadas del SAT es lo suficientemente grande como para obtener un descuento en el contrato de un enlace privado y que de acuerdo a los estándares de descuentos que ofrecen los operadores es del 15%.

Cada individuo en la oficina pasa alrededor de una hora y media por día comunicándose vía telefónica o vía fax. Un poco más de un cuarto de esta hora va desde y hacia las oficinas que están en la rama de la red y las oficinas centrales. La tabla siguiente muestra el volumen potencial de tráfico de voz y fax y su costo.

Locación C. Hidalgo	Tipo	# Personas	Promedio Mins. Por persona al día	% de Tráfico a otra Cd.	Días de trabajo al mes	Total de Mins. Por persona por mes	Total de Mins. Por Oficina por mes	Costo por Min.	Costo mensual por Oficina
Módulo 1	Local	167	90	20%	21,67	390,06	65140,02	$ 5,00	$ 325.700,10
Módulo 2	Local	527	90	20%	21,67	390,06	205561,62	$ 5,00	$1.027.808,10
Módulo 3	Local	700	90	20%	21,67	390,06	273042	$ 5,00	$1.365.210,00
Módulo 4	Local	1139	90	20%	21,67	390,06	444278,34	$ 5,00	$2.221.391,70
Módulo 5	Local	552	90	20%	21,67	390,06	215313,12	$ 5,00	$1.076.565,60
Módulo 6	Local	681	90	20%	21,67	390,06	265630,86	$ 5,00	$1.328.154,30
Módulo 7	Local	556	90	20%	21,67	390,06	216873,36	$ 5,00	$1.084.366,80
Módulo 8	Local	187	90	20%	21,67	390,06	72941,22	$ 5,00	$ 364.706,10
Guadalajara	Regional	20	90	20%	21,67	390,06	7801,2	$ 5,00	$ 39.006,00
Monterrey	Regional	35	90	20%	21,67	390,06	13652,1	$ 5,00	$ 68.260,50
Puebla	Regional	30	90	20%	21,67	390,06	11701,8	$ 5,00	$ 58.509,00
Querétaro	Regional	30	90	20%	21,67	390,06	11701,8	$ 5,00	$ 58.509,00
Yucatán	Regional	15	90	20%	21,67	390,06	5850,9	$ 5,00	$ 29.254,50

Tabla 5.1 Volumen y costos de la PSTN

Supuestos:

- ✓ Este es el promedio del costo por minuto y se asume que el 50% de las llamadas son hacia las ciudades y otro 50% desde las ciudades.
- ✓ El costo de la llamada de voz está basada en la cuota del operador sin impuestos y con descuento.

El SAT utilizará servicio de frame relay público. La topología se muestra en la figura 5.2. La configuración de la red y los gastos mensuales concurrentes o Run-Rate, se muestran en la tabla 5.1. Nota, sólo hay un PVC (Circuito Virtual Privado) para enlazar las ciudades.

Locación	Tipo	Línea de Acceso	Velocidad Inicial del Puerto	CIR Inicial del PVC	Cargos de Frame Relay
Módulo 1	Local	E-1	128	64	$ 3.000,00
Módulo 2	Local	E-1	128	128	$ 5.700,00
Módulo 3	Local	E-1	128	128	$ 5.700,00
Módulo 4	Local	E-1	128	128	$ 5.700,00
Módulo 5	Local	E-1	128	128	$ 5.700,00
Módulo 6	Local	E-1	128	128	$ 5.700,00
Módulo 7	Local	E-1	128	128	$ 5.700,00
Módulo 8	Local	E-1	128	64	$ 5.700,00

Guadalajara	Regional	E-1	128	64	$ 3.500,00
Monterrey	Regional	E-1	128	64	$ 3.000,00
Puebla	Regional	E-1	128	64	$ 3.500,00
Querétaro	Regional	E-1	128	64	$ 3.000,00
Yucatán	Regional	E-1	128	64	$ 4.000,00
TOTAL					$59.900,00

Tabla 5.2. Configuración Inicial de la Red

En este caso se puede utilizar cualquiera de las tecnologías de paquetización de voz para hacer una red multiservicios. De cualquier forma, debido a la familiaridad, simplicidad, conectividad y costo con Frame Relay, se eligió Voz sobre Frame Relay.

5.2 REDISEÑO DE RED

El objetivo para rediseñar la red de datos es para soportar tráfico de voz adicional para que no afecte en forma adversa el rendimiento de la misma. El primer paso, como se mencionó anteriormente es determinar el ancho de banda adicional requerido en la red de datos para soportar tráfico de voz y fax, la mejor manera de hacerlo es recolectando información de tráfico tanto del PBX como del ruteador y graficar el tráfico de voz y datos simultáneamente para observar que tan frecuente la combinación del tráfico excede el ancho de banda disponible.

Si esta información no fuera fácil de conseguir, entonces se deberá estimar cuanto o si es requerido más ancho de banda. Se recomienda hacer pruebas de la calidad de la voz simultáneamente con la carga de datos en el enlace, para estimar el ancho de banda requerido.

Esto es, aumentando el ancho de banda, pasar datos y voz, si el usuario nota latencia en los datos y/o decremento en la calidad de la voz, entonces se deberá aumentar el ancho de banda. Regularmente, el tráfico de voz y datos llegan a los picos en diferentes horas del día.

Consecuentemente, la red de datos se verá beneficiada con el ancho de banda adicional.

La red es rediseñada considerando los siguientes supuestos:

- ✓ El volumen total de voz y fax por persona será igual a aproximadamente 90 minutos por día.
- ✓ El volumen de llamadas entre ciudades y entre las LANs representa alrededor del 20% del total del volumen de llamadas o aproximadamente ¼ de hora.
- ✓ Se considera apropiado un factor de carga (horas ocupadas) del 17%.
- ✓ La voz será comprimida a 8Kbps, más 8Kbps de overhead (11Kbps). Así que cada troncal de 64Kbps soporta 5 canales de voz.
- ✓ El PBX en las oficinas requiere módulos de troncales adicionales.

La cantidad de tráfico de voz y fax será determinado con las suposiciones escritas arriba. En la tabla 5.3 se resumen los cálculos para proporcionar el número de troncales en el PBX que se requerirían en cada sitio.

No. De Usuarios	No. De Sitios	Hrs. por día en el teléfono	Mins. Por día	Hrs. Pico (17%)	Mins. Por Hr. Pico	% de tráfico a la OC	Total de Erlangs al OC	Líneas Requeridas para el bloque de probabilidad de 0.05
167	1	1,5	15030	0,17	2555,1	20%	0,1	3
527	1	1,5	47430	0,17	8063,1	20%	0,1	6
700	1	1,5	63000	0,17	10710	20%	0,1	6
1139	1	1,5	102510	0,17	17426,7	20%	0,1	8
552	1	1,5	49680	0,17	8445,6	20%	0,1	6
681	1	1,5	61290	0,17	10419,3	20%	0,1	6
556	1	1,5	50040	0,17	8506,8	20%	0,1	6
187	1	1,5	16830	0,17	2861,1	20%	0,1	3
20	1	1	1200	0,17	204	20%	0,1	1
35	1	1	2100	0,17	357	20%	0,1	1
30	1	1	1800	0,17	306	20%	0,1	1
30	1	1	1800	0,17	306	20%	0,1	1
15	1	1	900	0,17	153	20%	0,1	1
				Total de Erlangs por OC			*1,3*	*49*

Tabla 5.3. Análisis de Troncales

Las oficinas más grandes que cuentan con 1139 personas, se planearon de tal manera que lleven un máximo de 8 líneas de voz de tráfico sobre la red Frame Relay. Esta ráfaga de datos a su máximo podrá alcanzar 88Kbps (siempre y cuando cada línea de voz pueda cargar un máximo de 11kbps). El puerto en la oficina remotas se aumentará de 128kbps a 256kbps, lo bastante holgado para poder tener un alto desempeño en la red (reducir el retraso del buffer en el puerto), para el tráfico más sensible y para dejar espacio para crecimiento a futuro. El PVC CIR se incrementará de 64kbps a 128kbps, para asegurar que el retraso debido a la probable congestión de red del proveedor, sea mínimo también, como antes, con una red de frame relay, se deberá observar muy de cerca la mediciones de latencia para ver que el PVC CIR esté configurado correctamente.

El siguiente paso es determinar el ancho de banda adicional requerido en la red de frame relay para soportar el tráfico de voz y fax. Como se indicó en las suposiciones, cada 64kbps de ancho de banda proveerá un mínimo de 5 canales de voz.

Cada oficina remota fue enlazada originalmente a la red de frame relay vía un puerto de 128kbps (utilizando una línea de acceso E1), con un PVC puesto a 64kbps. Esto era más que suficiente para manejar el tráfico de datos, sin embargo no era suficiente para manejar también el tráfico de voz comprimida, así que el ancho de banda para cada localidad tiene que ser actualizada.

En lugar de hacer estudios para cada localidad, se considerará actualizar todas las localidades con el mismo nivel de ancho de banda, para un mejor desempeño y dejar cierta capacidad disponible para futuros requerimientos.

Este aumento de ancho de banda es también para mejorar el desempeño de la transmisión de datos. El tráfico de voz, aún en su máximo requerimiento, toma todavía menos ancho de banda que el que tendrá el nuevo puerto de mayor velocidad. Además, el tráfico de voz, siendo excepcionalmente variable sobre el tiempo, deja el ancho de banda disponibilidad para una transmisión más rápida en datos durante la mayor parte del día. Mientras que el tráfico de voz y su pico adiciona una carga extra de 88kbps al circuito de frame relay, en promedio adiciona menos de 30kbps de datos a lo largo del día. El resto de lo actualizado del ancho de banda (128kbps) es para mejorar el desempeño de la los datos en la red.

Si se requiriera más ahorros, a las oficinas más pequeñas se les podría dejar un circuito de un poco de mayor velocidad. Se considera que en las oficinas locales se necesitan añadir 5 o 6 circuitos de voz añadiendo al puerto 64kbps (actualizando de 128kbps a 192kbps) y sería más que suficiente.

Conforme la institución lo siga soportando en el caso de los negocios, de cualquier forma, es preferible actualizar la red una sola vez e ir reduciendo el ancho de banda, los gastos, de acuerdo a los patrones y a la experiencia.

CPE

Se instaló en cada oficina local y en la central un equipo Concentrador de Acceso Múltiple marca Cisco modelo MC3800, como se puede ver en la tabla 5.4, la velocidad de los puertos y el CIR de los PVC's se incrementaron para acomodar el tráfico de voz. No fue necesario adicionar un PVC para la voz, ya que el MC3800 da prioridades de tráfico en un sólo PVC. Esta opción permite olvidar el costo de otro PVC.

Cada oficina local se conecta con el número de troncales apropiadas del PBX al equipo de Acceso Múltiple MC3800. El PBX puede direccionar aproximadamente el 95% del tráfico destinado a las oficinas centrales y regionales preferentemente a una de las troncales conectadas al equipo MC3800. El resto del tráfico estimado 5%, es direccionado a la PSTN (Red Pública de Telefonía Conmutada).

Usando el logaritmo de compresión G.729, el MC3800 comprime cada canal de voz de 64kbps a una trama de datos de aproximadamente 11kbps (8kbps más 3kbps de encabezado), direccionando este tráfico de voz comprimido a través de la red frame relay. Los 11kbps es una cantidad conservadora porque todavía no se incluyen algunas bondades de este tipo de multiplexores, como es el caso de técnicas de supresión de silencio, etc.

El MC3800 es capaz de transportar hasta 24 canales de voz comprimida a 8kbps que se podrá transportar a través de una red pública o privada de frame relay, ATM o líneas privadas.

Existen varios diseños de red que pueden ser aplicables para esta institución. Una opción es aumentar un PVC para transportar el tráfico de voz. Lo anterior no nos permitiría aprovechar la priorización del tráfico y por lo tanto el ahorro de ancho de banda, así como su mayor aprovechamiento. Además que la mayoría de los proveedores de redes públicas de frame relay cobran por PVC. Al utilizar un sólo PVC para transportar voz y datos nos ahorraría muchos costos.

De igual forma, requerimos que nuestro equipo Multiplexor nos permita administrar el tráfico de voz de manera centralizada, por ejemplo, poder configurarlo para que conmute las llamadas entre las oficinas locales y regionales. Como un valor agregado, el equipo multiplexor está preparado para soportar vídeo conferencia o vídeo sobre IP para cuando sea requerido.

Locación	Tipo	Línea de Acceso	Velocidad Inicial del Puerto	CIR Inicial del PVC	Cargos de Frame Relay	Velocidad del Puerto Actualizada	Actualización del CIR del PVC	Cargos de Frame Relay	Costos por actualización
Módulo 1	Local	E-1	128	64	$ 3.000,00	256	128	$ 4.756,00	$ 1.756,00
Módulo 2	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 3	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 4	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 5	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 6	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 7	Local	E-1	128	128	$ 5.700,00	2048	128	$ 10.598,00	$ 4.898,00
Módulo 8	Local	E-1	128	64	$ 5.700,00	256	128	$ 8.806,00	$ 3.106,00
Guadalajara	Regional	E-1	128	64	$ 3.500,00	256	128	$ 5.506,00	$ 2.006,00
Monterrey	Regional	E-1	128	64	$ 3.000,00	256	128	$ 4.756,00	$ 1.756,00
Puebla	Regional	E-1	128	64	$ 3.500,00	256	128	$ 5.506,00	$ 2.006,00
Querétaro	Regional	E-1	128	64	$ 3.000,00	256	128	$ 4.756,00	$ 1.756,00
Yucatán	Regional	E-1	128	64	$ 4.000,00	256	128	$ 6.256,00	$ 2.256,00
TOTAL					**$ 59.900,00**			**$ 103.930,00**	**$ 44.030,00**

Tabla 5.4 Costo de actualización de la red para soportar el tráfico de voz adicional

Análisis Financiero

Los costos para las oficinas locales y regionales, así como para la central, se muestran en la tabla 5.5. Los costos para el ancho de banda adicional se muestran en la tabla anterior, siendo $44,030.00 por mes. Comparando los ahorros a estos costos adicionales en la tabla 5.6, se ilustra los ahorros mensuales netos por mes.

Enrutador-Multiplexor Cisco MC3800s	$ 520,000.00
Módulos troncales requeridos en el PBX de las Ofic. locales	$ 50,000.00
No. Requerido	12
Total	**$ 600,000.00**
Módulos troncales requeridos en el PBX de la Ofic. Central	$ 100,000.00
No. Requerido	1
Total	**$ 100,000.00**
Costo total del capital	**$ 1,220,000.00**

Tabla 5.5 Costos

Gastos mensuales por PSTN	$ 540,000.00
Multiplicado por 95%	95%
Ahorros mensuales en la PSTN	$ 513,000.00
Costo de ancho de banda requerido	$ 44,030.00
Total de ahorros mensuales netos	**$ 468,970.00**
Ahorros netos anuales	**$ 5,627,640.00**
Costo total del capital	$ 1,220,000.00
Instalación	$ 200,000.00
Total costos de capital	**$ 1,420,000.00**
Periodo de recuperación de inversión	**8 meses**

Tabla 5.6 Ahorros anuales

La institución ahorra $ 5,627,640.00 por año si migra el tráfico de voz sobre la misma red de datos frame relay. El periodo de recuperación de la inversión es de aproximadamente 8 meses.

En una organización, el costo de las llamadas por minuto es muy alto, como se muestra en la tabla 5.1. Para enviar el 95% del tráfico en la misma red de datos, se requiere actualizarla en el ancho de banda, lo cual representa un costo, sin embargo, en un periodo determinado se concluye que el costo por llamada por minuto se reduce en aproximadamente un 30%, lo cual trae como consecuencia un ahorro en costos de larga distancia como valor agregado, además del mejor desempeño de nuestra red de datos y la posibilidad de agregar servicios de vídeo a futuro.

Es muy importante tener referencias de otros productos que nos pueda dar la solución con los resultados esperados, para poder hacer comparaciones y elegir siempre lo más óptimo para nuestros proyectos. Enseguida se muestran los costos aproximados de un servicio satelital y de un servicio con fibra óptica.

Renta de un enlace Satelital con capacidad de un E1:

Capacidad Satelital = $ 4,000.00 Dlls. Por 1 MHz, con QPSK se utilizan 4 MHz por portadoras de Tx 2 MHz y Rx 2 MHz, dando un total de $ 16,000.00 Dlls. Mensuales.

Equipo de 2 estaciones con antenas de 3.8 mts. De diámetro = $40,000.00 de inicio.

Servicio que incluye Instalación, Reparación, Call Center, Administración del enlace = $18,000.00 Dlls. Mensuales.

Renta de un enlace de Fibra Optica:

Renta de un enlace de Fibra Optica Clear Channel de Tijuana a Cancún (Puntos más alejados dentro del territorio de la República mexicana) = $18,000.00 Dlls. Mensuales.

Instalación $10,000.00 dlls.

CONCLUSIONES

De acuerdo a lo presentado en este trabajo, en cuanto a los desarrollos y expectativas de las tecnologías de voz y datos, las tendencias y expectativas internacionales para el empleo de la tecnología Frame Relay, ATM, IP como dorsales de alta velocidad y el estado actual de la red de comunicaciones del SAT, se pueden concluir los siguientes aspectos relativos a la factibilidad de aplicación de dichas tecnologías a la red del SAT:

1. La tecnología Frame Relay permite hacer una red muy rápida con optimización del ancho de banda, aplicada como dorsal en redes de cobertura amplia para la interconectividad de redes locales de datos, para emplear aplicaciones que requieran el manejo de altos volúmenes de información, para la transferencia de gráficas o imágenes e inclusive el manejo de voz.

2. Frame Relay permite también, reducir los costos de operación y de mantenimiento de una red de conmutación de paquetes ya que las características de operación de dicha tecnología están definidas en las especificaciones Q.921 de la ITU las cuales constituyen una estandarización de acceso al medio, por lo que los dispositivos Frame Relay pueden instalarse en una red de datos que este en operación, sufriendo solamente ligeros cambios en la programación de esta manera, es posible integrar el protocolo Frame Relay de manera transparente.

3. De acuerdo con las expectativas de desarrollo comercial de Frame Relay, se tiene que los fabricantes ya ofrecen productos con la tecnología para integrar la información de voz, datos y vídeo algunos de los más importantes que ya tienen en el mercado sus productos con esta tecnología son: Cisco Systems, Stratacom, Nortel, Lucent Technologies, Motorola, etc.

Se puede decir entonces que Frame Relay es una tecnología perfectamente definida, soportada por estándares internacionales y con alto apoyo y desarrollo comercial, resultando una tecnología altamente costeable ya que decrece la cantidad de inversión en equipo con la capacidad especial de poderse adaptar con la infraestructura y dispositivos (puentes, enrutadores, conmutadores, etc.) ya existentes, dándole con esto un gran empuje al mercado de interconectividad de redes locales.

Una vez instalada la dorsal Frame Relay en la red del SAT esta tendrá capacidades potenciales que pueden ser explotadas según las necesidades y demandas de los usuarios. Los servicios adicionales que podrá ofrecer de manera inmediata (con solo agregar nuevos módulos a los conmutadores) son:

- ✓ Servicio de Fax rápido
- ✓ Servicio de voz paquetizada
- ✓ Aplicaciones de datos más robustas
- ✓ Vídeo
- ✓ Videoconferencia

Se recomienda utilizar un software de administración de la red para mantener el control de la misma, así como capacitar al personal técnico involucrado en la operación de la red con el objetivo de tener una máxima eficiencia, control y seguridad en la transmisión de información.

Una de las ventajas de este trabajo es que su contenido es una recopilación de información que no esta disponible en una sola bibliografía.

Finalmente, el haber hecho una investigación que incluye conceptos teóricos, costos y necesidades reales de una empresa en el área de comunicaciones, nos dio la oportunidad de poder aplicar dichos conceptos para optimizar una red de datos ya existente en un caso practico; Así mismo, es un material de apoyo para los nuevos estudiantes en su formación profesional dentro del área de comunicaciones.

APENDICE A
MEDIOS DE TRANSMISIÓN

INTERFACES FISICAS

	CONECTORES
RS-232	DB-9
V.35	DB-25
RS-422/449	Manchester 34

MEDIOS PRIMARIOS

	CONECTORES	
CABLE COAXIAL	BNC ó N	
PAR TRENZADO	RJ-11	
	RJ-12	
	RJ-45	
FIBRA OPTICA	ST	Signal terminator
	FDDI	Fiber Distributed Data Interface

MEDIOS SECUNDARIOS

MICROONDAS
SATELITES

RS-232
Diseñada para comunicación serial asíncrono / Síncrona de baja velocidad entre DTE y DCE con velocidades entre 300bps y 19,200 (hasta 56 kbps)

RS-442 y RS-449
Diseñada para conexiones seriales síncronas / asíncronas de alta velocidad y a grandes distancias desde 100 Kbps hasta 10 Mbps.

V.35
Diseñada para conexión serial Síncrona de lata velocidad para enlaces remotos utilizando un conector tipo Manchester de 34 pines con velocidades desde 40 kbps hasta 168 kbps (2.048 mbps)

CABLE COAXIAL DELGADO
Clasificación RG-58 y RG-59 cumple con IEEE 802.3 10base2 (10 Mbps/baseband/200mts./ Impedancia de 50 ohms) con óptimo inmunidad EMI/RFI (interferencia electromágnetica y de radiofrecuencia)

CABLE COAXIAL GRUESO
Clasificación RG-8 y RG-9 cumple con las características del cable coaxial delgado pero con mejor inmunidad al EMI y RFI.

CATV
Clasificación RG-6 utilizado en redes Broadband 802.4 y transmisión de vídeo inpedancia de 75 ohms y excelente inmunidad al EMI y RFI.

CABLE PAR TRENZADO
Calibres 22,24 y 26 AWG (dat/data-voice/voice grade) cumple con IEEE 802.3 10baseT (10 Mbps/baseband/ Twisted pair) hilos codificados con colores (primario/secundario) y baja inmunidad a EMI y RFI y conectores de (8,4 y 6 hilos)

TIPOS DE CABLES

Tipo 1	STP, 2 pares blindados
Tipo 2	STP 2 pares blindados, 4 fuera de blindaje
Tipo 3	UTP 2 parres
Tipo 5	2 fibras de 100/140 micras
Tipo 6	STP, 2 pares (patch cables)

STP Shielded twisted pair (cable con aislamiento)
UTP unshielded twisted pair

FIBRA OPTICA
Filamentos de vidrio/plástico que conducen impulsos luminosos con diametros comúnes de 62.5/125u y 50/125u de tipos multimodo y monomodo. Velocidades hasta Gbps
Totalmente inmune a EMI y RFI.

MICROONDAS
Frecuencia desde 100 hasta 300 MHz con bajas velocidades susceptible a interferencias atmosféricas

SATELITE
Transmisión de datos vía microondas de alta frecuencia con rango de frecuencias de 1 a 14.5 GHz existencia de tres bandas.

C de 3.7 a 6.4 GHz
Ku de 11.7 a 14.5 GHz
L de 1.64 a 1.66 GHz

APENDICE B
NORMA RS-232

Esta norma fue propuesta por la Asociación de Industrias Electrónicas (el cual, es un organismo registrado de fabricantes de electrónica), y se le conoce propiamente como **EIA RS-232-C**.

La versión internacional se encuentra incluida en la recomendación **V.24** del I.T.U. que es parecida, pero difiere un poco en algunos circuitos que se utilizan rara vez. La terminal o la computadora se nombran oficialmente en las normas como **DTE** (Equipo terminal de datos), y al modem, también oficialmente, se le conoce como **DCE** (Equipo terminal de circuito de datos).

ESPECIFICACIONES

Mecánica Considera un conector de 47.04 mm de ancho (del centro de un tornillo al centro del otro tornillo del mismo) con 25 pines. Todas las demás dimensiones del conector están igualmente bien especificadas. En la fila superior se numeran los pines del 1 al 13 y en la fila inferior del 14 al 25, de izquierda a derecha.

Eléctrica Considera que decidir un 1 binario se debe tener un voltaje más negativo que -3 volts, y que un 0 binario se tendrá cuando el voltaje positivo sea superior a los +4 volts. Es posible tener velocidades de datos de hasta 20 Kbps, así como longitudes de cable de hasta 15 metros.

Funcional Indica los circuitos que están conectados a cada uno de los 25 pines, así como el significado de cada uno de ellos. En la figura B-1 se muestran 9 pines que casi siempre están soportados, el resto de ellos con frecuencia se omiten.

Cuando la terminal o computadora se enciende, ésta activa (es decir, pone un 1 lógico) la señal **Data Terminal Ready** (pin 20). Cuando el modem se enciende, se activa la señal correspondiente al **Data Set Ready** (pin 6). Cuando el modem detecta una portadora sobre la línea telefónica, se activa la señal de **Carrier Detect** (pin 8). El **Request to Send** (pin 4) indica que la terminal quiere enviar datos. El **Clear to Send** (pin 5) significa que el modem está preparado para aceptar datos. Los datos se transmiten con el **Transmit Circuit** (pin 2) y se reciben con el **Receive Circuit** (pin 3).

Especificación del procedimiento Es el protocolo, es decir, el establecimiento de la secuencia legal de eventos. El protocolo está basado en la definición de **pares acción-reacción**. Por ejemplo, cuando la terminal activa el **Request to Send** (Solicitud de envío), el modem contesta con un **Clear to Send** (Libre para enviar) si tiene la capacidad para aceptar la información.

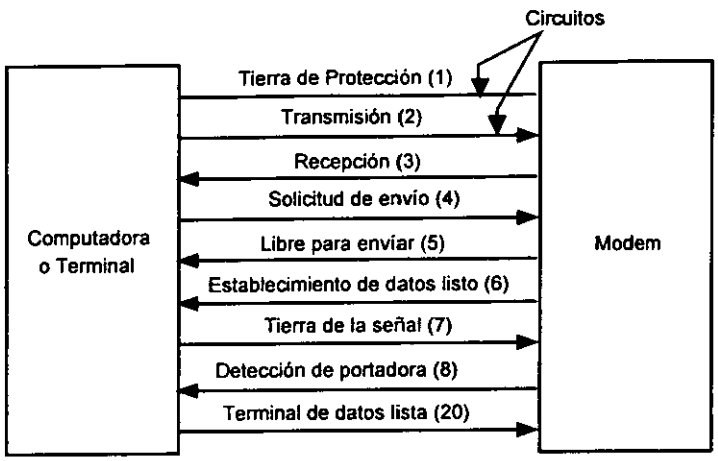


Figura B-1 Circuitos principales del RS-232-C.

APENDICE C

RECOMENDACIÓN PARA MÓDEM

RECOMENDACION	VELOCIDAD (bps)	MODULACION
V.21	300	Duplex y semiduplex FSK
V.22	1200	Duplex PSK
V.26	2400	Semiduplex y duplex DPSK
V.27	4800	semiduplex a dos hilos ó duplex a 4 hilos DPSK
V.29	9600	semiduplex y duplex QAM
V.32	9600	TCM
V.33	14400	TCM

APENDICE D
Estándares de IEEE

Estandar IEEE 802.3 (Ethernet)

La norma o estándar **IEEE 802.3** se utiliza en las redes tipo LAN con protocolo de acceso al medio **CSMA/CD** (Acceso múltiple por detección de portadora con detección de colisión).

Con este protocolo, cuando una computadora desea transmitir, escucha la información que fluye a través del cable. Si el cable se encuentra inactivo, la computadora transmite de inmediato, en caso contrario espera a que se desocupe. Si dos o más computadoras comienzan a transmitir en forma simultánea a través del cable, se generará una colisión. Estas computadoras interrumpirán su transmisión, esperarán un tiempo aleatorio y repetirán de nuevo todo el proceso completo.

La compañía Xerox diseñó un sistema CSMA/CD de 2.94 Mbps, para conectar hasta 100 computadoras personales en un cable de 1 km de longitud. A este sistema se le llamó **Ethernet,** en honor del *éter luminífero,* a través del cual se pensó alguna vez que se propagaban las ondas electromagnéticas.

El sistema Ethernet desarrollado por Xerox tuvo tanto éxito que esta compañía y las empresas DEC e Intel propusieron una norma para un sistema de 10 Mbps, lo que constituyó la base para la norma IEEE 802.3. Esta norma describe una familia completa de sistemas CSMA/CD, operando a velocidades que van de 1 a 10 Mbps, en varios medios físicos.

Mucha gente incorrectamente utiliza el nombre de "Ethernet" en un sentido genérico para referirse a todos los sistemas CSMA/CD, aun cuando éste sólo se refiere al sistema 10 Base 5 especificado en la norma 802.3.

En la figura D-1 se muestra la configuración usual del sistema Ethernet. En ella puede identificarse un **transceptor** que se encuentra sujeto al cable de tal manera que su conector haga contacto con el núcleo. Este **transmisor-receptor** contiene la electrónica necesaria para poder manejar las detecciones de portadora y de colisión. Al detectar una colisión, un transceptor coloca una señal especial de invalidación en el cable para asegurar que todos los demás transceptores tengan conocimiento de ello.

El cable de un transceptor, que contiene 5 pares trenzados, conecta a éste con una tarjeta de interfase que se encuentra en la computadora y puede llegar a tener una longitud de hasta 50 metros.

La longitud máxima permitida para un **cable coaxial Ethernet,** que es el medio de difusión de este sistema, es de 500 metros. Para hacer que el sistema se extienda sobre una distancia mayor, es necesario utilizar **repetidores**. Un repetidor, como se especificará posteriormente, es un dispositivo de la capa física que recibe, amplifica y transmite señales en ambas direcciones.

Un sistema Ethernet puede estar constituido por varios segmentos de cable coaxial y varios repetidores, pero no es posible que dos transceptores se encuentren separados por una distancia mayor de 2.5 km, ni tampoco es posible que exista una trayectoria entre dos transceptores que atraviese más de cuatro repetidores.

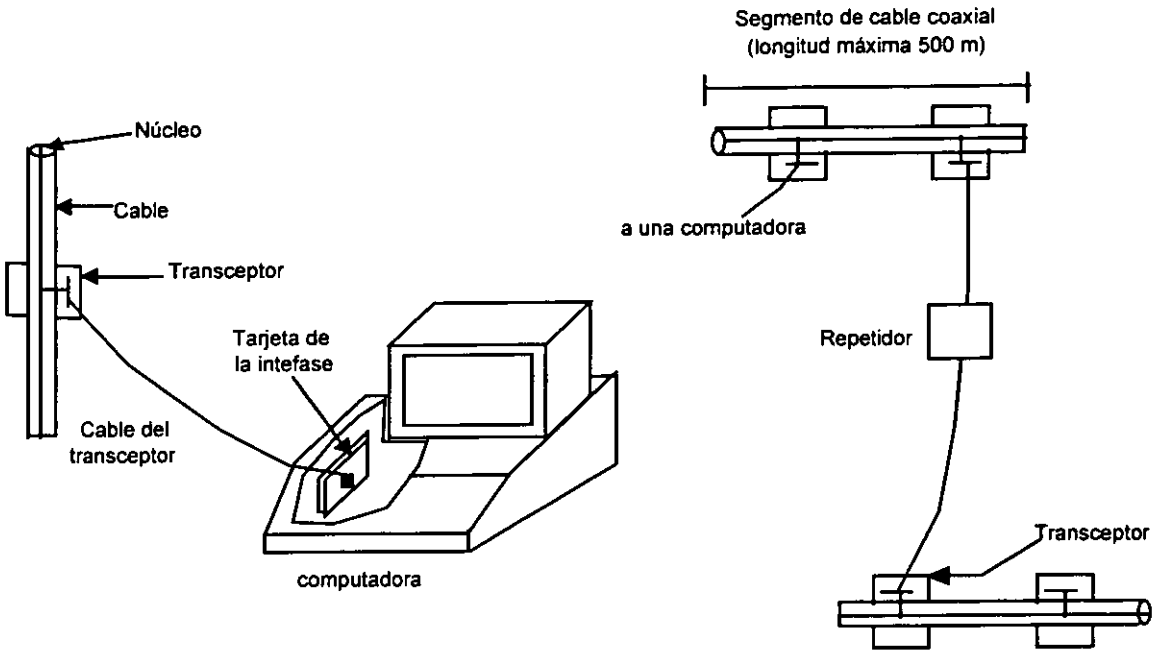


Figura D-1 Red Ethernet:
a) Posición de un transceptor y una interfase.
b) Conexión de dos segmentos de cable usando un repetidor.

Como se mencionó anteriormente la norma 802.3 especifica una familia completa de sistemas, entre los cuales se encuentran:

10 Base 5 Permite una velocidad de 10 Mbps y un segmento de cable coaxial (conector BNC) máximo de 500 m. Se conecta en configuración tipo bus. También conocido como sistema Ethernet.

10 Base 2 La longitud máxima del segmento de cable coaxial (conector BNC) es de 185 m. El cable es más delgado y barato que el del sistema anterior. Soporta velocidades de hasta 10 Mbps y su configuración también es tipo bus.

10 Base-T Maneja velocidades de 10 Mbps. Emplea topología en estrella con conexiones de par trenzado (conectores RJ-45 o AUI). La longitud máxima entre el punto central y los dispositivos es de 100 m.

El término **base** viene de **baseband** lo cual significa que una señal se transmite en su forma original y no modificada por algún proceso de modulación, es decir, que los datos de una computadora se envían en forma digital.

Estandar IEEE 802.4 (Token Bus)

Aunque la norma 802.3 es la que se usa más en la actualidad (sobretodo en oficinas), dado que cuenta con una enorme infraestructura y una considerable experiencia operativa, durante el desarrollo de la norma 802, General Motors y otras compañías interesadas en la automatización de fábricas, fueron bastante escépticas con respecto a ella. La razón fue que, debido a la característica probabilística de su protocolo CSMA/CD, con un poco de mala suerte, un dispositivo tendría que esperar mucho tiempo en forma arbitraria, para poder transmitir una trama (en el peor de los casos

ilimitado). Otra razón, es que las tramas de la norma 802.3 no gozan de prioridad alguna, de tal forma que resultan inadecuadas para sistemas de tiempo real, en los que las tramas importantes no pueden retrasarse debido a las que son intranscendentes.

Para solucionar estos problemas se diseñó la **norma 802.4** conocida como **Token Bus.** En los sistemas Token Bus, los dispositivos están físicamente conectados a un bus (cable lineal), pero están organizados lógicamente en un anillo (fig.D-2).

En el anillo cada uno de los dispositivos conoce la dirección del dispositivo a su "izquierda" y "derecha". Cuando el anillo lógico se inicia, el dispositivo que tiene la prioridad mayor es el que puede enviar la primera trama. Después de que éste lo hizo, pasa la autorización a su vecino inmediato, mediante una trama de control especial llamada **token** para que éste a su vez pueda transmitir información. El token se propaga alrededor del anillo lógico, de tal forma que sólo su poseedor está autorizado para transmitir tramas. Como solamente un dispositivo puede tener el token a la vez, no hay posibilidad de colisiones. Este método de acceso al medio se conoce con el nombre de **Token-passing**.

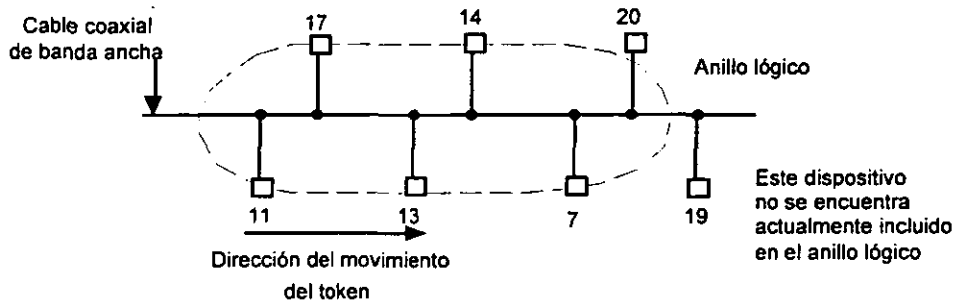


Figura D-2 Red Token Bus.

Un punto interesante que hay que entender es que el orden físico en el que se encuentran conectados los dispositivos al cable no es importante. Como el bus es de manera inherente un medio físico de difusión, cada dispositivo recibe todas las tramas y descarta las que no le están dirigidas. Cuando un dispositivo pasa el token, envía una trama de token dirigida específicamente a su vecino lógico en el anillo, independiente del lugar físico en donde se encuentre en el bus.

Es importante también hacer notar que, cuando los dispositivos se activan por primera vez éstos no están dentro del anillo (por ejemplo, obsérvese el caso de los dispositivos 19 y 20 en la figura D-2), de tal forma que el protocolo MAC tiene la capacidad para agregar y retirar dispositivos del anillo. El *protocolo MAC de la norma 802.4 es bastante complejo.*

Para la capa física, se utiliza el cable coaxial de banda ancha de 75 ohms que normalmente se emplea para televisión por cable. El término **banda ancha** significa que se usan señales analógicas para transmitir los datos.

Se pueden manejar velocidades de 1, 5 y 10 Mbps. La capa física, en su totalidad, es completamente incompatible con la de la norma 802.3 y tiene un grado de complejidad mucho mayor.

Estandar IEEE 802.5 (Token Ring)

Las redes en anillo han tenido un empleo muy significativo tanto en redes de área local como en las que tienen mayor cobertura geográfica.

Entre sus muchas características atractivas, está el hecho de que un anillo se comporta como un medio de difusión, pero realmente es una colección de enlaces punto a punto individuales que conforman un círculo. Los enlaces punto a punto utilizan una tecnología que ha sido muy bien entendida y probada en la práctica, y puede funcionar en medios como par trenzado, cable coaxial o fibra óptica.

IBM seleccionó al anillo como su LAN y la IEEE ha incluido una norma de anillo en la **802.5** (compatible con la de IBM) denominada **Token Ring** y que también está basada en el método de acceso al medio **Token-passing.**

Como se mencionó anteriormente, un anillo está constituido en realidad por una colección de interfases de anillo conectadas por medio de líneas punto a punto. En la figura D-3 se muestran una red Token Ring y sus modos de operación.

En una red Token Ring se tiene un patrón de bits especial, el cual se conoce como **token**, que circula alrededor del anillo siempre que los dispositivos se encuentren inactivos (sin transmitir). Cuando un dispositivo quiera transmitir una trama, necesita capturar el token y quitarlo del anillo, antes de efectuar la transmisión. Debido a que solamente hay un token, un solo dispositivo puede transmitir en un instante dado, por lo que se resuelve el problema del acceso al canal del mismo modo que en las redes Token Bus.

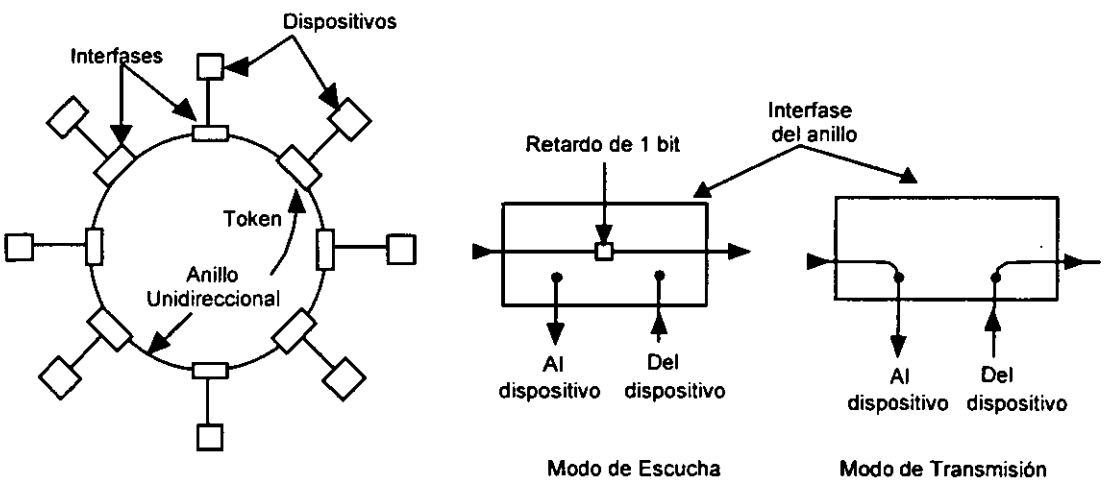


Figura D-3 Red Token Ring y sus modos de operación.

Hay dos modos de operación de las interfases del anillo, uno para escuchar y el otro para transmitir.

En el modo de escucha, cada uno de los bits que llegan a una interfase se copia en una memoria temporal para después copiarse de nuevo sobre el anillo. Mientras el bit se encuentre en la memoria temporal, puede inspeccionarse, y quizá hasta modificarse, antes de ser escrito nuevamente sobre el anillo. Este proceso de copiado introduce un retardo de 1 bit en cada

interfase. En el modo de escucha, un dispositivo verifica la dirección que tiene el paquete de datos y en caso de que sea su dirección lo procesa.

En el modo de transmisión, que sólo ocurre después de que el token ha sido capturado, la interfase rompe la conexión existente entre su entrada y su salida para introducir sus propios datos al interior del anillo.

A medida que regresan los bits que se han propagado alrededor del anillo, el transmisor los retira del anillo directamente. El dispositivo transmisor puede optar por almacenarlos, con objeto de compararlos con los datos originales para controlar la confiabilidad del anillo, o bien, desecharlos.

Después de que un dispositivo ha terminado de transmitir el último bit de su última trama, deberá regenerar el token. Cuando el último bit de la trama haya recorrido la trayectoria y haya regresado, se deberá retirar, y la interfase deberá conmutarse inmediatamente al modo de escucha, para evitar perder el token y tener la posibilidad de volver a transmitir en caso de que ningún otro dispositivo lo haya recogido.

Cuando el tráfico sea moderado, el token pasará la mayor parte de su tiempo en un estado inactivo, circulando alrededor del anillo; ocasionalmente será capturado por un dispositivo para transmitir una trama y, después, será emitido nuevamente.

Sin embargo, cuando el tráfico sea muy elevado, de tal forma que haya una cola de espera en cada dispositivo, tan pronto como un dispositivo termine su transmisión y regenere el token, el siguiente dispositivo en orden descendente lo verá y lo retirará.

De este manera, la autorización para transmitir información gira paulatinamente alrededor del anillo, siguiendo un orden de transmisión en cadena. La eficiencia de la red puede llegar a acercarse al 100 % bajo condiciones de carga elevada.

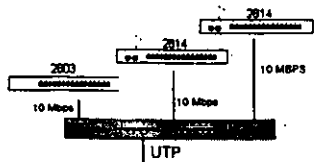
En la capa física, la norma 802.5 define la utilización de pares trenzados y velocidades de 1, 4 y 16 Mbps.

APENDICE E
INVENTARIO SAT

CONJUNTO HIDALGO
Modulo 1

INSTER

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BSETX
4 PTO. OCUPADOS
8 PTOS 10/100 LIBRES



100 Mbps

UTP

OC-3

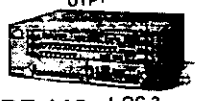
IDF 111

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BSETX
3 PTO. OCUPADOS
2 PTOS A 10/100 PARA SERVIDORES
3 PTOS 10/100 PARA CRECIMIENTO
3 PTOS 10/100 PRIORITARIOS
1 PTOS LIBRES

100 Mbps

UTP



OC-3

IDF 112

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

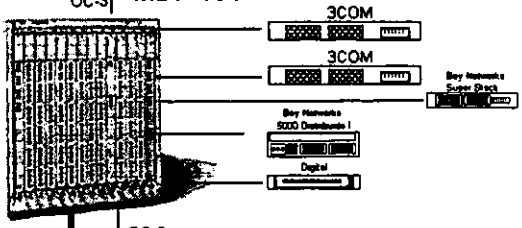
P1

155 MBPS

155 MBPS

OC-3

MDF 101



OC-3

OC-12

OC-3

EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
2 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

ESPECIFICACIONES:
3 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTO ATM OC-12 A 622 MBPS
5 PTOS 10/100 Ocupados
2 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIOS
15 PTOS 10/100 LIBRES
9 SLOTS LIBRES

HACIA MODULO 2

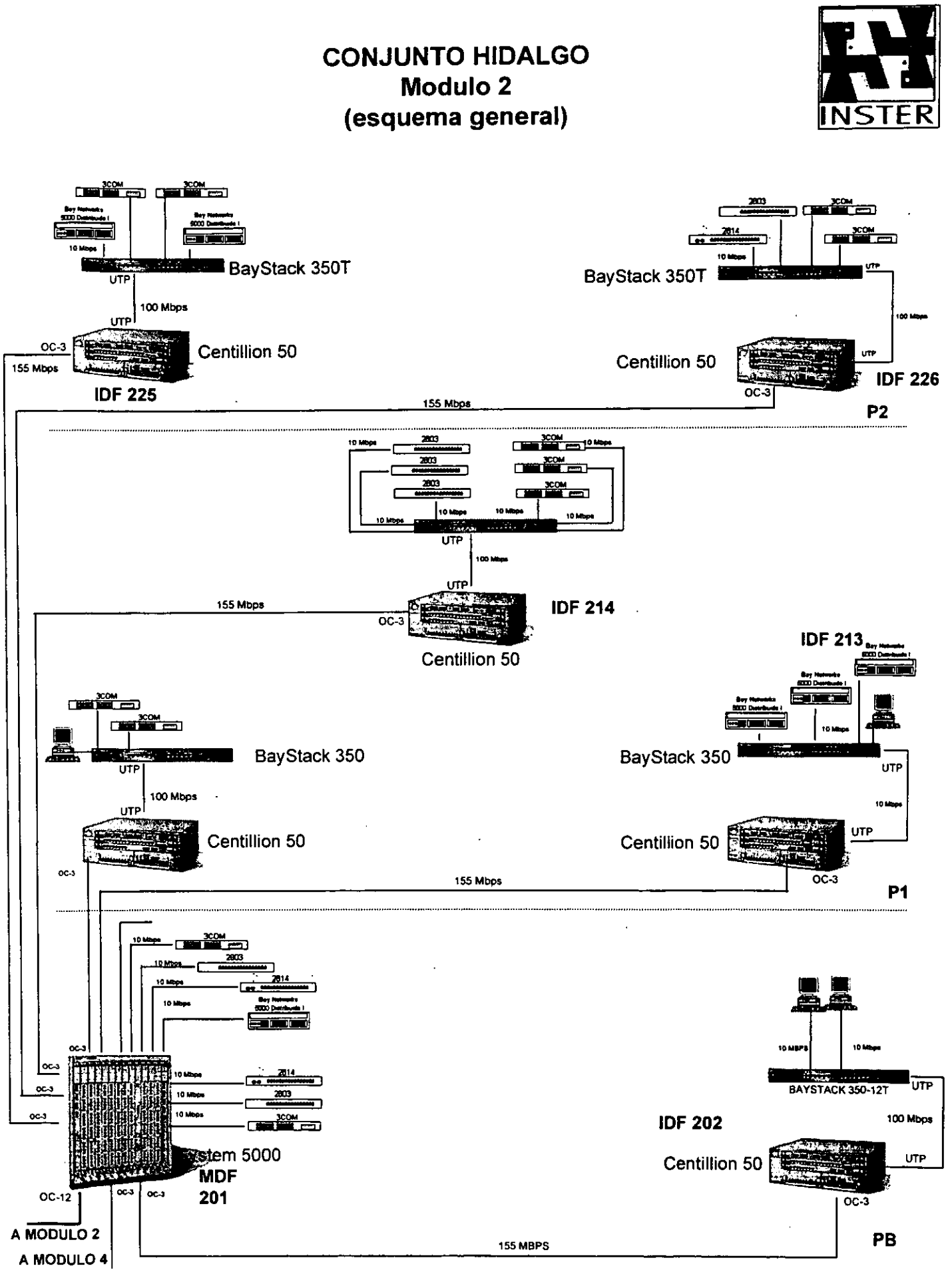
622 Mbps

HACIA MODULO 4

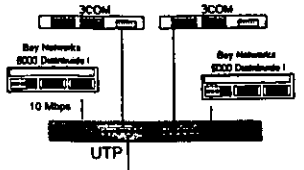
155 Mbps

PB

CONJUNTO HIDALGO
Modulo 2
(esquema general)



CONJUNTO HIDALGO
Modulo 2-A



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
5 PTO. 10/100 OCUPADOS
7 PTOS 10/100 LIBRES

100 Mbps

UTP

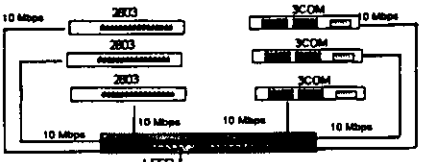
OC-3
155 Mbps

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 225

155 Mbps — **A IDF226** — **P2**



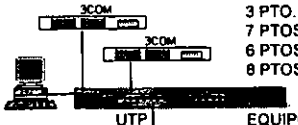
EQUIPO :
1 BAYSTACK 350T 12 PTS 10/100BASETX
7 PTO. 10/100 OCUPADOS
2 PTO 10/100 PRIORITARIO
3 PTOS 10/100 LIBRES

155 Mbps

OC-3

IDF 214

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BSETX
3 PTO. 10/100 OCUPADOS
7 PTOS 10/100 SERVIDORES
6 PTOS 10/100 PARA CRECIMENTO
8 PTOS 10/100 LIBRES

IDF 212

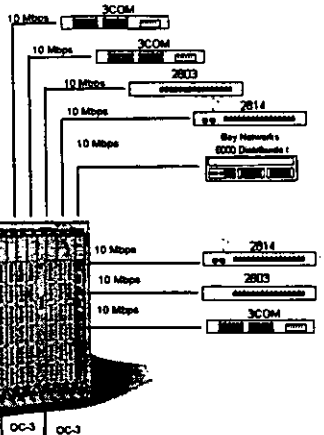
100 Mbps

UTP

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

OC-3

155 Mbps — **A IDF213** — **P1**



EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
1 TARJETA ATM MDA
4 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

ESPECIFICACIONES:
7 PTO. ATMOC-3 A 155 MBPS
1 PTOS ATM OC-3 LIBRE
1 PTO ATM OC-12 A 622 MBPS
8 PTOS 10/100 Ocupados
16 PTOS 10/100 LIBRES
8 SLOTS LIBRES

MDF 201

PB

OC-12

OC-3 OC-3

A IDF202

155 MBPS

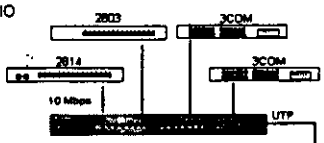
A MODULO 2

A MODULO 4

CONJUNTO HIDALGO
Modulo 2-B

IDF 226

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
5 PTO. 10/100 OCUPADOS
2 PTO 10/100 SERVIDORES
3 PTO 10/100 CRECIMIENTO
2 PTO 10/100 PRIORITARIO



EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

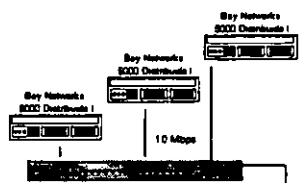
A MDF 201

155 Mbps

P2

IDF 213

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BSETX
4 PTO. 10/100 OCUPADOS
8 PTOS 10/100 LIBRES



EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

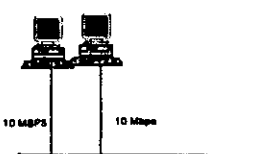
A MDF 201

155 Mbps

P1

IDF 202

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
1 PTO 10/100 OCUPADO
1 PTO 10/100 PARA SERVIDOR
3 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
5 PTOS 10/100 LIBRES



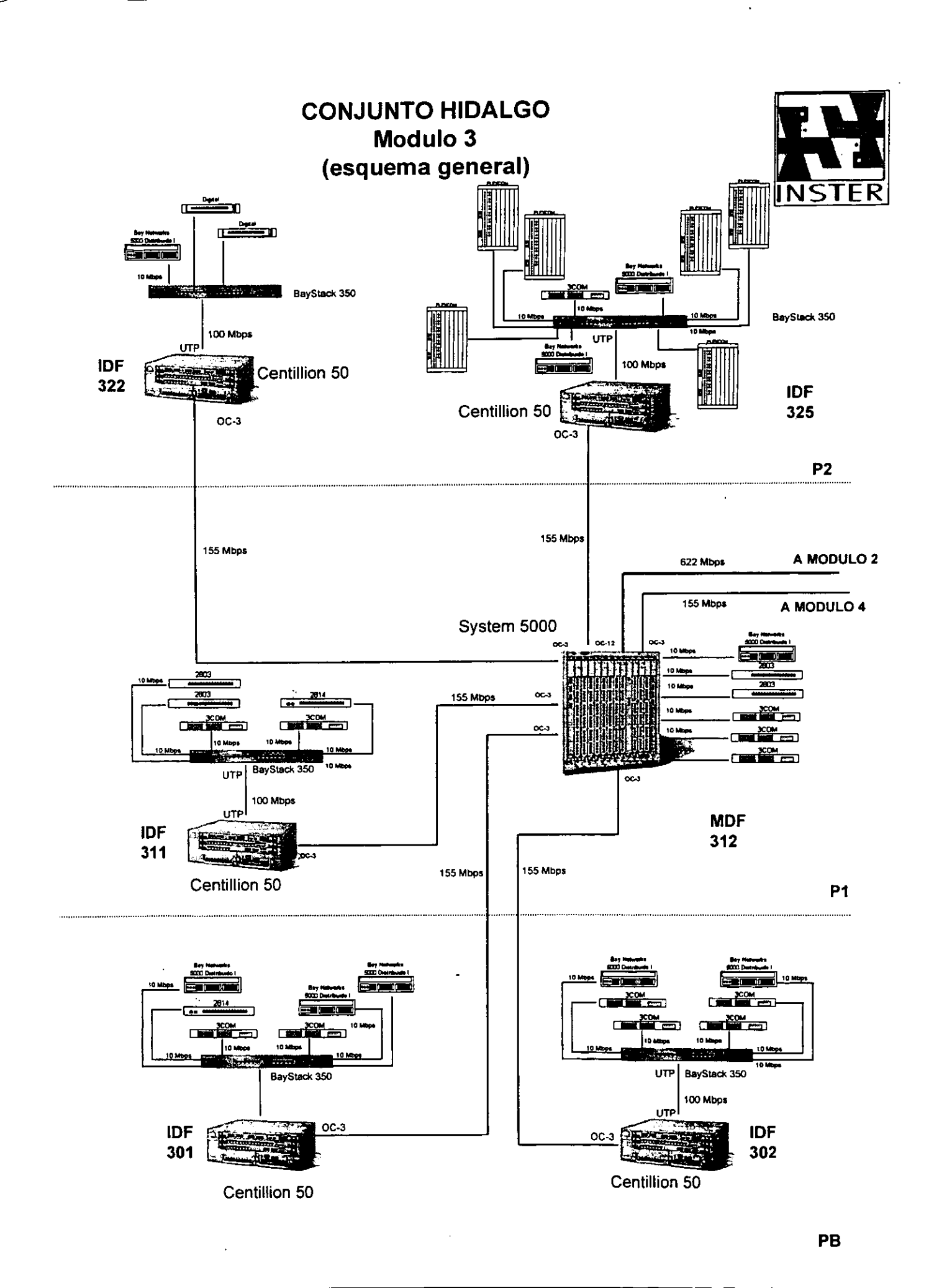
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

A MDF 201

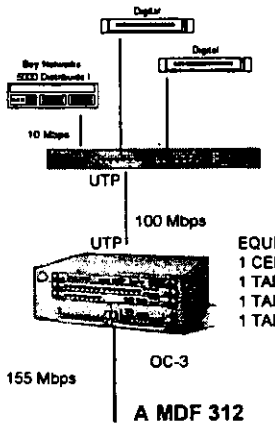
155 MBPS

PB

CONJUNTO HIDALGO
Modulo 3
(esquema general)



CONJUNTO HIDALGO
Modulo 3-A



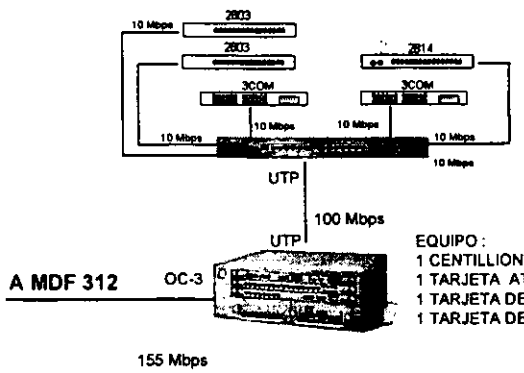
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
4 PTO. 10/100 OCUPADOS
2 PTOS 10/100 SERVIDORES
5 PTOS 10/100 CRECIMIENTO
1 PTOS 10/100 PRIORITARIOS
0 PTO 10/100 LIBRES

IDF 322

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2



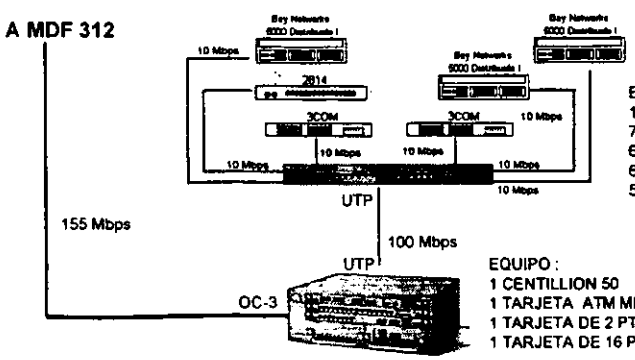
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
6 PTO. 10/100 OCUPADOS
1 PTOS 10/100 SERVIDORES
4 PTOS 10/100 CRECIMIENTO
1 PTOS 10/100 PRIORITARIOS

IDF 311

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
6 PTOS 10/100 SERVIDORES
6 PTOS 10/100 CRECIMIENTO
5 PTOS 10/100 LIBRES

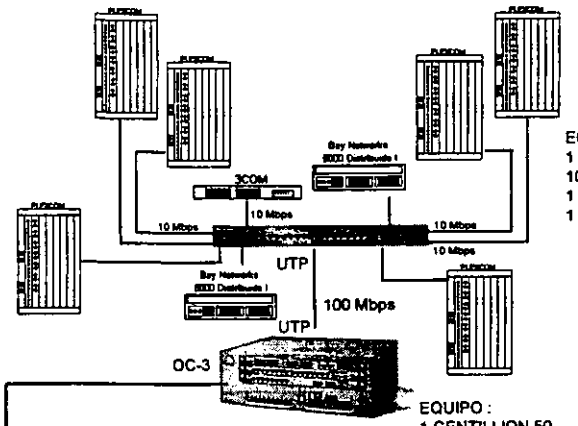
IDF 301

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 3-B



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
10 PTO. 10/100 OCUPADOS
1 PTO 10/100 PRIORITARIO
1 PTOS 10/100 LIBRES

IDF 325

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2

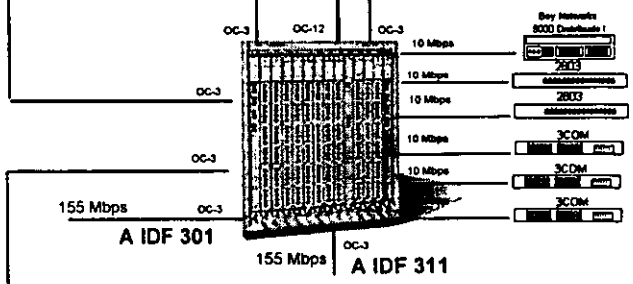
155 Mbps

A IDF 322

622 Mbps — **A MODULO 2**

155 Mbps — **A MODULO 4**

155 Mbps



155 Mbps — **A IDF 301**

155 Mbps — **A IDF 311**

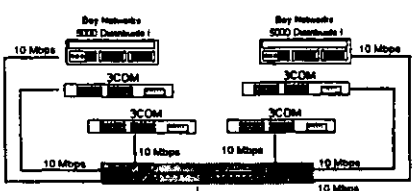
MDF 312

EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
1 TARJETA ATM MDA
3 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

ESPECIFICACIONES:
6 PTO. ATM OC-3 A 155 MBPS
0 PTO ATM OC-3 LIBRE
1 PTO ATM OC-12 A 622 MBPS
6 PTOS 10/100 Ocupados
18 PTOS 10/100 LIBRES
8 SLOTS LIBRES

155 Mbps

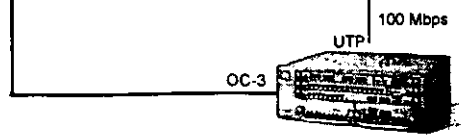
P1



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
2 PTOS 10/100 PRIORITARIOS
3 PTOS 10/100 LIBRES

IDF 302

100 Mbps

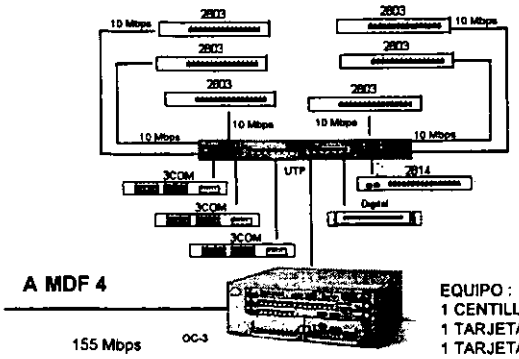


EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 4-A



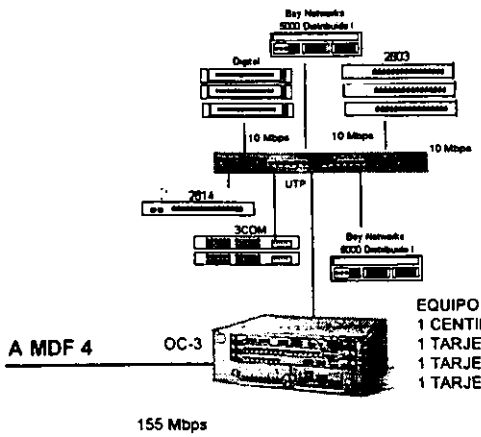
EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
12 PTO 10/100 OCUPADOS
5 PTOS 10/100 SERVIDORES
6 PTOS 10/100 CRECIMIENTO
1 PTO 10/100 LIBRE

IDF 421

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2



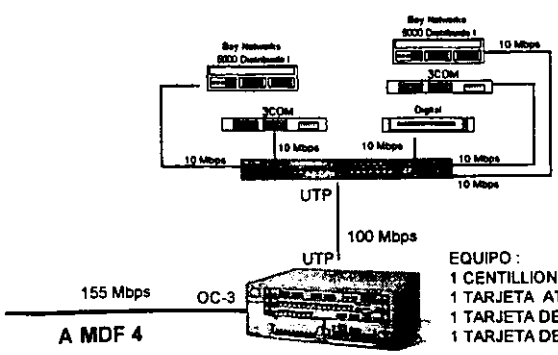
EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
4 PTOS 10/100 SERVIDORES
7 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
4 PTOS 10/100 LIBRES

IDF 411

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
6 PTO. 10/100 OCUPADOS
1 PTOS 10/100 SERVIDORES
3 PTOS 10/100 CRECIMIENTO
2 PTIS 10/100 LIBRES

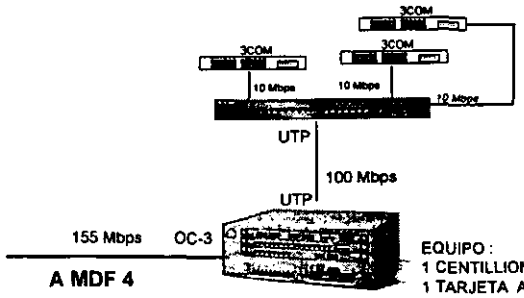
IDF 401

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 4-B



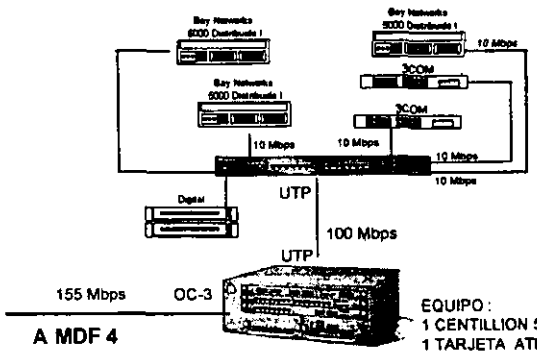
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
4 PTO. 10/100 OCUPADOS
2 PTOS PRIORITARIOS
6 PTOS 10/100 LIBRES

IDF 422

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2



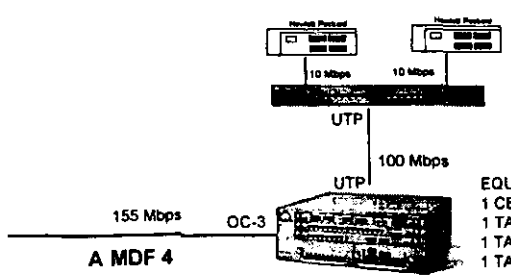
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
5 PTOS 10/100 LIBRES

IDF 412

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
2 PTOS 10/100 PRIORITARIOS
7 PTOS 10/100 LIBRES

IDF 402

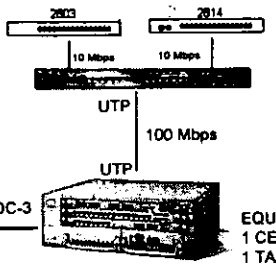
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 4-C

INSTER



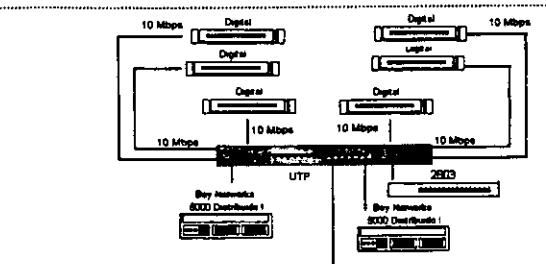
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
1 PTO 10/100 CRECIMIENTO
2 PTO 10/100 PRIORITARIO
6 PTOS 10/100 LIBRES

IDF 461

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P6



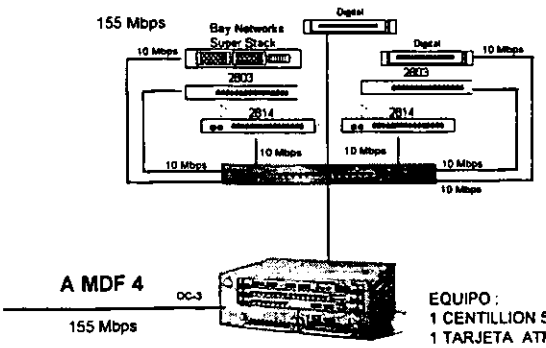
EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
10 PTO. 10/100 OCUPADOS
7 PTOS 10/100 SERVIDORES
4 PTO 10/100 CRECIMIENTO
2 PTO 10/100 PRIORITARIO
1 PTO 10/100 LIBRES

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 451

P5



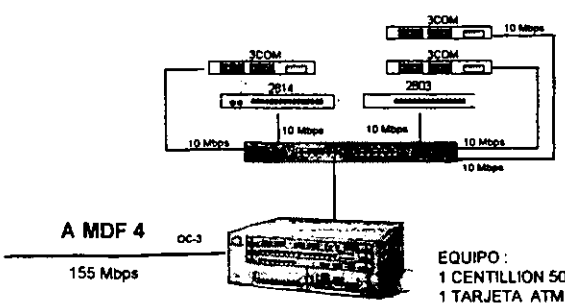
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
8 PTO. 10/100 OCUPADOS
2 PTOS 10/100 PRIORITARIO
2 PTOS 10/100 LIBRES

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 441

P4



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
6 PTO. 10/100 OCUPADOS
2 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
2 PTOS 10/100 LIBRES

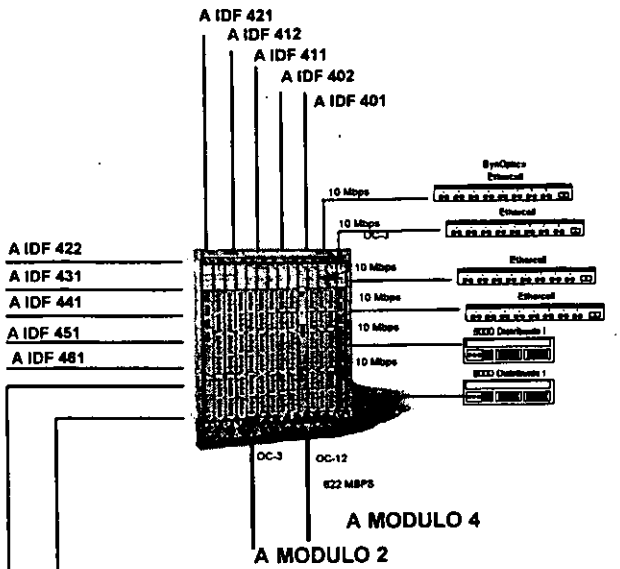
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 431

P3

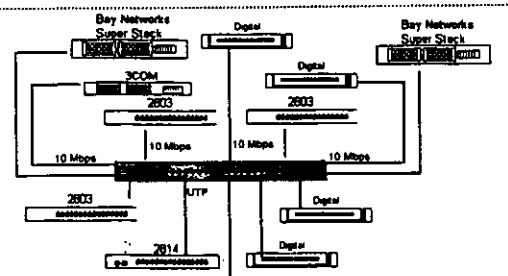
CONJUNTO HIDALGO
Modulo 4-D



EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
3 TARJETA ATM MDA
7 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR
ESPECIFICACIONES:
13 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTO ATM OC-12 A 622 MBPS
6 PTOS 10/100 OCUPADOS
18 PTOS 10/100 LIBRES
6 SLOTS LIBRES

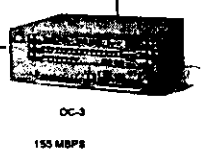
MDF 4

P5



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
12 PTO. 10/100 OCUPADOS
4 PTOS 10/100 SERVIDORES
7 PTOS 10/100 CRECIMIENTO
1 PTOS 10/100 LIBRES

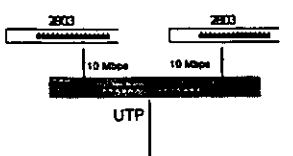
IDF 442



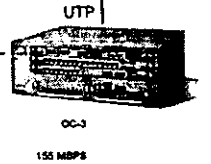
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P4



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
9 PTOS 10/100 LIBRES



EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

MDF 432

P3

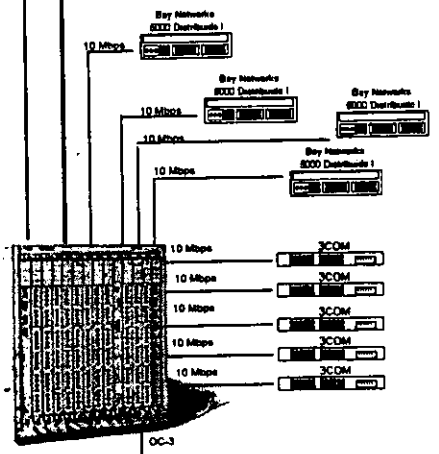
CONJUNTO HIDALGO
Modulo 5

A MODULO 2

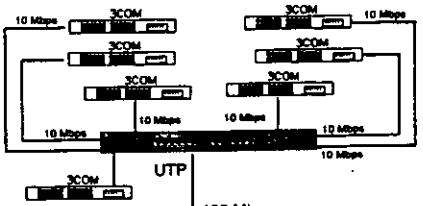
A MODULO 4

155 Mbps

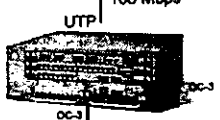
622 Mbps



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
8 PTO. 10/100 OCUPADOS
2 PTOS 10/100 SERVIDORES
6 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIOS
6 PTOS 10/100 LIBRES



100 Mbps



IDF 512

155 Mbps

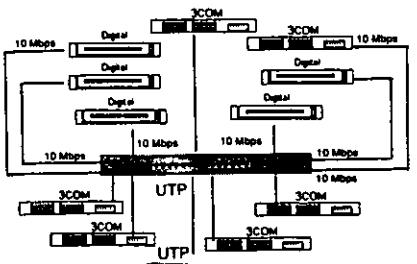
EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
2 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR
ESPECIFICACIONES:
3 PTO. ATMOC-3 A 155 MBPS
1 PTOS ATM OC-3 LIBRE
1 PTO ATM OC-12 A 622 MBPS
9 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES
9 SLOTS LIBRES

MDF 511

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1

155 Mbps



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
12 PTO. 10/100 OCUPADOS
4 PTOS 10/100 SERVIDORES
1 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
5 PTOS 10/100 LIBRES

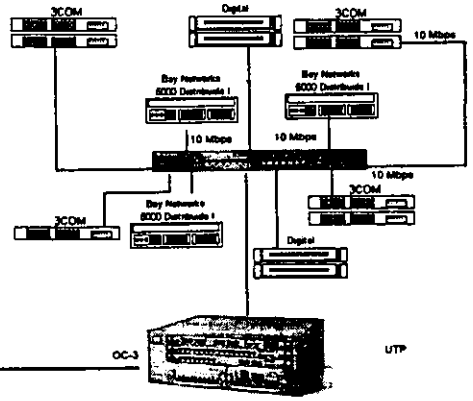
IDF 501

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 6



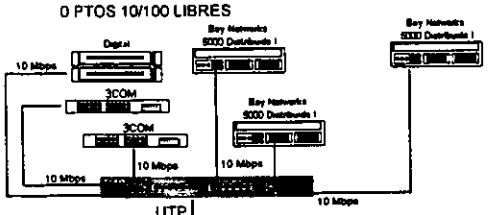
EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
10 PTO. 10/100 OCUPADOS
2 PTOS 10/100 SERVIDORES
5 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
5 PTOS 10/100 LIBRES

IDF 621

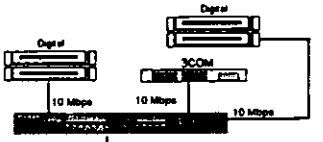
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2

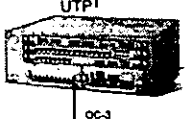
EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
1 PTOS 10/100 SERVIDORES
4 PTO 10/100 CRECIMIENTO
0 PTOS 10/100 LIBRES



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
4 PTO. 10/100 OCUPADOS
1 PTO. 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
5 PTOS 10/100 LIBRES



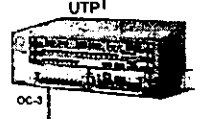
UTP



EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 611

155 Mbps

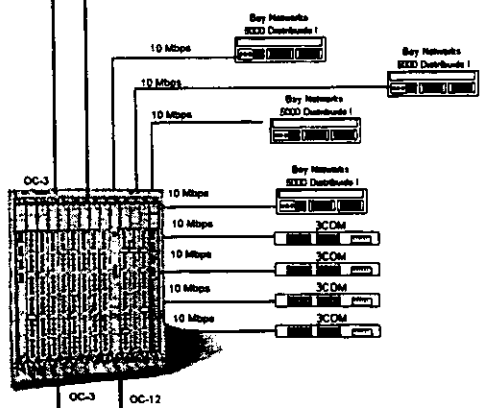


EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

IDF 612

155 Mbps

P1



EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
2 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

ESPECIFICACIONES:
4 PTO. ATMOC-3 A 155 MBPS
0 PTOS ATM OC-3 LIBRES
1 PTO ATM OC-12 A 622 MBPS
8 PTOS 10/100 Ocupados
16 PTOS 10/100 LIBRES
9 SLOTS LIBRES

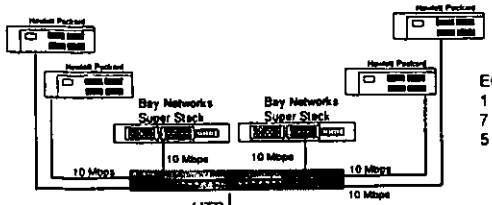
MDF 601

A MODULO 2

A MODULO 4

PB

CONJUNTO HIDALGO
Modulo 7



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
7 PTO. 10/100 OCUPADOS
5 PTOS 10/100 LIBRES

1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
11 PTOS 10/100 SERVIDORES
6 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
4 PTOS 10/100 LIBRES

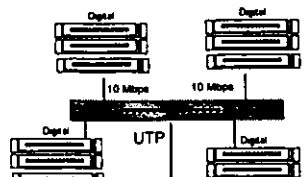
100 Mbps
UTP
OC-3

IDF 761

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P6



EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
12 PTO. 10/100 OCUPADOS
4 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
6 PTOS 10/100 LIBRES

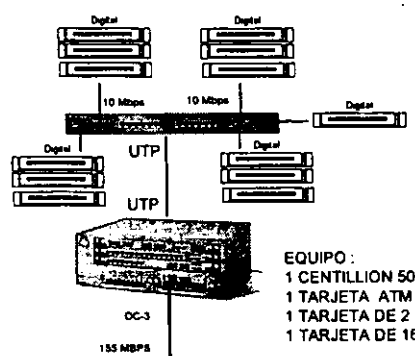
IDF 731

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P3

155 MBPS



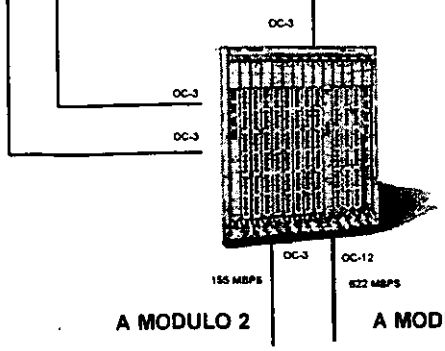
EQUIPO :
1 BAYSTACK 350T 24 PUERTOS 10/100BASETX
6 PTO. 10/100 OCUPADOS
8 PTOS 10/100 SERVIDORES
7 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
1 PTOS 10/100 LIBRES

IDF 711

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1



EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
2 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

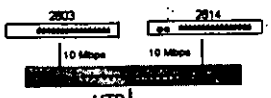
ESPECIFICACIONES:
4 PTO. ATMOC-3 A 155 MBPS
0 PTOS ATM OC-3 LIBRES
1 PTO ATM OC-12 A 622 MBPS
8 PTOS 10/100 Ocupados
16 PTOS 10/100 LIBRES
9 SLOTS LIBRES

A MODULO 2 **A MODULO 4**

MDF 701

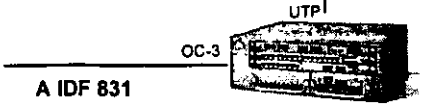
PB

CONJUNTO HIDALGO
Modulo 8-A



EQUIPO :
BAYSTACK 350T 12 PUERTOS 10/100BASETX
6 PTO. 10/100 OCUPADOS
1 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
6 PTOS 10/100 LIBRES

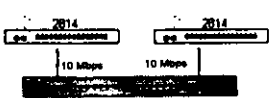
IDF 821



EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

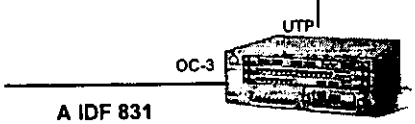
ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P2



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
1 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
6 PTOS 10/100 LIBRES

IDF 811



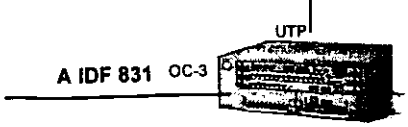
EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P1

EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
2 PTOS 10/100 SERVIDORES
2 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
3 PTOS 10/100 LIBRES

IDF 801

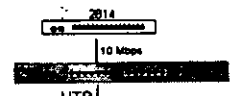


EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

PB

CONJUNTO HIDALGO
Modulo 8-B



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
2 PTO. 10/100 OCUPADOS
1 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
7 PTOS 10/100 LIBRES

IDF 851

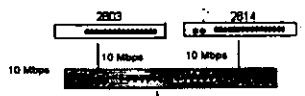
UTP

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

P5

155 MBPS



EQUIPO :
1 BAYSTACK 350T 12 PUERTOS 10/100BASETX
3 PTO. 10/100 OCUPADOS
1 PTO 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
6 PTOS 10/100 LIBRES

IDF 841

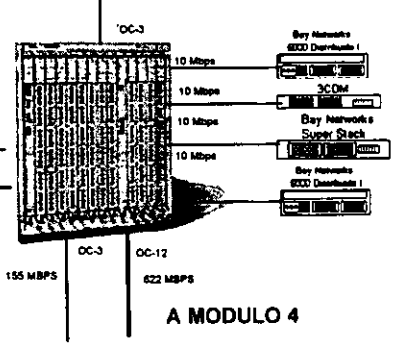
UTP

EQUIPO :
1 CENTILLION 50
1 TARJETA ATM MDA MCP
1 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA DE 16 PTOS (100BASETX)

ESPECIFICACIONES:
1 PTO. ATMOC-3 A 155 MBPS
1 PTO ATM OC-3 LIBRE
1 PTOS 10/100 Ocupados
15 PTOS 10/100 LIBRES

155 MBPS

P4



A IDF 821
A IDF 811
A IDF 801

A MODULO 4

A MODULO 2

EQUIPO :
1 SYSTEM 5000
1 TARJETA SUPERVISORA 5110
1 TARJETA DE 24 PTOS. 10/100BASE TX AUTOSENSE
1 TARJETA ATM MDA MCP
2 TARJETA ATM MDA
3 TARJETA DE 2 PTOS. SONET/SDH MMF ATM
1 TARJETA ATM MDA MCP CON 1 PUERTO SONET MMF OC-12
1 TARJETA 5782 CENTILLION MULTIPROCOL
SOFTWARE SYSTEM 5000 ATM VNR

ESPECIFICACIONES:
6 PTO. ATMOC-3 A 155 MBPS
0 PTOS ATM OC-3 LIBRES
1 PTO ATM OC-12 A 622 MBPS
4 PTOS 10/100 OCUPADOS
3 PTOS 10/100 SERVIDORES
2 PTOS 10/100 CRECIMIENTO
2 PTOS 10/100 PRIORITARIO
13 PTOS 10/100 LIBRES
7 SLOTS LIBRES

MDF 831

P3

BIBLIOGRAFIA

1. **Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture.**
   Douglas E. Comer
   3rd edition, 1995
   Prentice Hall
2. **Redes globales de Inf. con Internet y TCP / IP**
   Douglas E. Comer
   3ra edición
   Prentice Hall / Pearson
3. **Routing TCP/IP Volume I (CCIE Professional Development)**
   Jeff Doyle
   Vol.1, 1998
   Cisco Systems
4. **Redes de computadoras**
   Tanenbaum
   3ra edición
   Prentice Hall / Pearson
5. **IP Routing Fundamentals**
   Mark A. Sportack, Julie Fairweather
   1999
   Cisco Press
6. **Designing Cisco Networks**
   ***Cisco Systems Incorporated Diane Teare* (Editor)**
   1999
   Cisco Systems Inc
7. **Core Technologies NT (Windows NT 4.0)**
   1999
   Microsoft Inc.

BIBLIOGRAFIA

8. **Enterprise Manager NT (Windows NT 4.0)**
   1999
   Microsoft Inc
9. **Cisco Router Configuration**
   Allan Leinwand Bruce Pinsky
   1998
   Cisco Systems Inc
10. **Understanding Local Area Networks**
    Neil Jenkins Stanley Schatt
    1995
    Sams
11. **Tópicos en Telecomunicaciones Redes de Datos**
    Dr. Leonardo Soto Sumuano
    1997
    GS Comunicaciones
12. **Estudios de Factibilidad en Redes de Comunicaciones**
    Notas de Estudios
    Instituto Mexicano de Comunicaciones
13. **Integración de Voz y Datos**
    Cisco Seminar Series
    1998
14. **Voice Networking Study**
    Manual Motorola University
    1999

BIBLIOGRAFIA

15. Backbone Applications Guide

Nick Lippis – Strategic Network Consultants

2000

16. Revista RED

Número 112

2000

17. Revista DATA COMMUNICATIONS

1998

18. Telecommuting Access Equipment

Competitive Analysis - Folleto

1995

19. The Buyer's Guide to Frame Relay Networking

Tom Jones

Ken Rehbehn

Netrix Corporation

Páginas WEB Internet

1. **www.frforum.com**
2. **www.atmforum.com**
3. **www.cisco.com**
4. **www.motorola.com**